

Number, Space and the Structures of Mathematics

Scott A. Taylor

with illustrations by Michael Scholz

Contents

Introduction	vii
To the student	xii
To the teacher	xv
1 Sets	1
1.1 Sets, informally	3
1.2 Proving set membership	7
1.3 Subsets	12
1.4 Sets whose elements are sets	16
1.5 Proving set equality	19
1.6 Uniqueness of certain elements	22
1.7 Additional Exercises	24
2 Sets with Structure	27
2.1 Groups	29
Examples and non-examples of groups	30
Two theorems about groups	32
2.2 Metric Spaces	33
Examples and non-examples of metric spaces	35
Theorems concerning metric spaces	36
2.3 Graphs	37
2.4 The natural numbers	41
Arithmetic with natural number systems	46
2.5 Application: Symmetry Groups	49

2.6 Appendix: Euclidean metric	53
3 Logic	55
3.1 Statements, predicates, and quantifiers	56
3.2 Conjunctions, and Disjunctions	57
3.3 Negations	63
Negations of simple statements	63
Negations of conjunctions and disjunctions	64
Negations with quantifiers	65
3.4 Implications	69
Implications and their negations	70
Implication and predicates	72
Implications and natural language	73
How to prove an implication is true	74
Equivalent statements	76
3.5 A remark on uniqueness	77
3.6 Basic exercises in logic	78
3.7 Russell's Paradox	82
3.8 Application: The Halting Problem	86
4 Proof Techniques I	89
4.1 Direct Proof	89
4.2 Proof by Contraposition	91
4.3 Proof by Contradiction	92
4.4 Existence	95
4.5 Uniqueness	97
4.6 Application: <i>p</i> -values and Scientific Reasoning	98
4.7 Writing Well	101
4.8 Additional Proofs	104
5 Building Sets	106
5.1 Subsets	107
5.2 Complements	109
5.3 Intersections	111

5.4	Unions	116
5.5	Power Sets	120
5.6	Cartesian Products	122
5.7	The persistence of structure	125
	Convexity	126
	Groups	130
	Open sets in \mathbb{R}^2	133
	Event Spaces	136
5.8	Application: Configuration Spaces	139
5.9	Application: The geometric structure of data	141
5.10	Additional Problems	145
6	Set Theory Axiomatics	148
6.1	The ZFC axioms	151
6.2	The controversies	159
6.3	The existence of a natural number system	160
6.4	The existence of the Cartesian product	162
6.5	Functions, Formally	163
7	Equivalence Relations	166
7.1	Partitions	167
7.2	Equivalence Relations	171
7.3	Equivalence Classes	176
7.4	Quotient Sets	181
7.5	Equivalence Relations vs. Partitions	185
7.6	Angle addition	186
7.7	Constructing the integers and rationals	188
	Constructing the integers	188
	Constructing the rationals	189
7.8	Modular Arithmetic	191
7.9	Application: Configuration spaces of unlabelled points	194
7.10	Additional Problems	197
8	Functions	201

8.1	The definition of a function	202
8.2	Visualizing Functions	209
	Graphs of functions	209
	Venn Diagrams	210
	Dots and arrows	210
	Labels and lightbulbs	211
	Transformations	213
8.3	Important Functions	215
	Identity Functions	215
	Constant Functions	215
	Coordinate functions	215
	Sequences	216
8.4	Extended examples	218
	Paths in graphs	218
	Rotations of a circle	221
8.5	Combining and adapting functions	223
	Restricting Domains and Codomains	223
	Composing Functions	225
8.6	Being Well-defined	227
8.7	Properties of Functions	231
	Injective/Surjective/Bijective	231
	Inverses	241
	Algebraic and Metric Structures	243
8.8	Application: Affine Encryption	247
8.9	Application: Campanology	250
8.10	Application: Probability Functions	255
8.11	Application: Electrical Circuits	257
8.12	Additional Problems	261
9	Proof Techniques II	266
9.1	Regular old induction	267
9.2	Complete Induction	283
9.3	Well-Ordering Principle	294

9.4	Constructing sequences recursively	301
9.5	Other induction methods	305
	Induction over the Reals	305
	Well-orderings and transfinite induction	307
9.6	Application: Probability	311
9.7	Application: Iterated Function Systems	313
9.8	Application: Paths in Graphs	317
	Eulerian Paths and Circuits	317
	DNA sequencing	320
9.9	Additional Exercises	323
9.10	Appendix: The Well-Ordering Theorem	325
10	The sizes of sets	328
10.1	Finite Sets	328
10.2	Infinite Sets	333
10.3	Countable Sets	337
10.4	Uncountable Sets	341
10.5	Producing Larger Cardinalities	343
10.6	The Cantor-Bernstein Theorem	346
10.7	Application: Transcendental Numbers	349
10.8	Application: Countable Sets and Probability	353
10.9	The cardinal numbers	356
10.10	Application: Cardinality and Symmetry	359
10.11	Application: dimension and space-filling curves	366
	Intervals and Trees	371
	Squares and Trees	374
	Constructing the Hilbert Curve	377
	Image Compression	384
10.12	Application: Infinity in the Humanities	387
	Philosophical, Religious, and Mathematical conceptions of the Infinite	388
	The infinite in literature	390
11	Sequences: From numbers to spaces	392

11.1 Subsequences	394
11.2 Convergent Sequences	398
11.3 Completeness	403
11.4 Sequences and subsequences in \mathbb{R}	407
11.5 Application: Circular Billiards	412
Rotations of a Circle	413
Circular pool tables	415
11.6 Additional Problems	417
12 New Numbers from Completed Spaces	418
12.1 Metric Completions	419
12.2 The 10-adic numbers	423
12.3 Constructing \mathbb{R}	427
Axioms	435
Summary of Proof Techniques	438
Typography	444
Bibliography	445
Index	450

Introduction

Number, Space, and the Structures of Mathematics is a gate, an architect, and a docent.

Mathematics offers a wealth of riches for understanding the world. Unfortunately, many of these riches are hidden in fortresses impenetrable by outsiders. Indeed, mathematics' two biggest strengths: formal, precise language and abstraction are also the highest walls surrounding the subject. This text is a gate in those walls.

Mathematics has accumulated a tremendous variety of techniques, concerns, concepts, and methods. These are unified by the common concern of studying Number and Space. This text is the architect who reveals the blueprint exhibiting how the building blocks are assembled in pursuit of a coherent structural vision.

Mathematics is an architectural wonder of the world. It combines skyscrapers and sprawling palatial complexes. Whether meeting prerequisite after prerequisite as you climb the sky scraper of abstraction or curiously exploring room after room of treasure, it helps to have a guide. This text is the docent that gives you your first tour, explaining the underlying structure that governs not just the unity of architectural vision but also the girders that allow us to build strong, flexible mathematical arguments.

Number, Space, and the Structures of Mathematics aims to:

- Increase your ability to absorb new mathematical definitions, understand theorem statements, and construct proofs of those statements using the definitions;
- Provide ample opportunities for writing formal arguments to ensure (to the best of our ability) the intellectual soundness of our arguments;
- Provide a variety of examples demonstrating how formal arguments can be written to ensure the greatest possible understanding in the mind of the reader;
- Use a variety of images and metaphors to convey an informal and intuitive understanding of the topics;
- Give a variety of useful applications showing how mathematics is useful in both science and art;
- Balance mathematics that will or might be encountered later in a students' undergraduate mathematics career (such as in real analysis or abstract algebra) with material that the student might otherwise not encounter.

- Explore sets and operations pertaining to both number systems and geometric/topological spaces;
- Introduce you to important themes of mathematical culture, in particular the particular role of axiom systems and notions of infinity.

We pay particular attention to motivating topics and demonstrating their genuine usefulness. Courses acting as a bridge from introductory calculus to upper-level math courses must convince students that *abstract mathematics is worth studying*. This is true regardless of whether you are more inclined to applied mathematics or to pure mathematics. Some of us find abstraction very difficult. If that's you, I hope that seeing the applicability of the abstractions to (more) concrete ideas is helpful in making the abstract concrete. Others of us may relish abstraction for its own sake. If that's you, I hope that you see how abstraction, in addition to being fun, is a method for understanding aspects of the world. Furthermore, all of us students of mathematics should be able to explain to non-mathematicians why mathematics is worthwhile. Although a single text or a single course will not transform a person into the super-hero of mathematics communication, I hope this text will help you on your journey.

Particular features of this text include:

- specific guides on how to structure the different kinds of proofs.
- an emphasis on modern mathematics, including:
 - references to recent high profile mathematical successes;
 - applications showcasing the relevance of mathematics to computer science, the natural sciences, the arts and humanities;
 - nuanced handling of foundational issues in mathematics, including comparisons of the Zermelo-Fraenkel axioms and category theoretic axioms for set theory;
 - use of topics from more advanced courses, presented at an appropriate level, to demonstrate the relevance of the concepts beyond the current course;
- the use of analogies to explain mathematical topics, including a discussion of the limitations of the analogies;
- proofs of significant results which are left to the reader, as well as outlines of proofs with important steps left to be filled in by the reader
- early introduction of interesting mathematical results. In some cases this necessitates delaying important steps to later in the text. All such interdependencies are carefully noted. This models the way professional mathematicians are willing to delay the proofs of important steps until they have thought through the entire argument.

The emphasis of this text is on writing mathematics. Just as playing a musical instrument enables the player to be a better listener at a concert, so writing mathematics enables students to be better readers of mathematics. Only after we have wrestled with the organization of a proof or the proper order of quantifiers can we understand and appreciate the meticulousness writing of professional mathematicians and technical professionals. Similarly, the act of converting intuition into formal mathematics helps us also develop the ability to convert formal mathematics into intuition. Becoming adept at this is, for most people, many years work, but my hope is that this text provides an excellent starting point.

Finally, in the midst of difficult mathematical work, it can be easy to lose sight of the fact that mathematics is fun, creative, and inventive. My friend Michael Scholz generously provided whimsical illustrations of key ideas. When you see these, be reminded that there are many different ways to conceive of mathematical objects and that we can draw on all of our senses (including our sense of humor!) to understand them. Indeed, I challenge you to find your own original images or stories that embody mathematical ideas.

Who is this book for?

Students who want to develop the ability to read, write, and construct mathematical proofs with a view to developing the mental flexibility, intellectual rigor, and diligence of character necessary to enter into advanced mathematics. On a few occasions, the book uses examples from multivariable calculus, but on the whole the book should be accessible to anyone with some small amount of calculus, computer science, discrete math, or formal logic background. Most students with one year of mathematics, statistics, or computer science at the university level should be amply prepared to use this text.

The text is designed to be very readable; more advice on how to read it is given in the chapter “To Students.” That said, I do assume that there is a teacher to give you feedback on the proofs that you write and that you have someone with whom you can discuss mathematical ideas. The book is designed to be readable and should work well for both lecture-style classrooms and flipped classrooms. My own are a hybrid of the two methods.

Acknowledgements

I am grateful to my undergraduate teaching assistants in the timespan 2014-2017. Conversations with former students and TAs Dan Medici and Allyson Redhunt helped me tremendously in clarifying and refining my approach to the material. Allyson also provided numerous helpful comments on the very first version of this text. Early versions of the book were tested at Bates College, Colby College, and University of California, Long Beach. I thank my colleagues at those institutions for productive conversations. Meredith Greer, Fernando Gouv  a, and Nora Youngs, in particular provided helpful feedback on the text. Thanks to Fernando for suggesting the quotation that opens Chapter 4 and to Keith Barnatchez for the quote that opens Section 10.5. My approach to this material has also been significantly influenced over the years by my research collaborators; especially, Ken Baker, Ryan Blair, Marion Campisi, Jesse Johnson, Maggy Tomova, and Alex Zupan. Bill Thurston’s well-known essay *On proof and progress in mathematics* Thurston has, in my view, not had sufficient impact on mathematical pedagogy. I’ve attempted to draw on some of his ideas in the construction of this book. A grant from the Colby Writing Program and a Colby College research grant helped fund work on this book.

This text is also indebted in its basic organization and content to the “introduction to proofs” books I have either studied or taught from in the past. I would be remiss if I did not particularly mention *Chapter Zero* by Carole Schumacher [110] in this regard. I am not the only one to give proof outlines for the different types of proofs. The book [61] gives similar proof outlines. This book has a similar perspective on writing proofs to [61] and [72]. Those excellent texts develop the basic ideas of logic and proofs and contain a host of introductory examples and exercises. Occasionally, I give brief biographical information for mathematicians. They are mostly drawn from the most excellent MacTutor History of Mathematics Archive [97]. I grateful to all the folks (far too numerous to mention) at stackoverflow for

tremendous help with L^AT_EX, python, and matplotlib.

I am exceedingly grateful to my wife Stephanie and sons George and Milo who have supported my mathematical and academic career immeasurably.

Finally, I am eager to hear from students and instructors. Feel free to email me at scott.taylor (at) colby.edu with comments, questions, and suggestions.

To the student

Mathematics provides a language and a powerful set of tools for precisely describing, modelling, and understanding the physical, conceptual, and aesthetic worlds. It is, of course, the language in which much of the physical sciences are expressed. It also provides tools for modelling environmental, biological, and economic systems. Probability and statistics are mathematical tools for analyzing data, and as such, are the primary tools that scientists (both natural and social) use to demonstrate the trustworthiness of conclusions drawn from experimental data. Mathematics, often via engineering or statistics, also provides useful tools for analyzing artistic works and it provides useful concepts for philosophers to wrestle with. Mathematical revolutions have contributed to artistic revolutions (see, for example, [67]). Even apart from its intrinsic interest, mathematics is worth studying. This text will give you, dear reader, the tools necessary for entering into the world of professional mathematics and numerous examples for why it is worthwhile to do so.

Just as a person cannot claim to be fluent in a foreign language if they have never used the language to convey and understand fresh ideas, so a person cannot claim to be fluent in mathematics if they cannot write and understand mathematical ideas. This text is designed to help you on your road to fluency – but you will not travel far down that road if you do not invest significant time and effort to move yourself along. Many of the theorems in this text are given without proof: **you should provide proofs for yourself**. Of course, how do you know if you've written a correct and understandable proof? Although there are sample proofs throughout the text, the only way to know if you've written a correct and understandable proof is to have someone else read it and give you feedback. Here are some suggestions for how to get the most of out of this text:

- Go slowly. Reading mathematics is different from reading other kinds of writing. Mathematics, through the process of abstraction, conveys a lot of information in very few symbols. You should spend time on each sentence in a paragraph and, sometimes, each word in a sentence. If it is claimed that one sentence follows logically from the previous one – think about it! Does it? Why? If a definition or previous result is referred to, go back and check the definition or the result – is it being used appropriately? have the hypotheses of the theorem been verified? Studies (e.g. [6]) have shown that professional mathematicians read the same material very differently from student mathematicians: experts move slower, refer more to other locations on the page, and spend more time with sentences as opposed to formulas than do students. Work towards becoming an expert.
- Read quickly. If you are feeling bogged down in a particular sentence, read ahead a bit. Try to put the idea you are struggling with into context. Does more explanation come after the sentence you are stuck on? Can you connect the difficult ideas to easier ideas? Often the best way to gain intuition for a new math concept is not to get bogged down in the definition, but rather to focus on

the essential properties of the idea, which are usually contained in examples and theorems coming after the original definition. For example, the definition of “group” is given by a list of axioms, but the best way to understand it is by keeping particular examples of groups (such as the integers, or the group of symmetries of some shape) in mind.

If the previous two pieces of advice seem to conflict, we can only appeal to a dictum of Pascal: “When we read too fast or too slowly, we understand nothing.” (*Penseé* 69)

- Write. It is not enough to simply think through an argument in your head. Write it down carefully. It is easy to convince yourself that you understand something when you don’t. This is especially true if you feel like you have internalized the informal, intuitive sense of a mathematical concept but have not internalized or used the formal definition or statement. The informal, intuitive senses of mathematical concepts are only approximations to the precise formulation. That’s why mathematics holds surprises – things are not always as they seem! Most of the theorems in this book do not have complete proofs given - that’s your job! Be sure to take the time to work on understanding how each proof should be structured, developing the key mathematical ideas, and then writing them down as clearly as possible.
- Rewrite. Mathematical writing, although it is more condensed and may contain equations and formulas, is still writing. And good writing almost always starts out as less-good writing. After you have written a mathematical argument, re-read it. How can you rewrite it to make the argument clearer? to reduce unnecessary steps? to make it better organized? Good writers write for their readers, not for themselves. In the past, perhaps, you’ve been used to writing mathematics so that your instructor can verify that you understand it. Now is the time to write so that others can understand and either verify or dispute your arguments and conclusions. It is not enough that you understand what you have written, a reader *who is not as mathematically advanced as yourself* must also be able to understand what you have written. It is normal to write *several* drafts of a proof, before settling on the one that you will show other people.
- Draw pictures. Rarely is a picture a substitute for a carefully written definition, theorem, or proof. However, pictures are very useful for developing an intuition for what formal mathematics encapsulates. Including pictures in your proofs, again while no substitute for careful writing, aids the reader in understanding the essence of the argument. When you encounter a new mathematical concept, try to draw a picture, perhaps schematic, of it. Better yet, attempt to draw several very different ones. When you encounter a picture used in a proof that someone else has written attempt to draw a different one - does their argument still apply? When you are rereading a proof you have written, ask yourself if including a picture will assist the reader in understanding what you have written. This especially true if you introduce a lot of notation - a single picture showing all the notation is an exceedingly useful mental crutch for the reader.
- Work with others. Find one or two other people with whom you can share your proofs or ideas for proofs. Have them read what you write and ask them for detailed, constructive feedback. Being told either “It’s awesome!” or “It sucks!” isn’t useful. If the person you’re working with only gives feedback of that sort, find someone else. Conversely, find one or two people who are willing to share their proofs with you. You should only read their proofs after you’ve thought about the problem and attempted your own solution though! Give them detailed constructive feedback. Where do they express an idea particularly clearly? Where do they make an illegitimate logical leap? Where do they misapply a definition? Where are they too vague? Where would a picture help their proof?

- Listen. As you work with others, be sure to both share your own ideas and to listen carefully to those of others. Even if someone is saying something you think is obvious, listen to them. First of all, you never know if you've thought of everything and there are often multiple approaches to a particular problem. Secondly, it builds the other person up and helps them develop the confidence to become an independent mathematician. The more mathematicians there are, the more people there are who are capable of appreciating your mathematical ideas. Thirdly, you can learn not just from what someone is saying, but from how they say it. Do they find part of an argument easy when you found it hard? Why? Do they find part of an argument hard when you find it easy? Why? People come into mathematics from many different backgrounds. By discussing mathematical ideas with those from different backgrounds you learn not just more math but also more about what it means to be human.
- Embrace hard work. Many of the theorems and exercises in this book have solutions that can be found online and those that aren't currently there can easily be put there. But using a stranger's solution (which might not even be right!) won't help you learn how to prove theorems yourself. You can easily spend an hour looking for a correct solution online - but wouldn't it be better to spend that hour thinking about the right way to organize your proof, reviewing the relevant definitions, and looking for similar theorems that were proved in class or in the text?
- Give generous credit. All of us make use of the work of others. Maybe someone gave us an idea for how to prove a theorem. Maybe someone told us what they tried that didn't work. Maybe someone simply provided a listening ear. Whoever it is, give them credit. Maybe it's your classmate or TA or maybe it was someone with the moniker "AwesomeMathPerson27" on the internet. Whoever it was, give them credit. It makes you into a better person, it encourages the other person, and it contributes to making mathematics a positive, welcoming community of truth-seekers.
- If you despair, journey on! Mathematics is difficult. Anyone who doesn't find it difficult hasn't done it long enough. When you are totally stuck on a problem, use it as an opportunity to learn humility, appreciate that there is more to the world than you can understand at the moment, and to acknowledge that you are a human being who needs other humans. When you grasp a concept easily and it seems like second nature, ask yourself if you are making it too easy or have overlooked something. Maybe you haven't! In which case, ask yourself how you can use your newfound knowledge to help others learn and appreciate mathematics better.

When others seem to grasp ideas more quickly than you do, keep in mind that any of the following might be true:

1. They don't actually understand things as much as they think they do. Sometimes the loudest people are the most wrong.
2. They have a more mathematically-oriented background than you do. In which case, there's no additional glory for them in simply making use of things they already knew or skills they already have. It's fine if you have spent less time doing mathematics than someone else. The purpose of this text is to give you more opportunities to do mathematics!
3. They are brilliant. This is also fine. Not everyone has to be brilliant and not every mathematician has to be brilliant. Do your best to learn from such a person. If they have a hard time communicating with you in a way you can understand, see (1). There are many roads to becoming a mathematician. You're taking a different road - that's good and it makes the mathematical community a more interesting one to be a part of.

- Encourage others. Mathematical terminology can be used to help convey ideas efficiently or to intimidate others. Be the sort of mathematician who uses understanding and knowledge to contribute positively to the community. How easily someone grasps mathematical ideas has nothing to do with their worth as a person. There is more worth in striving and failing to understand a mathematical concept than there is in readily grasping it and using it to bully others.

To the teacher

In the past several decades, “Introduction to Proof” courses have become standard fare at most colleges and universities and a veritable host of textbooks have risen up to help teachers and students with this course. With those texts comes increasing (though by no means universal) agreement on what mathematical topics should appear in such courses. This book incorporates most of those topics:

- elementary logic
- sets and set arithmetic
- proof techniques
- equivalence relations
- functions
- cardinality
- introductory material from more advanced classes such as graph theory, abstract algebra, and real analysis.

The challenge for courses of this sort is to not simply rattle off a laundry list of topics a beginning math major should “know”, but also to tie those topics together into a well-motivated coherent and stimulating whole¹. Here is how this book does that:

- **Emphasis on writing.** Students are given many models of well-written proofs, many theorems whose proofs are only outlined, and many theorems whose proofs need to be constructed from scratch. Beginning mathematics students need good models for how to organize a proof and, especially how to juggle the complicated statements from analysis (in particular). Especially early on, the reader is asked to make minor modifications to a given proof. Proofs that I judge to be beyond the status of a difficult homework problem are provided, as are proofs that do not contribute to the main thrust of the text. Some hints or partial solutions for particularly challenging proofs are given. The proofs left for the reader are not simply busy-work, but are essential for learning to write mathematics that is relevant to all future math classes. In addition to the proofs left to the reader, the text also includes a plethora of examples and exercises. The exercises require more work to complete than the examples, but less work than proving the theorems. Some of the exercises are more open-ended, providing an opportunity for considering why certain choices, and not

¹As with set theory, perhaps this another instantiation of the philosophical problem of “the many and the one.”

other choices, are made in definitions or writing style. Quickly internalizing the basic framework of particular kinds of proofs is essential for freeing up the mental and emotional spaces needed for wrestling with the *ideas* in the proofs. As befits the title, particular attention is paid to the structure of mathematical proofs. For each of the typical proof forms, I provide an outline which students are intended to follow when writing their own proofs. Taking the burden off the organization of the proof lets students focus on the act of deciding what kind of proof to write, constructing it, and polishing their write-ups.

- **Creative motivation.** The exposition motivates concepts and helping the reader gain intuition using a wide variety of examples, analogies, and metaphors. Each mathematical idea is situated in the context of mathematics as a discipline and explicit connections to more advanced mathematics classes are included. Whenever possible, examples from modern mathematical achievements are highlighted and used as the basis for exercises. Material from more advanced courses is woven throughout the text, with the connection to the material at hand explained and emphasized.
- **Number and Space are unifying themes.** Almost all concepts are illustrated with both geometric and number (both integer and real) examples. Since Euclid, mathematicians have developed an astonishing variety of number systems and spaces. One of the auxilliary goals of this text is to give students a flavor of the immense creativity and freedom that allow the creation and discovery of genuinely new mathematical ideas. In particular, new number systems give rise to new spaces and new spaces give rise to new number systems. The final chapter give some idea how this can be done. Chapter 12 shows how spaces (namely, metric spaces) can be completed to fill in “missing points.” Applying this construction to the rationals using a certain non-standard distance function creates the p -adic numbers. A very careful application to the rationals using the standard (euclidean) distance function creates the reals. That final chapter brings together concepts on equivalence relations, sequences, and cardinality.

Throughout the book, I have tried to highlight proofs that involve geometric ideas. There are two chief reasons for this. The primary reason is my perception that students entering into a math major have had little experience with geometric modes of thought (as compared to algebraic or analytic modes.) Many students delight in the ability to bring geometric thinking to algebra and analysis; this text provides a foundation for them to do so. Secondarily, metric spaces are a wonderful context for bringing together combinatorial, analytic, and algebraic reasoning.

- **Applications are highlighted.** Mathematics students at all levels want to be convinced that mathematics is worth doing. Certainly, its intrinsic beauty and elegance make the study of mathematics worthwhile. Highlighting the wide applicability of mathematics to other disciplines, both scientific and humanistic, is another key way to motivate its study. For each major concept in the text, I have included several “applications.” The tricky thing about applications, however, is that deep understanding of them requires both deep understanding of mathematics *and* deep understanding of the domain discipline to which the mathematics is being applied. At least as much time can be spent in learning biology, philosophy, chemistry, art, physics, and religion, etc. as can be spent in learning the relevant mathematics. The applications in this text, then, are of necessity presented in a rather shallow fashion. The goal is to show that mathematics beyond calculus is useful in a wide variety of contexts, and, furthermore, knowing mathematics may enable one to make genuinely new contributions to other fields. Although I have taken a minimalist approach to explaining each application, the applications themselves are genuine and references to deeper expositions are provided. In the context of a course, these applications make a good basis for projects.
- **Sophisticated connections to advanced mathematics.** University students early in their edu-

tion are absolutely capable of sophisticated reasoning about mathematical concepts. This book aims to help them develop those reasoning powers in ways that are authentically connected to more advanced mathematics courses in graph theory, topology, geometry, analysis, and probability. The book genuinely transitions students from a place where mathematics may be mostly about calculations to a place where mathematics is about creative ideas carefully expressed. Apart from the final chapter, the book does not go into tremendous depth on any of these topics, but it does motivate them and interweave introductory material in a way that motivates and situates the material at hand.

- **Sophisticated looks at elementary mathematics.** Using the historical concern with mathematical foundations as a guide, we show how set theory and equivalence relations can be used to develop elementary topics such as the natural numbers, rationals, and angle measurements in a way that shows that the long familiarity of those topics engendered by their early introduction obscures ideas of surprising depth and utility.

The book includes incorporates the following pedagogical features:

- **Proof structures.** These outlines explicitly indicate how certain kinds of proofs (proof by contradiction, induction, etc.) are usually structured. Relieving the mental burden of how to organize a proof or what exactly is required to demonstrate a certain statement is true, allows the student to focus on mathematical ideas. These proof structures also build student confidence, by inculcating in them the language of formal mathematics.
- **Proof outlines.** Many of the more sophisticated proofs are given in outline form, with key steps left to the reader. These allow students to begin working on a proof *before* coming to class, removing the “I have no idea how to start” obstruction.
- **Multiple proofs of the same theorem.** In order to emphasize that mathematics is about ideas and communication, several important theorems are proved in more than one way. Students are then asked to reflect on the advantages and disadvantages of each proof.
- **Close attention to the language of mathematics.** Drawing on recent research on the differences between the use of mathematical concepts and natural language uses (such as “if … then”), the book includes explicit discussion of the similarities and differences between how humans use the same language in multiple ways in different contexts.
- **Spiraling content.** Important advanced mathematical ideas (e.g., number systems, graphs, groups, event spaces) are introduced early and then revisited several times, each time with greater depth, as the text continues. This means that it is okay for students to feel like they do not completely understand a topic before moving on; it will be revisited later at which point students have a greater understanding of the context and importance of the idea.
- **An emphasis on understanding through usage.** Students are asked to work with mathematical ideas in interesting ways early on, but with tremendous guidance. For instance, shortly after the introduction of the definition of set intersection, students are asked to prove that the intersection of an arbitrary number of convex sets is convex. By actually using the formal definition to prove an interesting result, students must learn to rely on the definition rather than on pure intuition. When combined with the explicit given proof structures, this builds in students the confidence and capability for handling tasks that professional mathematicians consider “routine.” In many cases, these ideas are applied in more than one context, and so students develop a strong understanding of the underlying principles.

- **An emphasis on visualization.** All topics are illustrated, visually or metaphorically, in ways that make the essential idea visceral. Particular attention is paid to the visualization of functions, since broadening students' conception of what a function is, is a key goal of the course.
- **An intentional development of intellectual flexibility.** When they are confronted with a new mathematical idea, math students should embrace it with eagerness, confidence, and aplomb. I seek to help students develop these virtues by presenting numerous new mathematical concepts, organized around the themes of number and space. The first steps with any new mathematical idea should be to figure out what can be done with it using only known tools. To that end, early in the text there are a number of examples of results concerning advanced concepts which use only basic set theoretic or logical arguments. As will be the case when students move on to more advanced texts, students will encounter numerous new definitions. Students should not be expected to memorize and remember all of them; rather they are intended to become comfortable facing new definitions. Crucial definitions are listed at the start of each chapter; the other concepts are intended to act as illustrations of the essential ideas.
- **An emphasis on equivalence relations.** Equivalence relations explicitly play a key role in more advanced math classes (such as algebra, analysis, and topology) and implicitly play a key role in others (such as linear algebra and differential equations). Yet, they are often de-emphasized in introductory proof-writing textbooks. Making them more central provides useful context for the study of functions. In particular, defining functions on quotient sets is an opportunity to deeply explore the notion of a function being "well-defined." They also provide an ideal setting for practicing basic set theoretic proof techniques in a more abstract setting. Finally, they provide a unifying theme for the latter half of the book, by allowing us to construct interesting examples of numbers and spaces.
- **An emphasis on the actual usage of induction arguments.** Unfortunately, many students in "introduction to proofs" courses only encounter induction arguments where it is obvious what the quantity to be inducted on should be and where the inductive step has a sense of inevitability. Drawing on examples from graph theory and geometry, we present students with more significant induction proofs, as well as a discussion of the conceptual basis underlying them.
- **A studied comparison of finite and infinite cardinalities.** Many "obvious" results concerning the cardinalities of finite sets are strikingly challenging to prove. The advantage of addressing them is that it balances the novelty of infinite cardinalities with the dawning recognition that there is awe and wonder to be found even in situations we think we know well. The striking conceptual shift needed for discussing cardinality is handled by addressing properties, both elementary and advanced, of injections and surjections prior to the introduction of cardinality.
- **A balanced approach to advanced set theory.** Any author introducing set theory for beginning math students must decide how foundational issues will be handled. The ZFC axioms for set theory are impenetrable unless one already has a good feeling for what one "should" be able to do with sets and why fastidiousness is a virtue in set theory. A more modern approach to foundational issues is to use the axioms from the "Elementary Theory of the Category of Sets" (ETCS) arising out of Category Theory. The most important of these axioms have the virtue of giving primacy to *functions* rather than *elements*; however many standard proofs (such as element arguments) in beginning mathematics unfortunately become convoluted when appealing to first principles. The approach taken in this text is to first introduce the basic constructions of sets that most mathematicians consider a necessity (complements, unions, intersections, power sets, Cartesian products) and then to briefly discuss both the ZFC and ETCS axiomatic approaches. More attention is

paid to ZFC due to its historical importance and widespread acceptance in the mathematical community. However, the book is structured so that discussion of foundational issues can be almost entirely avoided, if desired.

A book is defined not only by what it includes, but what it leaves out. Notable topics excluded from this text are partial orders, ordinal numbers, and many standard topics of discrete mathematics and graph theory. I also wish it were possible to include more examples from recreational mathematics. I can only apologize by way of admitting that the text already includes more material than can be fit into a single semester and hoping that there is enough flexibility in the presentation that instructors can find ways substituting their favorite topics in place of something they are less attracted to.

Pre-requisites:

The most natural audience for this text are students who have studied some multivariable calculus. Students who have studied some university level mathematics, computer science, statistics, or philosophy should find most of the book useful and accessible. Although explicit examples from calculus appear very rarely in the text, readers who have encountered sequences of real numbers, the plane \mathbb{R}^2 , and real-valued functions on \mathbb{R}^2 will find many of the examples and motivations more accessible than those who have not. No linear algebra is assumed in the text, though it is referred to on a very few occasions. There is, of course, ample opportunity for an instructor to make connections between the general discussion of injective and surjective functions in this text with the way those concepts arise in linear algebra.

Advice for teaching from this book:

The text certainly contains more material than should be fit into a single semester. I highly recommend that students be assigned to read portions of the text covering material which will not be discussed in class. The ability to independently learn and read mathematics is an essential skill for mathematicians of all kinds; bridge courses should help transition students to independence. Class time can be spent either discussing ideas students have a harder time learning on their own or having the students practice devising and writing proofs of theorems in the book.

In the internet age, ensuring that students complete work with a robust sense academic integrity is increasingly difficult and important. Many of the theorems in this book have proofs available online and if they are not already there, it is easy enough for a student to get someone else to put them there. I recommend supplementing textbook problems with problems custom written for your course as a way to mitigate the issue. Above all, I encourage you to have a frank discussion with students about appropriate and inappropriate uses of the internet, the purpose of assignments, and the value, necessity, and methods for giving other credit. Students should always be required to acknowledge collaborators and the use of internet (or other) sources.

Chapters 1 - 5 should be covered in order, though instructors are encouraged to emphasize and omit topics as appropriate for their students' interests and future mathematical work. Groups, graphs, and metric spaces are used as examples throughout the text and those concepts should not be omitted from Chapter 2. Chapter 6 can be skipped or covered very briefly either in class or with independent reading. Chapters 7 - 9 should also be covered in order, although there are numerous opportunities for abbreviating or cutting material. Each of those chapters include material that bring together material from Chapters 1 -

5. Chapter 10 is traditional material for a transition to higher mathematics course and should probably be covered, though much material may be omitted or relegated to independent reading. The early parts of Chapter 11 discuss subsequences; the later parts give an introduction to basic concepts from analysis. All of Chapter 11 is required for Chapter 12. I have had success in using the underlying ideas from Chapter 12 as a fun final class day topic, which I do not assess the students on.

Here is a general outline of how I teach my course from this book. As mentioned previously, I do not cover all the material in the textbook (or even all the material from any one chapter). Students have their first encounter with new material before coming to class and are required to at least begin working on assigned problems prior to class. My classes meet 3 times/week for 50 minutes each time.

- (Weeks 1, 2:) Chapters 1 and 2. Introduce students to the course using an accessible problem based on material that shows up later in the course (for instance circular billiards). I also show them \LaTeX and explain course policies. Break students into small groups to work on projects. Projects are designed to introduce the idea of number systems, graphs, or groups. Each project takes one class period, plus a small amount of out-of-class work. They hint at ideas of modular arithmetic, sequences, or equivalence relations. Projects are graded on a credit/no-credit basis, with lots of comments. The goal is to get students working together and to introduce themes that will show up repeatedly as the semester continues. Students work on Chapter 1 out-of-class with a small amount of in-class discussion if needed. Exercise 1.3.15 usually requires in-class discussion.
- (Week 3:) Chapters 2 -3. A small amount of class time is devoted to finishing up material from Chapter 2 that was not covered by the projects. We then rapidly cover sections 3.1 - 3.6, mostly by independent reading. Class time is primarily spent working on negations, which students tend to find very challenging.
- (Week 4:) Chapters 3 - 4. Sections 3.7, 3.8 are covered by lecture in class. Chapter 4 is covered primarily by independent reading, though we discuss in-class the proofs of theorems of classical importance.
- (Week 5:) Chapter 4 -5. If needed a small amount of time is devoted to finishing Chapter 4, but most of the time is spent on Chapter 5. Most of our time is spent on Sections 5.3 (Intersections) and 5.4 (unions). As we cover these corresponding material from Section 5.7 is integrated.
- (Week 6:) Chapter 5 - 6. We continue with Chapter 5, mostly the latter half of the chapter. One day is spent on either Section 5.8 or 5.9. I usually give an exam about now and the day after the exam spend one day on Chapter 6. I generally do not assess students on Chapter 6.
- (Week 7:) Chapter 7. Class time is spent working on problems. Students encountered the main ideas in their reading before class. Section 7.5 is the important one here.
- (Week 8:) Chapters 7 - 8. Finish up Chapter 7 as needed and move on to Chapter 8. Class time is spent on Sections 8.4 - 8.7. I usually do not cover algebraic and metric structures. I do usually cover Section 8.9, since it introduces permutations.
- (Week 9:) Chapters 8 - 9. Section 9.1 is covered fairly rapidly, with the focus being on the geometric examples of induction. Students need a lot of practice simply writing inductive assumptions and tasks. A lot of time is spent on Section 9.2. I usually give an exam in here too.
- (Week 10:) Chapter 9, focusing on Sections 9.3 and 9.4. Sometimes I cover Section 11.1 at this time as well.

- (Week 11:) Chapter 10. Usually, I cover this chapter in a somewhat reduced way, as students are working on individual projects or writing assignments. I often end the course by covering Lagrange's theorem from group theory since it is a nice example of how to use bijections for counting purposes and has applications to symmetry. Typically, I cover Sections 10.2 - 10.4 and 10.10 with care and leave the others for independent reading or inspirational final lectures.
- (Week 12:) Continue with Chapter 10, as needed. I sometimes hit some topics from Chapter 11. If I am able to cover significant parts of Chapter 11, I end the course with a one day lecture on how to create the reals and 10-adics using equivalence classes of sequences. Ending the course by investigating applications encountered earlier in the semester also works well.

1 | Sets

“On your mark, get set … go!”

Key Terms

- informal definitions of element and set.
- important examples of sets, including the empty set.
- formal definition of subset and proper subset
- uniqueness

Sets and functions are the fundamental structures of mathematics. We begin by studying sets. As we shall see, although humans have very good intuition for how sets with finitely many elements behave, our intuition for infinite sets is less good (possibly even terrible!) One of the purposes of formal mathematics is to reduce dependence on intuition so that we can be more confident in the conclusions we draw. A related purpose is to develop our intuition by increasing its sophistication and ensuring its connection to underlying truths. However, most of us require some time to get used to the formality and logical structure of modern mathematics. To help the transition be as painless as possible, this chapter introduces sets at a level that is likely between the informality used in prior math classes and the strict formality required later in the text. Chapter 6 discusses a more formal approach to set theory.

1.0.1

Warning

You should think of this chapter as the mathematical equivalent of the first week of French horn lessons. In the first week of horn lessons, you are given an instrument, taught the correct posture and breathing techniques, and then encouraged to make some awful noises. Over time, with lots of practice and good advice from a teacher, those initial honks, sputters, and blats are transformed into beautiful music.

In this chapter you are asked to begin writing proofs – but, chances are, you don't yet know how! Pay attention to the examples, try to follow the given advice, do your best, and get feedback on your progress. Periodically return to what you've written and ask yourself how you might improve it.

1.0.2

Warning

Oh yes, since this chapter is where you begin writing proofs, the expectations for what constitutes a clear and correct proof are lower than in later chapters. Put another way, maybe you can get away with a faulty proof now, but be prepared for expectations to increase as the text goes on!

Duly warned, let's jump right in.

1.1 Sets, informally

“We always have some kind of naive picture for things we are trying to describe by mathematical formalism. But the naive picture usually does not match up perfectly with the precise formalism. There is a gap between the two. We try to get them as close together as we can. That is one of the struggles that moves mathematics forward.”

-Lawvere¹ and Rosebrugh

The notion of set is a useful way of taking a “many” and thinking of it as a “one”².

1.1.1

Definition ▶ Set and Set Equality (Informal)

A **set** is a collection of **elements**. We write $a \in A$ to mean that a is an element of the set A . A set A is **equal to** a set B if and only if every element of A is also an element of B and every element of B is also an element of A . If A and B are sets that are not equal, we write $A \neq B$.



Figure 1.1: We often think of a set as a bag containing items, some or all of which might be other bags.

Our informal definition is less than satisfactory as we do not have a definition of “collection”. Nevertheless, we can do a lot with this imperfect definition. We often think of a set as being a bag and the things in the bag are its elements. Sometimes there is one bag inside another bag as might have been the case just before the larger bag spilled as in Figure 1.1. As we will see, however, this intuition for what a set is has its limitations, both mathematically and conceptually. There will always be some incongruity between an informal approach and a formal approach.

¹William Lawvere (b. 1937) is the creator of the ETCS axiom system for set theory. We'll discuss this again in Chapter 6. The quotation is from [84, Section 2.1]

²Or as with the United States of America: *E pluribus unum*. This conception of a set is due to the 19th century mathematician Georg Cantor whose ideas will feature prominently in this book.

Sometimes we want to indicate what the elements of a set are. We can do that in several ways:

1.1.2 We can list the elements of the set between curly braces: { and }. For example, the elements of the set {1, 7, 10} are the numbers 1, 7, and 10.

1.1.3 We can use an unspecified variable in curly braces to indicate an arbitrary element of the set and then specify a condition (called the **entrance criterion**) that an element must satisfy to belong to the set. For example,

$$\{a : a > 0\}$$

is the set of positive numbers. The entrance condition is $a > 0$. We read this as “the set of a such that a is greater than zero.” In general, a set contains every element which passes the entrance criterion and only those elements which pass the entrance criterion.

1.1.4 We can list representative elements of the set between curly braces and indicate that the list is not complete. For example, the elements of the set {2, 4, 6, 8, ...} are all the even natural numbers.

None of these three methods of writing sets is without issues. The first method only works when we can write down every element of the set – so it only works for sets with a finite (and relatively small!) number of elements. The second example is problematic since in mathematics we often are interested in sets of elements that are not numbers. In which case simply writing the variable a doesn’t help the reader know what kind of object a is. The third method has the issue that it may not be clear what the pattern is. Finally, all of these methods share another issue: *Simply writing items between curly braces does not imply that it is a set in the mathematical sense.* Indeed, we will see that $\{A : A \text{ is a set.}\}$ is not itself a set. Before we address these issues, however, we take a look at some sets, you’ve likely encountered before.

1.1.5 The set of **natural numbers** is the set of counting numbers. We denote it using the letter “N” in the “black-board bold” typeface.

$$\mathbb{N} = \{1, 2, 3, 4, 5, 6, 7, 8, \dots\}.$$

(See the [Typography](#) appendix at the end of the book for a list of various symbols, typefaces, letters, and fonts you may not have encountered before.)

1.1.6

Warning ▶ Objects vs. Representations

It is tempting to take the symbols

$$\mathbb{N} = \{1, 2, 3, 4, 5, 6, 7, 8, \dots\}.$$

as the *definition* of the natural numbers. Doing so, however, misses the distinction between what a number *is* and how we *represent* it. We could equally well use Roman numerals to represent natural numbers:

$$\mathbb{N} = \{I, II, III, IV, V, VI, VII, VIII, \dots\}.$$

Or we could use English words to represent the numbers:

$$\mathbb{N} = \{\text{one, two, three, four, five, six, seven, eight, \dots}\}.$$

These are just three different ways of representing the same set.

The warning raises a question: If the natural numbers aren't defined by what they look like, what are they defined by? We'll take this question up in the next chapter when we discuss "sets with structure." For now, we'll continue with the working understanding of the natural numbers you've developed over the course of your previous mathematics education.

Some mathematicians include 0 in the set of natural numbers. We, however, will let \mathbb{N}^* (pronounced "N-star") denote this set and will call it the set of **extended naturals**. That is,

$$\mathbb{N}^* = \{0, 1, 2, 3, 4, \dots\}.$$

1.1.7

The **integers** are the set of positive and negative whole numbers and zero. We denote it:

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}.$$

1.1.8

The **rationals** are the set of fractions of integers, forbidding 0 from the denominator. We denote it:

$$\mathbb{Q} = \{a/b : a \in \mathbb{Z} \text{ and } b \in \mathbb{N}\}.$$

1.1.9

The **real numbers** \mathbb{R} are all the numbers on the number line. They have several more-or-less equivalent definitions, all too advanced to be given at present. We recall, however, that every real number has a decimal representation. Rational numbers have decimal representations which are eventually periodic: that is the same string of digits is repeated forever. In our notation, we place a line over the repeating digits. If the repeating digits are all 0, we usually omit them. For example,

$$\begin{aligned} 721/495 &= 1.45656\overline{56} \\ 3/5 &= .600000\overline{0} = .6 \end{aligned}$$

The decimal representation of an **irrational number** (that is a real number which is not rational) is not eventually periodic. Some rational numbers have two distinct decimal representations: one that ends in all 0s and one that ends in all 9s.

So for example:

$$\begin{array}{rcl} 1 & = & .99999\bar{9} \\ 2.4 & = & 2.39999\bar{9} \end{array}$$

and so forth. But this is the only situation in which a real number has two distinct decimal representations. Making the notion of “decimal representation” precise and proving (for example) that $1 = .\bar{9}$ is best done using the machinery of infinite series, which you likely studied in Calculus.

- 1.1.10 The **complex numbers** are the set:

$$\mathbb{C} = \{x + yi : x \text{ and } y \text{ are real numbers and } i^2 = -1\}.$$

The complex numbers will not feature heavily in this text, but they are extremely important in mathematics. Complex numbers can be added, subtracted, multiplied and divided (as long as we don’t divide by $0 + 0i$).

- 1.1.11 The **Cartesian plane** is the set:

$$\mathbb{R}^2 = \{(x, y) : x, y \in \mathbb{R}\}$$

These are ordered pairs of real numbers. Recall that $(a, b) = (c, d)$ if and only if $a = c$ and $b = d$. There is a natural correspondence between the Cartesian plane and the set of complex numbers obtained by associating the complex number $x + yi$ with the point $(x, y) \in \mathbb{R}^2$. Indeed, there is a sense in which the set of complex numbers *is* the Cartesian plane just with a particular way of doing arithmetic.

- 1.1.12 **Cartesian n -dimensional space** is the set:

$$\mathbb{R}^n = \{(x_1, x_2, \dots, x_n) : x_1, x_2, \dots, x_n \in \mathbb{R}\}$$

As with the Cartesian plane, we have

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

if and only if $x_1 = y_1, x_2 = y_2, \dots$, and so forth.

- 1.1.13 The **empty set** \emptyset is the set with no elements.

1.1.14 Exercise

Identify ways in which the preceding sets are not precisely defined and take a stab at attempting to give more precise definitions. Also, discuss different ways of representing the elements of each set (similar to what we did for the natural numbers).

We conclude with an example of how the bag metaphor for sets breaks down.

1.1.15 Warning

Mathematical objects behave differently from physical objects.

Consider the backpack and lunch bag of Figure 1.1. In everyday life, if the lunch bag contains an apple and if the lunch bag is contained in the backpack we would say that the apple is also in the backpack. However, in math we would *not* say that the apple is an element of the backpack. To continue the bag metaphor, we should think of the phrase “ x is an element of X ” as meaning “ x is loose inside X .” Thus, to say “the apple is an element of the backpack” means that the apple is loose inside the backpack. Returning to mathematics, let $X = \{1, 2, 3, \{4, 5\}\}$; this is analogous to the backpack. The set $A = \{4, 5\}$ is analogous to the lunch bag. We can write $A \in X$ since the lunch bag is loose inside the backpack. We can write $3 \in X$, since 3 is also loose inside the backpack. We cannot, however, write $4 \in X$, since 4 is not loose inside the backpack. It is loose inside the lunch bag, so we can write $4 \in A$.

Now consider the case when $X = \{1, 2, 3, \{3, 4\}\}$ is the backpack and $A = \{3, 4\}$ is the lunch bag. Again, $A \in X$. We also have $3 \in X$ and $3 \in A$ since 3 is loose inside X and 3 is also loose inside A . At this point, the metaphor of backpacks and lunch bags has broken down. For if there is an apple loose inside the lunch bag it is physically impossible for the very same apple to be loose inside the lunch bag, so we could not say that the apple is an element of the lunch bag and also that the apple is an element of the backpack. This thought experiment shows us that sets are better models for ways of organizing abstract concepts than they are models for the organization of physical objects. Nevertheless, sets are extremely useful in both theoretical and applied mathematics.

1.2 Proving set membership

“There is only one empty set, and it exists around the world,
the set of loyal lovers and living
unicorns, honest politicians

and the contents of the intersection of
any two non-intersecting
circles. Sets are aggregates of things,
to be divided and united.”

– Bonnie Jo Campbell, *Set Theory* [24]

One of the most basic tasks in mathematics is to show that certain elements belong to certain sets. In this section, we will look at some very simple examples, each of which is a simple rephrasing of the sort of math you would have done before college. As you read, focus on the overall structure of the proof. Ask yourself: How does the way the solution is written differ from the way I would naturally answer it? What advantages and disadvantages does this new way of writing have?

As you’ll see, in the proofs, we do rely on elementary arithmetic and algebra. Although you’ve known how to do this for a long time, you have likely never seen

a proof that basic algebra and arithmetic operations are valid. By the end of this text, you will have the essential ideas for how to construct such proofs. For now, however, we will (unless otherwise indicated) assume that the basic arithmetic of integers and rational numbers is valid. We will sometimes make use of more sophisticated properties (such as the existence and uniqueness of prime factorizations or that real numbers have decimal expansions), but if possible we prefer to not have to appeal to those. In Chapter 3, we'll elaborate on the logic underlying the proofs in this first chapter. We focus on just two examples, but more are given in Section 1.7.

1.2.1

Warning

If you are ever unsure as to whether a particular fact or operation from your previous mathematical education is usable in a particular proof, it is better to list it as an unproven assumption than to simply hope that no one notices that you've used it without proof!

1.2.2

Example

Let X be the set whose elements are the real numbers that are solutions to the equation $x - \sqrt{x} = 2$. Prove that every element of X is also an element of the set $\{1, 4\}$.

We are asked to prove that every element of X is either 1 or 4. We will write our argument so that it pertains to any one of the elements of X , chosen without prejudice. Applying our argument to each element of X individually, allows us to conclude that the statement is true for *every* element of X . Since we write the argument out for only a single element x in X , but want to indicate that it applies to every element of X , we say that the element x is “arbitrary” or “fixed, but unspecified.”

Also observe that we are not (at this point) showing that 1 or 4 are themselves elements of X . (In fact, $1 \notin X$. Do you see why?)

Proof. Let x be an arbitrary element of X . We must show that x is either 1 or 4. By the definition of X , x is a real number and

$$x - \sqrt{x} = 2.$$

Define t to be the real number \sqrt{x} . That is, let $t = \sqrt{x}$. We can then rewrite our equation as:

$$t^2 - t - 2 = 0$$

Applying the quadratic formula, we see that $t = -1$ or $t = 2$. Since $x = t^2$, we see that $x = 1$ or $x = 4$, as desired. □

Here is a summary of how to organize a proof that every element of a set has a particular property. A little later we'll see a more general version of this argument.

ELEMENT ARGUMENT VERSION 1

To show: Every element x of a set X has a particular property.

Structure of Proof:

Assume $x \in X$ is arbitrary.

(*Do a bunch of work to show x has the desired property.*)

Hence, x has the desired property. Since x was arbitrary, every element of X has the desired property. \square

As we remarked earlier, in the proof in Example 1.2.2 we have *not* shown that 1 and 4 are themselves elements of X . In fact, hypothetically, X may not have any elements at all. We only showed that *if* some $x \in X$ *then* it is either 1 or 4. By way of analogy, our claim and proof are analogous to a friend saying:

"I'm not sure if Uriah Heep and Mr. Wickfield are in the office or not, but whoever is in the office, if anybody, is Uriah Heep or Mr. Wickfield."

Observe that, in this context, the statement "If somebody is in the office, then that person is Uriah Heep or Mr. Wickfield" would be a true statement if no one is in the office or if just Uriah Heep or Mr. Wickfield were in the office, or even if both of them were in the office. If three different people were in the office, however, it would not be a true statement since at least one of them wouldn't be Uriah Heep or Mr. Wickfield.

When we claim that every element $x \in X$ has a particular property, we are *not* claiming that X has any elements. If X has no elements (i.e. is the empty set) then we say that the property is **vacuously true** for elements of X . For example, let X be the set of all integers n such that $0 < n < 1$. Although it's slightly counterintuitive, we would affirm that for every $n \in X$, the number n is a multiple of 29. We would also affirm that for every $n \in X$, n is negative and that for every $n \in X$, n is positive. These statements, indeed all statements you might care to make about elements of X , are all *true* statements; however, there is nothing to apply those true statements to, since X does not have any elements.

1.2.3

Definition ▶ Vacuously True

Statements of the form:

"For all $x \in \emptyset$, ⟨ *some statement about x* ⟩"

or

"If ⟨ *a false statement* ⟩ then ⟨ *any statement whatsoever* ⟩."

are said to be **vacuously true**. That is, they are true statements, but they have no interesting content.

We will elaborate more on why we consider vacuously true statements to be true

in Chapter 3.

1.2.4 Example

Consider the statement:

“For every natural number $n \in \mathbb{N}$ such that $n^2 < 0$, we have $n > 0$.”

This is equivalent to the statement:

If $n \in \mathbb{N}$ has the property that $n^2 < 0$, then $n < 0$.

The first statement is vacuously true since the set $\{n \in \mathbb{N} : n^2 < 0\}$ is the empty set. The second statement is vacuously true since the statement “ $n \in \mathbb{N}$ has the property that $n^2 < 0$ ” is a false statement, no matter what n is.

1.2.5 Example

Consider the statement:

“Every square with width greater than length is a triangle.”

This statement is vacuously true since (by the definition of “square”) there is *no* square with width greater than length. Similarly, the statement

“If S is a square with width greater than length, then S is a triangle.”

is also vacuously true.

Statements that are vacuously true contain no useful information. To do interesting mathematics, we often have to show that a set does contain elements. Note the difference between the next example and Example 1.2.2. In Example 1.2.2, we showed that every element of X did satisfy the entrance criterion for the set $\{1, 4\}$. But that does not mean that 1 and 4 are elements of X or even that X has any elements at all. We now show that 4 is an element of X , but 1 is not.

1.2.6 Example

Let X be the set whose elements are the real numbers that are solutions to the equation $x - \sqrt{x} = 2$. Then $4 \in X$ and $1 \notin X$.

Proof. Let $x_0 = 4$. Then:

$$x_0 - \sqrt{x_0} = 4 - \sqrt{4} = 2.$$

Thus, $x_0 \in X$.

Let $x_1 = 1$. Notice that

$$x_1 - \sqrt{x_1} = 1 - \sqrt{1} = 0 \neq 2.$$

1.2.6

Thus, $x_1 \notin X$.

Therefore, both $4 \in X$ and $1 \notin X$, as desired. □

Putting Examples 1.2.2 and 1.2.6 together, we see that if X is the set whose elements are the real numbers that are the solutions to the equation $x - \sqrt{x} = 2$, then $X = \{4\}$. This follows, since Example 1.2.2 shows that every element of X is also an element of $\{1, 4\}$; Example 1.2.6 shows $1 \notin X$, so actually every element of X is also an element of $\{4\}$. Example 1.2.6 also shows that $4 \in X$. Our (informal) definition of “set” asserts that two sets are equal if and only if they have the same elements. Hence, $X = \{4\}$.

1.2.7

Exercise

Think carefully about Examples 1.2.2 and 1.2.6. Are there any steps of the proofs that you have no idea how to prove? What are they?

1.3 Subsets

“Pithy specificity is what we’re looking for, and we’ll know it when we see it. Example: {raven, writing desk}. Now we’re not *really* asking about this set itself. We’re asking about the set it’s a subset of.”

–William Flesch¹ [48]

1.3.1

Definition ▶ Subset

Suppose that A and B are sets. The set A is a **subset** of B if every element of A is also an element of B . We denote this by $A \subset B$. If A is a subset of B , then B is a **superset** of A and we write $B \supset A$. A is a **proper subset** of B if $A \subset B$ and $A \neq B$.

Some mathematicians use $A \subseteq B$ to mean that A is a subset of B and use $A \subset B$ to mean that A is a proper subset of B . We, however, will use $A \subsetneq B$ to indicate that A is a proper subset of B .

Here are some commonly occurring sets, each of which is a subset of one of the sets from Section 1.1.

1.3.2

An integer $n \in \mathbb{Z}$ is **even** if it is a multiple of 2. That is, if there exists $m \in \mathbb{Z}$ such that $n = 2m$. The set

$$2\mathbb{Z} = \{n \in \mathbb{Z} : n \text{ is even}\}$$

of even integers is a subset of the integers.

1.3.3

A number $p \in \mathbb{N}$ is **prime** if $p \neq 1$ and if p is a multiple only of itself and 1. More formally, if $p \in \mathbb{N}$ then p is prime if $p \neq 1$ and if whenever $m, n \in \mathbb{N}$ have the property that $p = mn$ then one of m, n equals 1 and the other equals p . The set of primes:

$$\{p \in \mathbb{N} : p \text{ is a prime}\}$$

is a subset of \mathbb{N} .

1.3.4

The unit circle in \mathbb{R}^2

$$S^1 = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$$

is a subset of \mathbb{R}^2 .

¹As Flesch points out, this is a reference to a famous riddle from *Alice in Wonderland*.

1.3.5

Much of mathematics is concerned with subsets of the real numbers \mathbb{R} . Intervals are particularly nice subsets of \mathbb{R} . Suppose that $a, b \in \mathbb{R}$ and $a < b$. Then we define the **open intervals** to be the sets:

- $(a, b) = \{x \in \mathbb{R} : a < x < b\}$
- $(a, \infty) = \{x \in \mathbb{R} : a < x\}$
- $(-\infty, b) = \{x \in \mathbb{R} : x < b\}$

Note that ∞ is not a real number, just a symbol helping us specify certain subsets of \mathbb{R} . We also define the **closed intervals** to be:

- $(\infty, b] = \{x \in \mathbb{R} : x \leq b\}$
- $[a, \infty) = \{x \in \mathbb{R} : a \leq x\}$
- $[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$
- $[a] = \{a\}$

We also have the intervals that are neither open nor closed:

- $[a, b) = \{x \in \mathbb{R} : a \leq x < b\}$
- $(a, b] = \{x \in \mathbb{R} : a < x \leq b\}$

1.3.6

Warning

Some notation is overused in mathematics. For example, out of context we can't tell whether $(1, 2)$ is an element of the Cartesian plane \mathbb{R}^2 or the open interval $\{x \in \mathbb{R} : 1 < x < 2\}$. We will have to live with this ambiguity and rely on context to tell us which meaning to use.

One of the most common tasks in mathematics is to show that one set is a subset of another. We begin by revisiting some earlier work.

1.3.7

Example ▶ (Examples 1.2.2 and 1.2.6 revisited)

Let X denote the set whose elements are the real number solutions to the equation $x - \sqrt{x} = 2$. In Example 1.2.2, we showed that if $x \in X$, then $x \in \{1, 4\}$. Thus, $X \subset \{1, 4\}$. In Example 1.2.6, we showed that $1 \notin X$. Thus, every element of X is equal to 4, so $X \subset \{4\}$. In Example 1.2.6, we also showed that $4 \in X$. Thus, $\{4\} \subset X$. By the definition of set equality, since X and $\{4\}$ have exactly the same elements, $X = \{4\}$.

The next theorem will be used (often without comment) throughout the text and its proof is a typical example of how to show one set is a subset of another set.

1.3.8

Example ▶ (transitivity of subsets)

We prove that if $A \subset B$ and $B \subset C$ then $A \subset C$.

Proof. Assume that $A \subset B$ and that $B \subset C$. We will show that $A \subset C$.

To show that $A \subset C$, we must show that every element of A is also an element of C . To that end, let $a \in A$ be arbitrary. Since $A \subset B$, by the definition of subset, $a \in B$. Since $B \subset C$, by the definition of subset, $a \in C$. Since this is true for every element of A , the set A is a subset of the set C . \square

This type of proof is another example of an **element argument**. Here's a summary of how it works in general:

ELEMENT ARGUMENT VERSION 2

To show: $X \subset Y$

Structure of Proof:

Assume $x \in X$ is arbitrary.

⟨ Do a bunch of work. ⟩

Hence, $x \in Y$. Since $x \in X$ was arbitrary, $X \subset Y$. \square

1.3.9

Example

Show that the interval $(2, 7)$ is a subset of the interval $[-5, 12]$.

Proof. Let $x \in (2, 7)$ be arbitrary. We will show that $x \in [-5, 12]$.

By the definition of the interval $(2, 7)$, we have $2 < x$ and $x < 7$. Since $-5 < 2$, we also have $-5 < x$. Hence, $-5 \leq x$. Similarly, since $7 < 12$, we also have $x < 12$. Since $-5 \leq x$ and $x < 12$, we conclude that $x \in [-5, 12]$. Since $x \in (2, 7)$ was arbitrary, $(2, 7) \subset [-5, 12]$. \square

The next theorem shows that every set is a subset of itself and that the empty set is a subset of every set. As will often be the case in this book, part of the proof is done for you and part you have to do!

1.3.10

Theorem

Let X be any set. Then $X \subset X$ and $\emptyset \subset X$.

Proof. We begin by explaining why $X \subset X$.

⟨ Explain why $X \subset X$. ⟩

We now explain why $\emptyset \subset X$. Since \emptyset is the set with no elements, it is vacuously true that every element of \emptyset (there are none!) is also an element of X . Thus, $\emptyset \subset X$. \square

1.3.11

Warning

It is crucial to distinguish between *elements* of a set X and *subsets* of a set X . What makes this challenging is that the English word “in” is ambiguous: it can mean either “element of” or “subset of”. For example, the sentence:

“ $\{1, 2\}$ is in the set X .”

could mean either $\{1, 2\} \in X$ (that is, the set $\{1, 2\}$ is an element of the set X) or $\{1, 2\} \subset X$ (that is, the set $\{1, 2\}$ is a subset of X).

1.3.12

Example

- $\{1, 2\}$ is an element of the set $X = \{7, 9, \emptyset, \{1, 2\}\}$ but is not a subset of X .
- $\{1, 2\}$ is a subset of $Y = \{1, 2, 3, 4, 5\}$ but is not an element of Y .
- $\{1, 2\}$ is both an element and a subset of the set $Z = \{1, 2, \{1, 2\}\}$.

1.3.13

Example

Let

$$\mathcal{U} = \{\emptyset, \{1, 2\}, \{1, 2, 3\}, \{a\}\}$$

Observe, for example, that $a \notin \mathcal{U}$ but $\{a\} \in \mathcal{U}$. Similarly, $\{a\} \notin \mathcal{U}$ but $\{\{a\}\} \subset \mathcal{U}$.

1.3.14

Exercise

Let $A = 1$ and $B = \{1\}$. Find an example of a set C such that $A \in B$ and $B \in C$ but $A \notin C$.

We begin to see some of the limitations of the box analogy for sets. If a set A is an element of a set B , the elements of A may or may not be elements of the set B . If we interpret \in as meaning “is inside,” we quickly run into problems since the elements of A will be inside A and A will be inside B , but the elements of A may or may not be inside B . The problem is not with our mathematics, but with our belief that \in exactly corresponds to our intuitive notion of what it means for one thing to be inside another thing. When in doubt, follow the literal meanings, not the imprecise intuition. As another example of this phenomenon, for single elements, we must distinguish between an element x and the set containing the element x , which is $\{x\}$. If $x \in X$, it is always the case that $\{x\} \subset X$, but it may or may not be the case that $\{x\} \in X$ or that $x \subset X$.

1.3.15

Exercise

For each of the sets \mathcal{U} below, determine which of the following statements are true. You may assume that a, b, c, d are fixed objects (not variables) having nothing to do with each other (so, for example, $a \neq \{b\}$, etc.)

(i) $a \in \mathcal{U}$

(iv) $\{a\} \subset \mathcal{U}$

(vii) $\{\{a, b\}\} \in \mathcal{U}$

(ii) $\{a\} \in \mathcal{U}$

(v) $\{a, b\} \in \mathcal{U}$

(viii) $\{\{a, b\}\} \subset \mathcal{U}$.

(iii) $a \subset \mathcal{U}$

(vi) $\{a, b\} \subset \mathcal{U}$

(ix) $\{a, b, c, d\} \subset \mathcal{U}$.

1. $\mathcal{U} = \{a, b, \{c, d\}\}$

5. $\mathcal{U} = \{\{a, b\}\}$

2. $\mathcal{U} = \{c, d, \{a, b\}\}$

6. $\mathcal{U} = \{\{a\}, \{b\}, \{a, b\}\}$

3. $\mathcal{U} = \{a, b, \{a, b\}\}$

7. $\mathcal{U} = \{\{\{a\}\}, \{b\}, \{\{a\}, b\}\}.$

4. $\mathcal{U} = \{a, \{a\}, b, \{b\}\}$

8. $\mathcal{U} = \{\{a\}, \{a, b\}, \{\{a\}\}, \{\{a, b\}\}\}$

1.4 Sets whose elements are sets

“ ‘That’s right,’ said Monty, who thought it good himself.

‘Yes. Wheels within wheels.’ ”

-P.G. Wodehouse, *Luck of the Bodkins*¹ [131]

In the previous section, we saw some examples of sets some of whose elements were also sets. Those examples were not very interesting, however, because they were created to make a point rather than in a natural setting. But it is the case that many sets in mathematics have elements that are sets. We will often denote such sets with a capital letter in a script typeface, such as \mathcal{A} , \mathcal{L} , or \mathcal{C} .

1.4.1

Example

For each natural number q , let

$$q\mathbb{N} = \{a \in \mathbb{N} : \text{there is an } m \in \mathbb{N} \text{ s.t. } a = mq\}$$

be the set whose elements are all the natural numbers which are multiples of q . The set

$$\mathcal{A} = \{q\mathbb{N} : q \in \mathbb{N}\}$$

is an example of a set whose elements are sets. One of its elements is the set of all multiples of 5. That is,

$$\{5, 10, 15, 20, \dots\} \in \mathcal{A}.$$

¹Monty Bodkin is alluding to the Biblical book of Ezekiel, chapter 1, verse 16.

Remark 1.4.1. We have remarked before on the necessity of keeping straight the difference between elements and subsets. Example 1.4.1 provides a good opportunity to test our observational powers. Notice that while $\emptyset \subset \mathcal{A}$ because the empty set is a subset of every set, $\emptyset \notin \mathcal{A}$ because none of the sets $q\mathbb{N}$ is the empty set.

1.4.2 Example

Let X be a set. Then

$$\mathcal{P}(X) = \{A : A \subset X\}$$

is the set such that $A \in \mathcal{P}(X)$ if and only if $A \subset X$. The set $\mathcal{P}(X)$ is called the **power set** of X . We study it more in Section 5.5.

1.4.3 Example

Let

$$\mathcal{O} = \{(a, b) : a < b\}$$

be the set of bounded open intervals in \mathbb{R} . That is, $I \in \mathcal{O}$ if and only if there exist $a, b \in \mathbb{R}$ with $a < b$ such that $I = (a, b)$. Clearly, each element of \mathcal{O} is also a set.

1.4.4 Example

For each $m \in \mathbb{R}$, let

$$L_m = \{(x, y) \in \mathbb{R}^2 : y = mx\}$$

be the line in \mathbb{R}^2 through the origin having slope m . The set

$$\mathcal{L} = \{L_m : m \in \mathbb{R}\}$$

is the set such that $\lambda \in \mathcal{L}$ if and only if λ is a non-vertical line in \mathbb{R}^2 passing through the origin. Each element of \mathcal{L} is a subset of \mathbb{R}^2 . (But, of course¹, not every subset of \mathbb{R}^2 is an element of \mathcal{L} , since not every subset of \mathbb{R}^2 is a line.)

1.4.5 Exercise

For each of Examples 1.4.2, 1.4.3, 1.4.4, consider whether or not \emptyset is an element of the set or is only a subset of the set.

We often need to refer to elements of a set using particular labels. We refer to the set of labels as the **index set**. For instance, in Example 1.4.4 the set \mathbb{R} is an index set for the set \mathcal{L} of non-vertical lines in \mathbb{R}^2 . This is because each element $L_m \in \mathcal{L}$

¹The phrase “of course” can be off-putting to some people. Whenever you see it in a mathematical text, the author is trying to indicate that you shouldn’t have to think very hard about why the statement is true. Typically, however, you have to think some! After you figure out whether or not the statement is true, it’s usually worth considering whether or not you agree with the author that it didn’t require very much thought.

corresponds to the real number $m \in \mathbb{R}$ and each real number $m \in \mathbb{R}$ corresponds to an element $L_m \in \mathcal{L}$. Here are some more examples. We generally won't make too big a deal out of index sets - they simply provide a convenient way of referring to elements from a set we care about. We will often use Λ to refer the index set and λ to refer to an index (or label). As is our tendency in mathematics, we will sometimes use symbols other than Λ , λ , and A_λ . What matters is the role each symbol plays, not what it looks like.

1.4.6 Example

Let $X = \{\frac{1}{n} : n \in \mathbb{N}\}$. That is:

$$X = \left\{1, \frac{1}{2}, \frac{1}{3}, \dots\right\}.$$

Then \mathbb{N} is an index set for X , since each natural number $n \in \mathbb{N}$ corresponds to some element (namely $1/n$) of X and each element of X corresponds to some element of \mathbb{N} .

1.4.7 Example

Let $p_1 = 2$, $p_2 = 3$, and $p_3 = 5$. Then the set $\Lambda = \{1, 2, 3\}$ is an index set for the set

$$X = \{2, 3, 5\}.$$

1.4.8 Example

Let $S^1 = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$ be the unit circle. Let x_θ be the point at the counter-clockwise angle θ radians from $(1, 0)$. Then

$$S^1 = \{x_\theta : \theta \in [0, 2\pi)\}$$

so $[0, 2\pi)$ is an index set for S^1 .

We've intentionally been somewhat vague about what an index set for a set X is. The essential requirement is that each element λ of the index set Λ corresponds to exactly one element of X and every element of X has at least one corresponding label $\lambda \in \Lambda$. Thus, the set $[0, 2\pi]$ is also an index set for S^1 , but in this case $\theta = 0$ and $\theta = 2\pi$ correspond to the same element of S^1 . Similarly, we could also use \mathbb{R} as an index set, since for each $\theta \in \mathbb{R}$, there is exactly one corresponding element $x_\theta \in S^1$ (the point at angle θ radians from $(1, 0)$) and if $x \in S^1$ then there exists some $\theta \in \mathbb{R}$ such that $x = x_\theta$.

We will often use index sets for sets whose elements are also sets. Example 1.4.4 was one such example (since a line is a subset of \mathbb{R}^2). Here are some more.

1.4.9

Example

For each $q \in \mathbb{N}$, let

$$A_q = q\mathbb{N} = \{a \in \mathbb{N} : \text{there is an } m \in \mathbb{N} \text{ s.t. } a = mq\}$$

be the set whose elements are all the natural numbers that are multiples of q . Let

$$\mathcal{A} = \{A_q : q \in \mathbb{N}\}.$$

Notice that for each $q \in \mathbb{N}$, the set A_q has the label q and that \mathcal{A} consists precisely of those sets which have such a label. Thus \mathbb{N} is an index set for \mathcal{A} .

1.4.10

Example

Let \mathcal{O} be the set of open intervals of length 2 in \mathbb{R} . For $r \in \mathbb{R}$, let $A_r = (r - 1, r + 1)$. We claim that \mathbb{R} is an index set for \mathcal{O} . To see this, observe that each $r \in \mathbb{R}$, the interval A_r is an element of \mathcal{O} . On the other hand, if $(a, b) \in \mathcal{O}$ is an open interval of length 2, we can define $r = (a + b)/2$. In which case, $A_r = (a, b)$. This makes \mathbb{R} into an index set for \mathcal{O} , since each $r \in \mathbb{R}$ corresponds to an element of \mathcal{O} and every element of \mathcal{O} has a corresponding $r \in \mathbb{R}$.

Our final example will show up again in the next chapter.

1.4.11

Example

An **oriented line** in \mathbb{R}^2 is a line, together with a direction (or arrow) on it. Each oriented line has a left side and a right side, which is a half plane to the left or right of the line. Keeping the line the same, but switching the direction changes the left side into the right side and the right side into the left side. Let Λ be the set of oriented lines in \mathbb{R}^2 . For each $\lambda \in \Lambda$, let $R(\lambda)$ be its right side. See Figure 1.2 for an example. Then the set

$$\mathcal{H} = \{R(\lambda) : \lambda \in \Lambda\}$$

of half planes is indexed by Λ .

1.5 Proving set equality

Logician: Here is an example of a syllogism. The cat has four paws. Isidore and Fricot both have four paws. Therefore Isidore and Fricot are cats.

Old Gentleman: My dog has got four paws.

Logician: Then it's a cat.

Old Gentleman: So then logically speaking, my dog must be a cat?

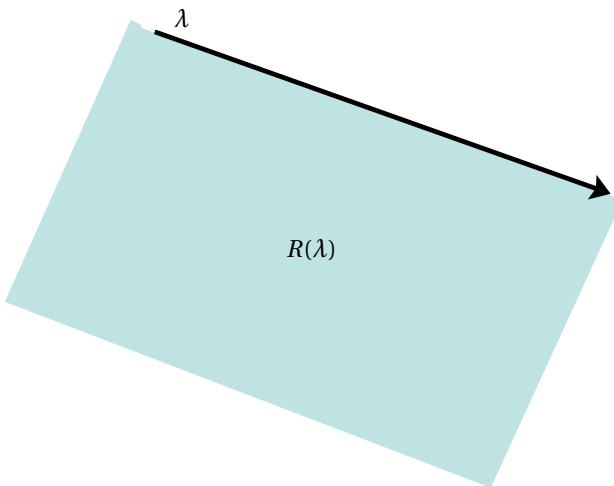


Figure 1.2: An example of a half plane indexed by the oriented line bounding it.

Logician: Logically, yes. But the contrary is also true.

– Eugène Ionesco¹, *Rhinoceros* [75]

We will often have to show that two sets are equal. From our initial informal definition, we know that two sets A and B are equal if every element of A is also an element of B and every element of B is also an element of A . This gives us the basic outline for how to show two sets are equal.

PROVING SET EQUALITY

To show: $A = B$ where A and B are sets.

Structure of Proof:

Claim 1: $A \subset B$.

Assume $a \in A$. We will show $a \in B$.

(Do it!)

Claim 2: $B \subset A$.

Assume $b \in B$. We will show $b \in A$.

(Do it!)

Since $A \subset B$ and $B \subset A$, we have shown $A = B$.

1.5.1

Example

Let X be the set whose elements are the real numbers that are solutions to the equation $x^2 - 1 = 0$. Then $X = \{-1, +1\}$.

¹Can you articulate the error made by the Logician? I take the Logician's statement "But the contrary is also true." to mean that the cat must also be a dog, rather than the negation which would be "My dog is not a cat."

Proof. We begin by showing $X \subset \{-1, +1\}$.

Assume $x \in X$. We will show that $x \in \{-1, +1\}$. By the definition of X , this implies $x^2 - 1 = 0$. Basic algebra shows that $(x - 1)(x + 1) = 0$. The product of two real numbers is zero if and only if one of them is zero. Therefore, either $(x - 1) = 0$ or $(x + 1) = 0$. Consequently, either $x = -1$ or $x = +1$. Thus, $x \in \{-1, +1\}$.

Next we show that $\{-1, +1\} \subset X$. Let $y \in \{-1, +1\}$. We will show that $y \in X$. Either $y = -1$ or $y = +1$. If $y = -1$, we have

$$y^2 - 1 = (-1)^2 - 1 = 0.$$

By the definition of X , this implies that $y \in X$.

On the other hand, if $y = +1$, then we have

$$y^2 - 1 = (1)^2 - 1 = 0.$$

1.5.1

Again, by the definition of X , we have $y \in X$. Since, no matter which $y \in \{-1, +1\}$ we choose, we have $y \in X$, we conclude that $\{-1, +1\} \subset X$.

Since $\{-1, +1\} \subset X$ and $X \subset \{-1, +1\}$, we know that $X = \{-1, +1\}$. \square

Remark 1.5.1. Our definition of set equality has the interesting consequence that all that matters is whether or not a particular element is an element of the set, not “where” it lives in the set or how many times it appears when we represent the set. Because of this, people often say that each element of a set appears in a set only once and that the order of elements in a set doesn’t matter.

1.5.2

Example

We have $\{1, 2, 3\} = \{2, 3, 1\}$, since the sets have exactly the same elements.

1.5.3

Example

We have $\{1, 1, 2, 3\} = \{1, 2, 3\}$ since the sets have exactly the same elements. In particular, $1 \in \{1, 1, 2, 3\}$ and $1 \in \{1, 2, 3\}$; $2 \in \{1, 1, 2, 3\}$ and $2 \in \{1, 1, 2, 3\}$; and $3 \in \{1, 1, 2, 3\}$ and $3 \in \{1, 2, 3\}$. Furthermore, neither $\{1, 1, 2, 3\}$ nor $\{1, 2, 3\}$ have any elements besides 1, 2, and 3.

1.6 Uniqueness of certain elements

“A Tour of the World in Eighty Days” is perhaps one of the most unique of the many unique novels that have emanated from the unique pen of that most unique of French Novelists, Jules Verne.”

– Advertisement in *The Lawrence Gazette*, December 26, 1889.

1.6.1

We have seen how element arguments can be used to show that some particular element x exists as an element of a set X . Often paired with the question of whether or not x exists as an element of a certain set is the question of whether or not x is the *unique* element of the set, or is the unique element of the set with a given property. More precisely, for a given property P , we say that $x \in X$ is the **unique element of X with property P** if x has property P and whenever $y \in X$ also has property P , then $y = x$.

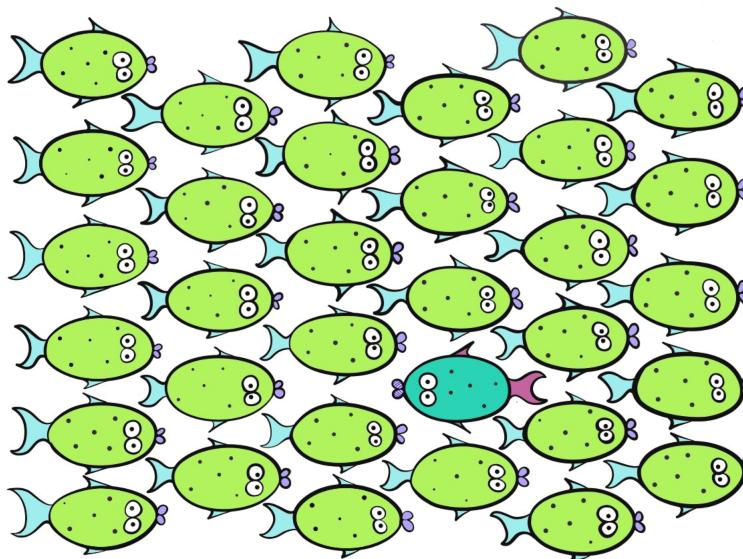


Figure 1.3: There exists a unique fish swimming from right to left.

1.6.2

We won’t be able to do any really interesting examples until we have developed more mathematics, but here is an initial example of how to write a uniqueness argument.

1.6.3

Theorem

There is a unique element $(x_0, y_0) \in \mathbb{R}^2$ such that $y_0 = 2x_0$ and $y_0 = x_0 + 1$.

Proof. We first present the element $(x_0, y_0) \in \mathbb{R}^2$ such that $y_0 = 2x_0$ and $y_0 = x_0 + 1$. We then prove that it is the unique element with that property.

Let $x_0 = 1$ and let $y_0 = 2$. Observe that $(x_0, y_0) \in \mathbb{R}^2$ has the property that

$$y_0 = 2 = 2 \cdot 1 = 2x_0$$

and

$$y_0 = 2 = 1 + 1 = x_0 + 1.$$

Thus, such an element $(x_0, y_0) \in \mathbb{R}^2$ exists.

Now suppose that $(x, y) \in \mathbb{R}^2$ is an element such that $y = 2x$ and $y = x + 1$. We will show that $(x, y) = (x_0, y_0)$. By algebra, we have

$$2x = x + 1$$

Subtracting x from both sides gives

$$x = 1 = x_0.$$

Since $y = 2x$, we also have $y = 2(1) = y_0$. Thus, $(x, y) = (x_0, y_0)$. Consequently $(1, 2)$ is the unique element of \mathbb{R}^2 satisfying $y = 2x$ and $y = x + 1$. \square

In our proof, it is natural to wonder where the choice of $x_0 = 1$ and $y_0 = 2$ at the beginning came from. The answer is that prior to writing the proof we worked the algebra out on scratch paper. The algebra suggests that the unique element should be $(1, 2)$ and we then verify that it works. When we write the proof up formally, the reader does not need to see the scratch work.

The typical outline for proving uniqueness is as follows.

UNIQUENESS THEOREMS

To show: There exists a unique element of a set X with a particular property P .

Structure of Proof: First we show that such an element exists. Define $x \in X$ by:

(explain how to define x)

Next we verify that x has property P :

(Show that x has property P)

Hence, there exists an element of X with property P .

Now we prove uniqueness. Assume that $y \in X$ and $z \in X$ both have property P .

(Show that $y = z$.)

Alternatively, we could simply show that if $y \in X$ has property P , then $y = x$, where x is the element we previously verified had property P . \square

We will discuss another way of proving uniqueness in Section 4.5.

1.7 Additional Exercises

Do you often come across people for whom, all their lives, a “subject” remains a “subject,” divided by watertight bulkheads from all other “subjects,” so that they experience very great difficulty in making an immediate mental connection between let us say, algebra and detective fiction, sewage disposal and the price of salmon – or, more generally, between such spheres of knowledge as philosophy and economics, or chemistry and art?"

– Dorothy L. Sayers, “The Lost Tools of Learning” (1947)

Here are some additional chances to begin learning how to write a proof by adapting proofs you’ve already encountered. As a reminder, the algebra involved in these exercises is intended to be relatively easy. The key point is that you are now supposed to frame the algebra with sentences explaining what you’re doing and how that is relevant to what you are supposed to prove. When you write down your proofs, be sure to get the structure of the proof correct.

1. (See Section 1.2.) Let X be the set whose elements are all pairs of real numbers (x, y) such that $y = x(x - 2)(x + 2)$ and $x = y^3 - 28y/3$. Prove that $(-1, 3) \in X$ and $(1, -3) \in X$.
2. (See Section 1.2.) Let X be the set of pairs of real numbers (x, y) that are solutions to both the equation $x^2 + y^2 = 1$ and the equation $x^2 - y^2 = 1$. Prove that $(1, 0) \in X$ and $(-1, 0) \in X$.
3. (See Section 1.2.) Let X be the set of pairs of real numbers (x, y) that are solutions to both the equation $x^2 + y^2 = 1$ and $x^2 - y^2 = 1$. Prove that (x, y) of X is either $(1, 0)$ or $(-1, 0)$. Combined with the previous exercise, this shows that $(x, y) \in X$ if and only if $(x, y) = (1, 0)$ or $(x, y) = (-1, 0)$.
4. (See Section 1.2.) It is a fact that if x is an odd integer, then there exists an integer n such that $x = 2n + 1$. Let \mathbb{O} denote the set of odd integers. Use the fact to prove that if $x \in \mathbb{O}$, then x^2 is one more than a multiple of 4.
5. (See Section 1.2 and 1.3.) Let C^2 be the set¹ of all functions $f: \mathbb{R} \rightarrow \mathbb{R}$ that have continuous second derivatives. Let $\mathcal{H} \subset C^2$ be the subset of all functions $f: \mathbb{R} \rightarrow \mathbb{R}$ with the property that $f''(x) = -4f(x)$ for all $x \in \mathbb{R}$. (This is an example of a differential equation describing “simple harmonic motion.” It shows up as a simple mathematical model of how a mass on a spring might move.)

For arbitrary $A, B \in \mathbb{R}$, let $g: \mathbb{R} \rightarrow \mathbb{R}$ be the function defined by $g(x) = A\sin(2x) + B\cos(2x)$. Explain why $g \in \mathcal{H}$.

¹The notation $f: \mathbb{R} \rightarrow \mathbb{R}$ means that f is a function with a graph that can be described as $y = f(x)$ where both x and y are real numbers. These are the sort of functions you studied in Calculus.

6. (See Section 1.3.) Explain why \emptyset is a subset of every set but is not an element of every set.
7. (See Section 1.3.) Let $6\mathbb{Z} = \{n \in \mathbb{Z} : \text{there exists } m \in \mathbb{Z} \text{ s.t. } n = 6m\}$. Let $3\mathbb{Z} = \{n \in \mathbb{Z} : \text{there exists } m \in \mathbb{Z} \text{ s.t. } n = 3m\}$. Prove that $6\mathbb{Z} \subset 3\mathbb{Z}$.
8. (See Section 1.3.) Let S be the set of real numbers that are solutions to the equation

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

Let Y be the set of real numbers that are not equal to 1. Prove that $S \subset Y$.

9. (See Section 1.3.) Let S be the set of real numbers that are solutions to the equation

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

Let Y be the set of real numbers that are not equal to 1. Prove that $Y \subset S$.

10. (See Exercise 1.3.15.) For each of the sets \mathcal{U} below, determine if the following statements are true. You may assume that a, b, c, d are fixed objects (not variables) having nothing to do with each other (so, for example, $a \neq \{b\}$, etc.)

- | | | |
|----------------------------------|--------------------------------------|------------------------------------|
| (i) $a \in \mathcal{U}$ | (iv) $\{\{a\}\} \subset \mathcal{U}$ | (vii) $\{a, b\} \in \mathcal{U}$. |
| (ii) $\{a\} \subset \mathcal{U}$ | (v) $\{\{a\}\} \in \mathcal{U}$. | |
| (iii) $\{a\} \in \mathcal{U}$ | (vi) $\{a, b\} \subset \mathcal{U}$ | |

- | | |
|--|--|
| (a) $\mathcal{U} = \{a, \{a\}, b, \{b\}, \{a, b\}\}$ | (d) $\mathcal{U} = \{a, b, \{\{a\}, \{b\}\}\}$. |
| (b) $\mathcal{U} = \{\{a, b\}, \{a, \{b\}\}\}$ | (e) $\mathcal{U} = \{\{a\}, \{\{a\}\}\}$ |
| (c) $\mathcal{U} = \{\{b, a\}, \{a, \{a\}\}\}$ | |

11. (See Section 1.4.) Write down a set \mathcal{C} such that $s \in \mathcal{C}$ if and only if s is a circle in \mathbb{R}^2 centered at the origin.
12. (See Section 1.4.) Write down a set \mathcal{A} such that $Z \in \mathcal{A}$ if and only if Z is an open interval in \mathbb{R} .
13. (See Section 1.4.) Give an example of a set \mathcal{N} such that $\emptyset \in \mathcal{N}$ and whenever $X \in \mathcal{N}$, then $\{X\} \in \mathcal{N}$.
14. (See Section 1.4.) Give an example of a set \mathcal{Q} such that *all* of the following hold:
- (a) If $A \in \mathcal{Q}$, then $A \subset \mathbb{N}$.
 - (b) Every element $A \in \mathcal{Q}$ has exactly 3 elements.

- (c) For every element $n \in \mathbb{N}$, there exists exactly one $A \in \mathcal{Q}$ such that $n \in A$.

The set \mathcal{Q} is an example of a partition of \mathbb{N} . We'll discuss partitions more in Section 7.2.

15. (See Section 1.4.) Let X be a set and let $\mathcal{S} = \{\{x\} : x \in X\}$. Explain why X is an index set for \mathcal{S} .
16. (See Section 1.4.) Let \mathcal{C} be the set of circles of radius 1 which are subsets of \mathbb{R}^2 . Find an index set for \mathcal{C} .
17. (See Section 1.4.) Suppose that \mathcal{A} is a set such that every element of \mathcal{A} is a set. Explain why \mathcal{A} is an index set for itself.
18. (See Section 1.5.) Let S be the set of real numbers which solutions to the equation

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

Let Y be the set of real numbers which are not equal to 1. Prove that $S = Y$. (You may appeal to previously proved results.)

19. (See Section 1.5.) Let A be the set of elements $(x, y) \in \mathbb{R}^2$ such that both $y = x^2$ and $y = x(x-1)(x+1)$. Let $B = \{(0, 0), (\frac{1+\sqrt{5}}{2}, \frac{3+\sqrt{5}}{2}), (\frac{1-\sqrt{5}}{2}, \frac{3-\sqrt{5}}{2})\}$. Prove that $A = B$.
20. (See Section 1.5.) Let Z be the set of real numbers which are elements of both the interval $(2, 8)$ and the interval $(5, 21)$. Prove that $Z = (5, 8)$.

21. (See Section 1.5.) Let C^1 be the set of all functions $f: \mathbb{R} \rightarrow \mathbb{R}$ which have continuous first derivatives. Let $\mathcal{F} \subset C^1$ be the subset of all functions $f: \mathbb{R} \rightarrow \mathbb{R}$ with the property that $f'(x) = -4f(x)$ for all $x \in \mathbb{R}$. (This is an example of a differential equation describing “exponential growth.”)

Let \mathcal{E} be the set of all functions $g_A: \mathbb{R} \rightarrow \mathbb{R}$ defined by $g(x) = Ae^{-4x}$ for some $A \in \mathbb{R}$ and all $x \in \mathbb{R}$. Explain why $\mathcal{F} = \mathcal{E}$.

22. (See Section 1.6.) Let $A = \{(x, y) \in \mathbb{R}^2 : y = 5x\}$. Let $B = \{(x, y) \in \mathbb{R}^2 : y = 3x - 6\}$. Prove that there is a unique element of \mathbb{R}^2 which is an element of both A and B .

23. (See Section 1.6.) Fix some $r > 0$. Let $D = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 \leq r^2\}$ be the disc in \mathbb{R}^2 centered at the origin and having radius r . Let

$$L = \{(x, y) \in \mathbb{R}^2 : y = -\sqrt{3}x + 2r\}.$$

Prove that there is a unique element of \mathbb{R}^2 which is an element of both D and L .

2 | Sets with Structure

“What does it take to be a mathematician? My experience has been that the key ingredient is the fascination with the theory and the manipulations of its structure. It does not take brilliance, but love of a great game!”

—Karen Keskulla Uhlenbeck² [30]

Key Concepts

Given an axiom system similar to the axioms for a group, metric space, or natural number system,

- be able to show that a given set satisfies the axioms;
- be able to use the axioms to prove theorems applicable to any set satisfying the axioms

Each branch of mathematics has sets of particular interest to that branch. For example, the sets of numbers \mathbb{Z} and \mathbb{Q} are of primary interest to number theorists and 3-dimensional space \mathbb{R}^3 is of particular interest to geometers. What makes each of these sets interesting, however, is how the elements of the set relate to each other. For \mathbb{Z} and \mathbb{Q} , numbers are related to each other by addition and multiplication (for instance). In \mathbb{R}^3 , elements are related to each other by how far apart they are from each other. In this chapter, we’ll explore four examples of sets with additional structure. Two of these structures (“group axioms” and “natural number systems”) are modelled on the addition of integers. Another (“metric space”) is modelled on notions of distance. We also explore networks (which we call “graphs”). These examples will recur throughout the text.

For each example, we present a list of properties called “axioms.” Historically, an **axiom** was a statement that was accepted to be true, without the need for proof. More recently, the word “axiom” is used to describe a property that may or may not hold for a particular set. A collection of axioms can be thought of as a list of essential features. Any theorem whose proof uses only those features applies to

²Karen Uhlenbeck does research in partial differential equations and was the first woman to be awarded the prestigious Abel prize for mathematics.

any object having those features.

2.0.1

Warning

When you first read the definitions of *group*, *metric space*, *graph*, and *natural number system* given below you will likely feel rather lost. That's okay! Only by jumping in and working through our unease can we get to the point where we can internalize abstract definitions. We haven't yet carefully discussed logic or proof structures, so your proofs of the theorems below will almost certainly be incomplete and unsatisfactory. You should revisit your proofs of these theorems again after working through the later chapters.



2.1 Groups

“We try to get natural problems from the physical world, but we also try to create problems based on the development of our understanding of nature. It’s like an artist who paints a picture. Some of the pictures are realistic and you can see the world. But an artist can also see nature and create an image related to it in an abstract way. We do that, too.”

—Shing-Tung Yau¹ [30]

The notion of a *group*, our first example of a set with additional structure, is chosen because there are very few axioms and the axioms capture some of the behavior of the familiar operations of addition, multiplication, and function composition. The hope is that groups are unfamiliar enough so that you see the need for abstract approaches, but close enough to familiar objects that you can draw on your previous math experience to explore them. In Section 2.5, we see how groups are used to describe symmetries of geometric objects.

2.1.1 Definition ▶ Axioms for a Group G

A set G , together with an element $\mathbb{1} \in G$ (called the **identity** of the group), and a way (denoted \circ) of combining elements of the set, is a **group** if the following hold:

(G1) (closure) For every $a \in G$ and $b \in G$ there is a some element $c \in G$ such that $c = a \circ b$. Furthermore, this combination is unique. In other words, if $a = a'$ and $b = b'$, then:

$$a \circ b = a' \circ b'.$$

(G2) (identity) The following hold:

- For every $a \in G$, $a \circ \mathbb{1} = a$.
- For every $a \in G$, $\mathbb{1} \circ a = a$.

(G3) (inverses) For every $a \in G$ there exists $b \in G$ (more traditionally denoted a^{-1}) such that the following hold:

- For every $a \in G$, $a \circ b = \mathbb{1}$.
- For every $a \in G$, $b \circ a = \mathbb{1}$.

(G4) (associativity) For every $a, b, c \in G$

$$(a \circ b) \circ c = a \circ (b \circ c).$$

Before we begin exploring groups, we should observe that, given the definition,

¹Shing-Tung Yau is one of the foremost differential geometers of the 20th and early 21st centuries.

we could try to do any of the following:

1. *Prove that certain choices of set G and operation \circ are examples of groups.*
Doing this will help us mentally connect the abstract definition of a group with concrete examples we've worked with before.
2. *Prove that certain choices of set G and operation \circ are not examples of groups.*
Doing this will help us know the limitations of the abstract definition.
3. *Prove theorems about groups, using only logic and the properties in Definition 2.1.1.* Doing this will provide true facts pertaining to any set G and operation \circ which are groups, not just our favorite, well-known ones.
4. *Find applications of group theory, either within mathematics or outside of mathematics.* This will show the usefulness of group theory and requires us to understand the extent to which group theory is appropriate for studying whatever it is we want to study.

In this section, we will get just a taste of tasks (1), (2), and (3). In future sections, we will see some examples of applications of group theory, both within mathematics and outside of mathematics.

Examples and non-examples of groups

It is crucial when discussing a set G that is (potentially) a group to specify not just what the set G is but also the operation \circ . In the definition, the symbols G and \circ are not important - what is important are their roles. In particular examples, the set might be denoted X , G' , Q , or something else and the operation might be denoted $+$, \cdot , \oplus , $*$, or something else. Likewise, although we are denoting the identity by $\mathbb{1}$, even when G is a set of numbers, $\mathbb{1}$ need not be the *number* one. On the other hand, when we are proving theorems that apply to any group, we do not need specify G , $\mathbb{1}$, and \circ precisely, since we are making statements that apply no matter what G , $\mathbb{1}$, and \circ are (as long as they form a group.)

Notice that each of the axioms claims something along the lines of “For every $a \in G$ ” (or “every $a \in G$ and $b \in G$ ”, etc.). If the axiom holds, we can replace the a with any other symbol representing an element of G . For example, it turns out that the integers \mathbb{Z} with addition $+$ and identity equal to the number 0, is a group. If we set $a = 5$ and $b = 7$, Axiom (G2) guarantees that $a + 0 = a$, (that is, $5 + 0 = 5$), but it also guarantees that $b + 0 = b$ (that is, $7 + 0 = 7$.)

To show that a set G with an identity $\mathbb{1}$ and an operation \circ is a group, we must explain why (G1) - (G4) all hold. Axiom (G4) is usually the most irritating to verify and, in this text, we will often omit the proofs showing that axiom holds. To show that a set G with an operation \circ is not a group we must show that at least one of (G1) - (G4) does not hold.

2.1.2

Example

For each of the following examples, verify that axioms (G1), (G2), and (G3) hold.

- \mathbb{Z}, \mathbb{Q} , and \mathbb{R} , each with operation $+$ and identity 0.
- $\mathbb{R} \setminus \{0\}$ (all real numbers except 0) with multiplication \cdot as the operation and the number 1 as the identity.
- The set $\{0, 1\}$ with the operation $+$ defined by $0+0=1+1=0$ and $0+1=1+0=1$ and number 0 as the identity.
- More generally, for a given $n \in \mathbb{N}$, let $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ with an operation \circ defined by letting $a \circ b$ be the remainder of $(a+b)$ when divided by n . The identity is the number 0.

2.1.3

Exercise

For each of the following examples, determine which of (G2), (G3), or (G4) do not hold. For each axiom which does not hold, specify particular elements of the group that do not satisfy the equations in that axiom.

- $\{0, 1, 2, \dots\}$ with operation $+$ and identity $1=0$.
- \mathbb{R} with operation \cdot (multiplication) and identity $1=1$.
- $\mathbb{Q} \setminus \{0\}$ (all rational numbers except 0) with operation \div (division) and identity $1=1$.

Here are some more advanced examples of groups, each is important in linear algebra.

2.1.4

Example

Let $M_2(\mathbb{R})$ be the set of all 2×2 arrays of real numbers. That is, $M \in M_2(\mathbb{R})$ if and only if there are $a, b, c, d \in \mathbb{R}$ such that

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

We define an operation, denoted $+$, on $M_2(\mathbb{R})$ by defining:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}.$$

Then $M_2(\mathbb{R})$ with the operation $+$ is a group having $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ as the identity.

2.1.5

Example

Let $GL_2(\mathbb{R})$ be the set¹ of all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{R})$ such that $ad - bc \neq 0$. Define

$$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a'a + b'c & a'b + b'd \\ c'a + d'c & c'b + d'd \end{pmatrix}.$$

Then $GL_2(\mathbb{R})$ is a group with operation \cdot and identity $\mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

2.1.6

Exercise

Verify that $GL_2(\mathbb{R})$ is a group by showing it satisfies all the group axioms.

Also if $T = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, find T^{-1} in terms of a, b, c, d .

2.1.7

Exercise

Let $SL_2(\mathbb{Z})$ be the set¹ of all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{R})$ such that a, b, c, d are integers

with $ad - bc = 1$. Define \cdot and identity as in Example 2.1.5. Adapt your solution to Exercise 2.1.6 to show that $SL_2(\mathbb{Z})$ is a group.

Two theorems about groups

The next two theorems concern the uniqueness of the identity and the uniqueness of inverses in a group. Note how the phrasing of the theorems parallels the definition of uniqueness given in 1.6 above. Be sure to structure your proofs of these theorems accordingly. The first proof is set up for you.

2.1.8

Theorem ▶ Uniqueness of Identity

Suppose that G is a group with operation \circ and identity $\mathbb{1}$. Suppose that $a \in G$. If x is an element such that $a \circ x = a$ or $x \circ a = a$, then $x = \mathbb{1}$.

Proof. Assume that G is a group with operation \circ and identity $\mathbb{1}$. Suppose, also, that $a, x \in G$ have the property that $a \circ x = a$ or that $x \circ a = a$. We will show that $x = \mathbb{1}$.

Case 1: $a \circ x = a$.

We will use axioms (G1), (G2), (G3), and (G4). Since $a \in G$, by axiom (G3) there exists an element $b \in G$ such that $b \circ a = \mathbb{1}$. By axiom (G1), $(a \circ x) \in G$ and

$$b \circ (a \circ x) = b \circ a.$$

¹The “G” stands for “general” and the “L” for “linear”. The 2 and the \mathbb{R} indicates that we are working with 2×2 arrays of real numbers.

²This time the “S” stands for “special.”

⟨ Use Axiom (G4) and the properties of b to show that $\mathbb{1} \circ x = \mathbb{1}$. ⟩

⟨ Use Axiom (G2) to show that $x = \mathbb{1}$. ⟩

Case 2: $x \circ a = a$.

⟨ Complete this case in a similar way to Case 1. ⟩

□

One important consequence of Theorem 2.1.8 below is that when claiming that something is a group we do not need to explicitly name which element we are considering to be $\mathbb{1}$. If the set and operation satisfy the group axioms, there is only one element which has the properties of $\mathbb{1}$. However, it is usually kind to the reader to say which element is the identity.

2.1.9

Theorem ▶ Uniqueness of Inverses

Suppose that G is a group with operation \circ and identity $\mathbb{1}$. Let $a \in G$ with a^{-1} an inverse of a in G given by axiom (G3). If $x \in G$ is an element such that $a \circ x = \mathbb{1}$ or $x \circ a = \mathbb{1}$ then $x = a^{-1}$.

Finally, we conclude with a useful exercise.

2.1.10

Exercise

Suppose that G is a group with operation \circ and identity $\mathbb{1}$. Prove that for all $a, b \in G$,

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

2.2 Metric Spaces

“Although I cannot claim to find it easy to balance my ambitions in mathematical research with the desire to be a good parent, to be an inspiring teacher, or to effect positive social change in the world, I do feel very fortunate to be able to spend my life tackling these challenges, which are extremely interesting and important to me.”

—Kate Adebola Okikiolu [30]

The group axioms each attempt to formally capture some of the properties of certain sets of numbers, most notably the ability to add or multiply. The axioms for a metric space, on the other hand, capture something of what we mean when we talk about “distance.”

2.2.1

Definition ▶ Axioms for a Metric Space

A set X is a **metric space** if the following hold:

- (M1) (positive) For every $x, y \in X$, there exists a unique real number $d(x, y) \in \mathbb{R}$ with $d(x, y) \geq 0$.
- (M2) (definite) For every $x, y \in X$, $d(x, y) = 0$ if and only if $x = y$.
- (M3) (symmetry) For every $x, y \in X$, $d(x, y) = d(y, x)$.
- (M4) (triangle inequality) For every $x, y, z \in X$,

$$d(x, z) \leq d(x, y) + d(y, z).$$

We call d the **metric**.

When specifying a metric space, we must always specify not only the set X but also the real numbers $d(x, y)$. It is possible (and indeed is usually the case) that a set X may have multiple, different, metrics. The elements of X are often called **points**. The number $d(x, y)$ is called the **distance** from x to y . The first axiom says that the distance between two points is always non-negative. The second axiom specifies that for each $x \in X$, the only element of distance zero from x is x itself. The third axiom says that the distance from a point x to a point y is the same as the distance from y to x . Finally, the triangle inequality says (informally) that the distance from x to z is never more than the distances obtained by going from x to y and then to z .

Given the definition of a metric space, as with the definition of a group, we may embark on 4 tasks:

1. *Show that some particular choices of X and d satisfy the definition of a metric space.*
2. *Show that some particular choices of X and d do not satisfy the definition of a metric space.*
3. *Prove theorems pertaining to any metric space.*
4. *Find applications of metric spaces either within or without mathematics.*

Metric spaces are studied more thoroughly in analysis and topology classes. In this book, we'll just get a sense for what they are and how they are useful. Metric spaces provide a helpful context for proving theorems using the definition and careful reasoning and also help develop geometric intuition. In this section, we'll just address tasks (1), (2) and (3). Task (4) will be addressed in future sections.

Examples and non-examples of metric spaces

2.2.2 Exercise

Let X be any set and define $d(x, y) = 1$ for all $x, y \in X$ with $x \neq y$. Also define $d(x, y) = 0$ if $x = y$. Prove that X (with the metric d) is a metric space by showing that (M1) - (M4) hold. We call d the **discrete metric** on X .

2.2.3 Exercise

Let $X = \mathbb{R}$ and let $d(x, y) = |x - y|$. Prove that X is a metric space (with metric d). For the triangle inequality, recall that $|x - y| = \sqrt{(x - y)^2}$ and use some algebra.

We may define a metric on \mathbb{R}^n for any $n \in \mathbb{N}$, by defining

$$d((x_1, x_2, \dots, x_n), (y_1, y_2, \dots, y_n)) = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2 + \dots + (x_n - y_n)^2}.$$

In the appendix to this chapter (Section 2.6) using methods unrelated to the rest of the text, we prove that (\mathbb{R}^n, d) satisfies the axioms of a metric space. The metric d is called the **euclidean metric** on \mathbb{R}^n .

The following are examples of metric spaces, though proving they are such can be rather tedious. There are many more examples of metrics on all kinds of different sets. Metric spaces are ubiquitous in mathematics.

2.2.4 • $X = \mathbb{R}^2$ and d_{\max} is the **max metric** defined by

$$d_{\max}((x_1, x_2), (y_1, y_2)) = \max(|x_1 - y_1|, |x_2 - y_2|).$$

2.2.5 • $X = \mathbb{R}^2$ and d is the metric defined by

$$d((x_1, x_2), (y_1, y_2)) = |x_1 - y_1| + |x_2 - y_2|.$$

2.2.6 • $X = \mathbb{R}^2$ and d_{comb} is the **comb metric** defined by

$$d_{\text{comb}}((x_1, y_1), (x_2, y_2)) = \begin{cases} |y_1 - y_2| & \text{if } x_1 = x_2 \\ |y_1| + |x_1 - x_2| + |y_2| & \text{if } x_1 \neq x_2. \end{cases}$$

2.2.7 • $A = [a, b] \subset \mathbb{R}$ and X is the set of continuous functions $f: A \rightarrow \mathbb{R}$. We define the **max metric** on X by declaring that

$$d(f, g) = \max\{f(x) - g(x) : x \in A\}.$$

The maximum is guaranteed to exist by the Extreme Value Theorem, from Calculus.

2.2.8

Example

Show that the following are *not* metric spaces by showing that one of the axioms for a metric space does not hold. For the second two, define the **length** of $a = (a_1, a_2) \in \mathbb{R}^2$, to be $\|a\| = \sqrt{a_1^2 + a_2^2}$.

1. The interval $X = (0, \infty) \subset \mathbb{R}$ with “metric” defined by $d(x, y) = \frac{x}{y}$.
2. The set $X = \mathbb{R}^2$ with “metric” defined by

$$d(a, b) = \begin{cases} 1 & \|a\| \leq 1 \text{ and } \|b\| > 1 \\ \|a - b\| & \text{otherwise,} \end{cases}$$

for all $a, b \in \mathbb{R}^2$.

3. The set $X = \mathbb{R}^2$ with “metric” defined by

$$d(a, b) = \begin{cases} 1 & \|a\| \leq 1 \text{ and } \|b\| > 1 \\ 1 & \|b\| \leq 1 \text{ and } \|a\| > 1 \\ \|a - b\| & \text{otherwise,} \end{cases}$$

for all $a, b \in \mathbb{R}^2$.

Theorems concerning metric spaces

The most interesting theorems for metric spaces require more mathematics than we have at present, but here are two sample results to give you the chance to practice using the definitions. The first proof is set up for you.

2.2.9

Theorem

Suppose that X is a metric space with metric d . Let $k > 0$ be a real number. For all $x, y \in X$, define $d'(x, y) = kd(x, y)$. Then X is a metric space with metric d' .

One way of interpreting the statement of the Theorem is that if d is a metric which we use to measure distances, and if we change our units of measurement by scaling, then the new way of measuring distances is still a metric. For example, if d measures in feet, then choosing $k = 12$, d' measures in inches, and is still a metric.

Proof. Assume that X is a metric space with metric d and that $k > 0$. Define $d'(x, y) = kd(x, y)$. We will show that X is a metric space with metric d' by showing that X and d' satisfy the axioms of a metric space. We will use the fact that we already know that d is a metric.

Axiom (M1): We must show that for every $x, y \in X$, there exists a unique real number $d'(x, y)$ with $d'(x, y) \geq 0$.

Let $x, y \in X$ be arbitrary. Since d is a metric, there exists a unique real number $d(x, y)$. Thus, $d'(x, y) = kd(x, y)$ is a real number. It is unique, since the product of two real numbers is a unique real number.

Axiom (M2): We must show that for every $x, y \in X$, $d'(x, y) = 0$ if and only if $x = y$.

Let $x, y \in X$ be arbitrary. We must show that if $x = y$ then $d'(x, y) = 0$ and we must also show that if $d'(x, y) = 0$ then $x = y$.

(Assume that $x = y$. Use the fact that $d(x, y) = 0$ to show that $d'(x, y) = 0$.)

(Assume that $d'(x, y) = 0$. Use the fact that $k \neq 0$ to show that $d(x, y) = 0$. Then use the fact that d is a metric to conclude that $x = y$.)

Axiom (M3): We must show that for every $x, y \in X$, we have $d'(x, y) = d'(y, x)$.

(Do it!)

Axiom (M4): We must show that for every $x, y, z \in X$, we have

$$d'(x, z) \leq d'(x, y) + d'(y, z).$$

(Do it!)

□

The next theorem gives one way of combining two different metrics into a single metric. You should organize the proof similarly to how the previous proof was organized.

2.2.10

Theorem

Suppose that X is a set and that d_1 and d_2 are both metrics on X . For all $x, y \in X$, define

$$d(x, y) = d_1(x, y) + d_2(x, y).$$

Then d is also a metric on X .

2.3 Graphs

“I should also point out, however, that most of the ideas that I have and the things that I try do not work, and I suspect that the same is probably true of many other mathematicians. Of course this just means that perseverance is a crucial part of the entire process, and that it is very important not to just give up too easily!”

–Adebisi Agboola [30]

In mathematics the term “graph” has (at least) two meanings. It can mean the “graph of a function”, as in Calculus courses. It can also, however, be used to refer to a network of nodes (called “vertices”) and connections (called “edges”). Throughout applied mathematics, computer science, and engineering this latter type of graph is used to model all kinds of networks.

2.3.1

Definition ▶ Graph

A **graph** consists of a set V (the set of **vertices**) and a set E (the set of **edges**) such that the following hold:

- For every edge $e \in E$, there are two (not necessarily distinct) vertices $v, w \in V$ called the **endpoints** of e . We write $\text{ENDS}(e) = \{v, w\}$.

Two graphs are the same exactly when they have the same set of vertices and the same set of edges.

Figure 2.1 shows a common way of visualizing graphs. We'll say more about visualizing graphs later.

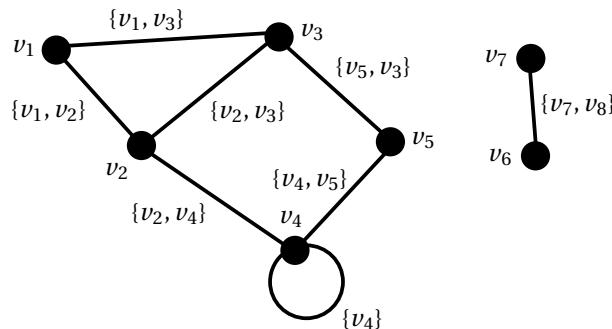


Figure 2.1: A graph with 7 vertices and 8 edges. We have given each vertex a label and marked each edge with the set of its endpoints. Note that the graph isn't “connected” and that there's a loop based at one vertex.

Using the formal definition of a graph, we can construct a few examples.

2.3.2

Example ▶ (The empty graph)

Let both the vertex set and the edge set be empty. The graph is called the **null graph**.

2.3.3

Example

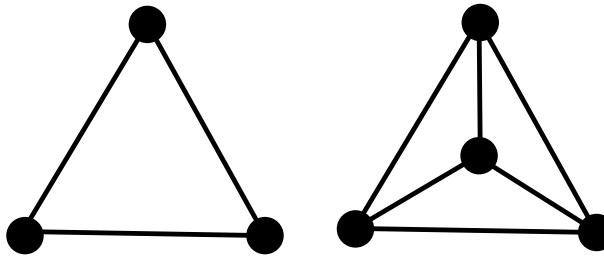
Let V be any set. The graph with vertex set V and edge set \emptyset is a graph with no edges; it consists of isolated nodes and no connections between them.

2.3.4

Example ▶ (The Web graph)

We can use graphs to model the World Wide Web. Let V be the set of web pages and let E be the set of edges such that for every pair of webpages $v, w \in V$ then the set $\{v, w\} \in E$ if and only if there is link in the webpage v linking v to w or vice versa. The graph is called the **web graph**. This graph changes over time.

As an indication of the complexity of the Web Graph, at [91] you can download

Figure 2.2: Pictures of the complete graphs $K(3)$ and $K(4)$.

a subset of the 2012 Web Graph, consisting of 3.5 billion vertices and 128 billion edges.

2.3.5 Exercise

Pick your favorite or least favorite social network (e.g. Facebook, Twitter, LinkedIn) and describe how to model it using a graph.

As we did above, in Figures 2.1 and 2.2, we can attempt to visualize some graphs (V, E) as follows. For each vertex $v \in V$, choose a point in the plane. If $\text{ENDS}(e) = \{v, w\} \in E$, draw a path from the point corresponding to v to the point corresponding to w .

Typically, we try to draw the paths as “nicely” as possible. Ideally, distinct edges should be drawn so that they do not intersect (except possibly at their endpoints). If such a picture is possible, then the graph is said to be **planar**. It can be very difficult to tell if a graph is or is not planar. To see why, try playing the game Planarity [123].

2.3.6 Definition ▶ Complete Graph

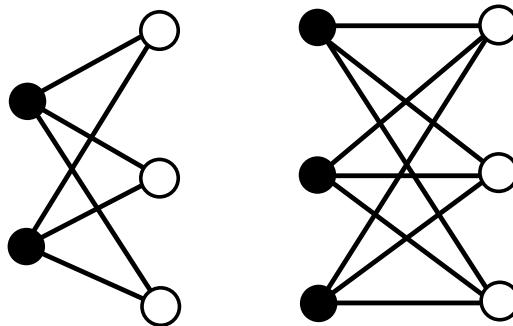
Let V be a set. The **complete graph** on V is the graph $K(V)$ with V the set of vertices and with edge set consisting of exactly one edge between each pair of distinct vertices. If V has n elements, we often write $K(n)$ instead of $K(V)$.

Complete graphs with very few edges are planar, as in Figure 2.2.

2.3.7 Definition ▶ Complete Bipartite Graph

Let V be a set with two non-empty subsets $B, W \subset V$ such that B and W have no elements in common and every element of V is either in B or in W . The **complete bipartite graph** $K(B, W)$ is the graph with vertices V and with an edge between every vertex of B and every vertex of W (and no other edges). If B has n vertices and W has m vertices, we often write $K(n, m)$ instead of $K(B, W)$.

Figure 2.3 shows some examples of complete bipartite graphs with few edges.

Figure 2.3: Pictures of the complete bipartite graphs $K(2, 3)$ and $K(3, 3)$.

2.3.8

Exercise

Let B and W be non-empty sets. Give a more formal definition of $K(B, W)$ by coming up with a description of the edge set of $K(B, W)$ as a set whose elements are sets.

Not surprisingly, most complete and complete bipartite graphs are non-planar. It should be easy to convince yourself (though maybe not so easy to write down a proof!) that $K(5)$ and $K(3, 3)$ are non-planar.

2.3.9

Exercise

Find a way of drawing $K(2, 3)$ so that no edges cross (i.e. show that $K(2, 3)$ is a planar graph).

Most of the graphs we consider in this text are “undirected”, meaning that edges do not have a starting vertex or an ending vertex. In the context of networks like the Web it might be more natural to consider directed graphs. For instance a *directed edge* might point from the webpage v containing the link to the webpage w to which v is linked. If there was no link in w linking back to v , then there would be no directed edge from w to v . If we wanted to consider directed edges, there are ways to modify the definition to do that. Start with an undirected graph G having vertex set V and edge set E and **direct** one or more of its edges. Informally, we place an arrow on one or more of the edges, as in Figure 2.4. This means that for each edge e we want to direct, if $\text{ENDS}(e) = \{v, w\}$, we declare one of v and w to be the **initial endpoint** of e and the other one to be the **terminal endpoint** of e . The directed edge e goes **from** its initial endpoint to its terminal endpoint. If every edge is directed, the graph is called a **digraph**.

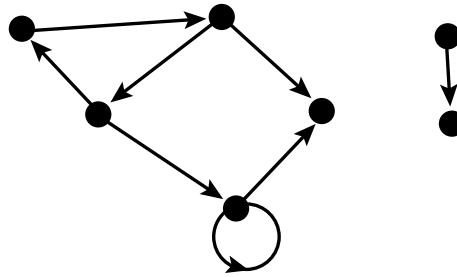


Figure 2.4: An example of a digraph. To turn a graph into a digraph, put an arrow on each edge so that it points from the initial endpoint to the terminal endpoint.

2.4 The natural numbers

“It was easier to know it than to explain why I know it. If you were asked to prove that two and two made four, you might find some difficulty, and yet you are quite sure of the fact.”

- Sir Arthur Conan Doyle, *A Study in Scarlet*

The set of natural numbers $\mathbb{N} = \{1, 2, 3, \dots\}$ is the set of counting numbers, but it is its *properties* rather than the particular names of its elements which establish its importance in mathematics. For example, rather than counting 1, 2, 3, 4, ..., we could count *I*, *II*, *III*, *IV*, ... or *a*, *b*, *c*, *d*, For that matter, we could count 0, 1, 2, 3, In 1889, the Italian mathematician Giuseppe Peano, published four properties (i.e. axioms) of a set which will guarantee that it is functionally equivalent to \mathbb{N} . That is, if a set N satisfies the three axioms below, then any statement about \mathbb{N} can be rephrased into a statement about N and vice versa. The axioms encapsulate the fact that after every natural number comes some other natural number.

For various reasons, historical and other, it is customary to state the axioms for the set of natural numbers together with 0 (that is, \mathbb{N}^*). For convenience, we define a **successor function** S on a set N to be an assignment to each $n \in N$, of a unique $S(n) \in N$. If $m = S(n)$, we also say that n is a **predecessor** of m . To make sense of the terminology, we can picture a set N with a successor function S as a digraph. The vertices of the digraph are the elements of N and we draw a directed edges from n to m if $m = S(n)$. Our rules for S guarantee that each vertex has exactly one outgoing edge. We pick one element **0** $\in N$ to be an **initial object**. We use a boldface font for **0** to indicate that (when all is said and done) the element has the same (or similar) properties to the familiar integer 0, but may not be literally equal to it. Figure 2.5 shows an example of a digraph representing a set with a successor function, as well as one possible choice for **0**.

Observe in Figure 2.5, we can start at **0** and “count” by following arrows. Once we choose our starting point, our counting path is completely determined, although in Figure 2.5 there will be many vertices that are never counted. Peano’s axioms are intended to make the counting exactly coincide with our intuitive notions of how counting through the elements of \mathbb{N} should work. When you first encounter the axioms, notice, however, that the axioms do not require that we already know

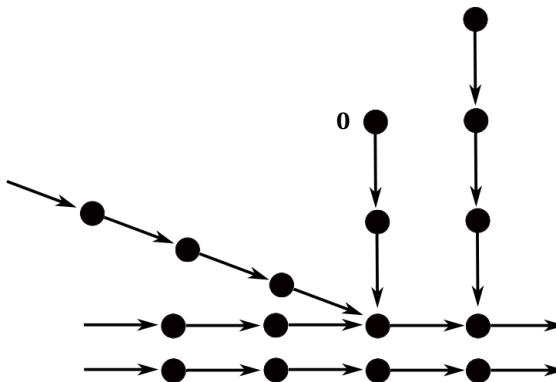


Figure 2.5: A digraph representing a set with a successor function. The arrows without two endpoints indicate an infinite progression of vertices and arrows. One of the elements is marked as an initial object.

about the existence of numbers or counting. For instance, as in Figure 2.6, we can *define* the number **1** to be the successor of the initial object and *define* **2** = $S(1)$ and **3** = $S(2)$ and so forth.

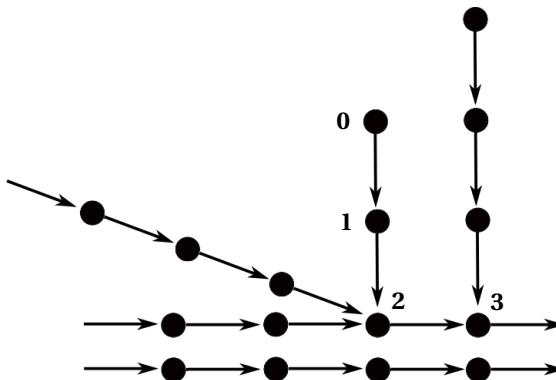


Figure 2.6: A digraph representing a set with a successor function. The arrows without two endpoints indicate an infinite progression of vertices and arrows. One of the elements is marked as an initial object **0**. We label the successor of **0** as **1**; the successor of **1** as **2**; and so forth.

If a set N has a successor function S , a nonempty subset $A \subset N$ is a **counting subset** of N if for all $n \in A$, $S(n) \in A$. Counting subsets of N have the property that we can start at any element of the subset and count as long as we like, while remaining in the subset.

2.4.1

Exercise

In the examples in Figures 2.5 and 2.6, identify 4 different counting subsets. Can you find one that does not contain **0**?

We are now ready for Peano's axioms.

2.4.2

Definition ▶ Peano's Axioms for a set N

Suppose that N is a set, that $\mathbf{0} \in N$ is a particular element (called the **initial object**), and that S is a successor function on N . We say that the triple $(N, \mathbf{0}, S)$ is a **natural number system** if the following axioms are satisfied:

- (P1) The initial object $\mathbf{0}$ does not have a predecessor. That is, there does not exist $n \in N$ such that $S(n) = \mathbf{0}$.
- (P2) No element has more than one predecessor. That is, for every $n, m \in N$, if $S(m) = S(n)$ then $m = n$.
- (P3) If $A \subset N$ is a counting subset such that $\mathbf{0} \in A$, then $A = N$.

2.4.3

Exercise

What do axioms (P1) and (P2) imply about the structure of the digraph created from a natural number system? Can such a digraph have a cycle? (That is a sequence of elements $x_1, x_2, \dots, x_n \in N$ such that $x_2 = S(x_1)$, $x_3 = S(x_2)$, ..., $x_n = S(x_{n-1})$ and $x_1 = S(x_n)$?) Can such a digraph have any vertices with more than one incoming edge?

Axiom (P3) is the most mysterious of the axioms, and it will likely remain mysterious for the duration of the chapter. Informally, it says that N has no proper subset that both contains the initial object and is closed under taking successors. Axiom (P3) is the basis for the method of proof known as “induction.” We explore that more in Chapter 9.

2.4.4

Exercise

For the Example in Figure 2.5, determine which of the Peano axioms are satisfied and which are not. Draw a digraph that satisfies (P1) and (P2) but not (P3). This shows that axiom (P3) is **independent** of axioms (P1) and (P2); that is, Axiom (P3) cannot be proved using only Axioms (P1) and (P2), the rules of logic, and the definitions.

2.4.5

Exercise

Observe that if we set $N = \mathbb{N}$, $\mathbf{0} = 1$, and $S(n) = n + 1$ for every $n \in \mathbb{N}$ then elementary algebra confirms that \mathbb{N} satisfies Axioms (P1) and (P2). Can you convince yourself that Axiom (P3) is also satisfied? Similarly, if we set $N = \{0, 1, 2, 3, \dots\}$, $\mathbf{0} = 0$, and $S(n) = n + 1$, then $(N, \mathbf{0}, S)$ also satisfies the Peano axioms.

Of course, Exercise 2.4.5 required that you already know that there is a set $\mathbb{N} = \{1, 2, 3, \dots\}$ and also required you to understand basic arithmetic. The whole point of the axioms, however, is to enable us to *deduce* the existence of such a set using the axioms as initial assumptions. The next exercises give you the opportunity to play around with the axioms to learn aspects of how each axiom captures some

feature of the natural numbers and can be used to exclude sets (or choice of **0** or **S**) which can't be used in place of the natural numbers.

2.4.6 Exercise

For the set $N = \mathbb{N}^*$ with **0** = 0, define a successor function S such that Axiom (P1) is satisfied but Axiom (P2) is not satisfied. You need to say exactly what $S(n)$ is for each $n \in \mathbb{N}$.

2.4.7 Exercise

For the set $N = \mathbb{N}^*$ with **0** = 0, define a successor function S such that Axioms (P1) and (P2) are satisfied but Axiom (P3) is not satisfied. Producing such an example shows that Axiom (P3) cannot be proved using the first two axioms alone. I suggest you follow these steps:

1. Specify $S(n)$ for each $n \in N$ (perhaps by writing down a formula).
2. Show that your choices satisfy (P1) and (P2). (If you can't do this, then you need make different choices for S .)
3. Produce an example of a subset $A \subset N$ such that $A \neq N$ but which satisfies the two bulleted properties in Axiom (P3). (If you can't do this, then you need make a different choice for S .)

The next exercise shows that if we have one choice of $(N, \mathbf{0}, S)$ satisfying the Peano axioms, then we can create other choices.

2.4.8 Exercise

Suppose that $(N, \mathbf{0}, S)$ satisfies the Peano axioms. Let $N' = \{n \in N : n \neq \mathbf{0}\}$. Prove that $(N', S(\mathbf{0}), S)$ also satisfies the Peano axioms.

Mathematicians differ as to whether or not 0 “should” be considered a natural number. In this text, we do not consider 0 as a natural number (so $\mathbb{N} = \{1, 2, 3, \dots\}$ not $\{0, 1, 2, 3, \dots\}$.) The previous exercise shows that whether or not we consider 0 to be a natural number doesn’t really matter, as long as we are consistent. To help us be consistent throughout the text, we let $\mathbb{N}^* = \{0, 1, 2, 3, \dots\}$. Henceforth, we will assume that there is a set \mathbb{N}^* (called the **extended naturals**), an element $0 \in \mathbb{N}^*$, and a choice of successor function S such that $(\mathbb{N}^*, 0, S)$ is a natural number system; though in Chapter 6, we will show that this assumption is actually a consequence of other axioms. We define $\mathbb{N} = \{n \in \mathbb{N}^* : n \neq 0\}$ and $1 = S(0)$ and observe (via the previous exercise) that $(\mathbb{N}, 1, S)$ is a natural number system.

In what follows, we outline how the most important properties of \mathbb{N}^* and \mathbb{N} follow from the Peano Axioms. In particular, any statement which is true for \mathbb{N}^* or \mathbb{N} can be converted into a true statement for any other natural number system. *What matters is not what we call the numbers, but what their properties are!* Since the content of these proofs is not tremendously important for what follows and since we have not yet explained basic logic or how proofs are written, you

are encouraged to just give the best explanations you can for the following results and to return to them later when you have a better understanding of proof techniques. We give some hints as to how your explanation might be structured.

In \mathbb{N}^* , every number except for 0 is one more than another element of \mathbb{N}^* . Here is the analogous statement for any natural number system.

2.4.9

Theorem ▶ All non-zero elements have predecessors

Let $(N, \mathbf{0}, S)$ be a natural number system. Every $m \in N$, other than the initial object, has a unique predecessor. That is, if $m \in N$ with $m \neq \mathbf{0}$, then there exists a unique element $n \in N$ such that $S(n) = m$.

The first part of the proof shows that such a predecessor exists and the second part shows that it is unique. The kind of proof used in the first part is called a “proof by contradiction.” We will study this more in Chapter 4. The basic idea is to assume that what we are trying to prove is false and then do some work to encounter a logical contradiction. The logical contradiction implies that our initial assumption must be false, and so what we are trying to prove must be true.

Proof. We prove existence using a proof by contradiction. Assume that there is an element $m \in N$ such that $m \neq \mathbf{0}$ and such that there is no element $n \in N$ with $S(n) = m$. We will contradict Axiom (P3), by constructing a counting subset $A \subset N$ such that $\mathbf{0} \in A$ and $A \neq N$.

Define $A = \{n \in N : n \neq m\}$. Notice that since $m \in N$ and $m \notin A$, $A \neq N$.

⟨ Explain why A is a counting subset of N . ⟩

Since A satisfies the hypotheses of Axiom (P3), by that axiom, $A = N$. Since the statements $A \neq N$ and $A = N$ contradict each other, our initial assumption must be false. Thus, for every $m \in N$, either $m = \mathbf{0}$ or there exists $n \in N$ such that $S(n) = m$.

Finally, let $m \in N$ and suppose that there exist elements $a, b \in N$ such that $S(a) = m$ and $S(b) = m$.

⟨ Explain how one of the Peano axioms implies $a = b$. ⟩

Thus, for each $m \in N$, other than $\mathbf{0}$, there is a unique element $n \in N$ such that $S(n) = m$. □

The previous theorem shows that every element of N , except for $\mathbf{0}$, has a unique predecessor. Given some $m \in N$, other than $\mathbf{0}$, we can find its predecessor. Either that predecessor is $\mathbf{0}$, or it also has a predecessor. We might worry that it is possible to find an infinite regress of predecessors for some element of N . If it were, N would be very different from our familiar \mathbb{N}^* . The next result shows that this is not possible. In other words, every element of N can be obtained from $\mathbf{0}$ by applying the successor function repeatedly.

2.4.10

Theorem

Suppose that $(N, \mathbf{0}, S)$ is a natural number system. There is no non-empty subset $B \subset N$ such that for each $b \in B$, the element b has a predecessor that is also an element of B .

Again, we do a proof by contradiction.

Proof. Assume, to achieve a contradiction, that there is such a subset B . Let $A = \{n \in N : n \notin B\}$.

⟨ Show that A is a counting subset of N . ⟩

Thus, by Axiom (P3), $A = N$. Hence, $B = \emptyset$, which contradicts the assumption that B is non-empty. Therefore, there is no non-empty subset B of N such that for each $b \in B$, $b \neq \mathbf{0}$ and $P(b) \in N$. \square

Arithmetic with natural number systems

Our results so far show that we can get to every element of N by starting with $\mathbf{0}$ and repeatedly taking successors. As an indication of how to show that every natural number system $(N, \mathbf{0}, S)$ has the same properties as N , we explain how to add numbers in N , using only the information available to us from the Peano axioms. This program was first developed by Richard Dedekind¹ in 1888 [55]. We use bold-face to denote elements of N ; they may not literally be elements of \mathbb{N}^* , though they have identical roles.

First we define what it means to add with $\mathbf{0}$:

2.4.11

Definition ▶ Adding Zero

For every $n \in N$, define $n + \mathbf{0} = n$.

This definition tells us that adding by zero on the right does what we expect. We haven't yet defined what it means to add by zero on the left. Having defined what it means to add zero, we now define what it means to add one. For convenience, we also define subtraction by 1. Recall that by Theorem 2.4.9, all elements n of N other than $\mathbf{0}$ have a predecessor $P(n)$.

¹Richard Dedekind (1831-1916) developed and promoted Cantor's set theory, as well as doing significant foundational work in number theory.

2.4.12

Definition ► Adding One

Define $\mathbf{1} = S(\mathbf{0})$ and for $n \in N$, define

$$n + \mathbf{1} = S(n).$$

That is, adding one is the same as finding the successor. Similarly, for $n \neq \mathbf{0}$, define

$$n - \mathbf{1}$$

to be the predecessor of n .

Observe that $\mathbf{0} + \mathbf{1}$ is defined to be $S(\mathbf{0})$ in Definition 2.4.12 and $S(\mathbf{0}) = \mathbf{1}$ by Definition 2.4.12. Thus, $\mathbf{0} + \mathbf{1} = \mathbf{1}$, which is what we want.

2.4.13

Exercise

Use the definitions to show that for every $n \in N$,

$$(n + \mathbf{1}) - \mathbf{1} = n$$

and for all $n \in N$, such that $n \neq \mathbf{0}$,

$$(n - \mathbf{1}) + \mathbf{1} = n.$$

We can now give names to other elements of N . This is what we did earlier when we began at an element of N and followed arrows. Define:

- $\mathbf{2} = S(\mathbf{1}) = \mathbf{1} + \mathbf{1}$,
- $\mathbf{3} = S(\mathbf{2}) = \mathbf{2} + \mathbf{1}$,
- $\mathbf{4} = S(\mathbf{3}) = \mathbf{3} + \mathbf{1}$,
- etc.

Finally, we define the addition of numbers other than $\mathbf{0}$ and $\mathbf{1}$.

2.4.14

Definition ► Adding other natural numbers

For $a, b \in N$ with $b \neq \mathbf{0}, \mathbf{1}$, define

$$a + b = (a + (b - \mathbf{1})) + \mathbf{1}.$$

Notice that our definition of $a + b$ requires that we already know how to define $(a + (b - \mathbf{1}))$. This is an example of a recursive definition. We'll explore these more in Chapter 9. We don't yet know that $+$ (as defined for elements of N) is commutative or associative. Before thinking about those properties, we work a few examples to build our intuition.

2.4.15

Example

We calculate $5 + 2$. Since 2 is not 0 or 1 , we use Definition 2.4.14. Recall that since $S(1) = 2$, we have $2 - 1 = 1$. Thus,

$$\begin{aligned} 5 + 2 &= 5 + (2 - 1) \\ &= (5 + 1) + 1. \end{aligned}$$

By definition, $6 = 5 + 1$, so

$$5 + 2 = 6 + 1.$$

By definition, $7 = 6 + 1$. Thus,

$$5 + 2 = 7,$$

as expected!

2.4.16

Example

We calculate $5 + 3$. Since 3 is not 0 or 1 , we use Definition 2.4.14. Recall that since $S(2) = 3$, we have $3 - 1 = 2$. Thus,

$$\begin{aligned} 5 + 3 &= (5 + (3 - 1)) \\ &= (5 + 2) + 1. \end{aligned}$$

In the previous example, we showed that $5 + 2 = 7$. Thus,

$$5 + 3 = 7 + 1,$$

which equals 8 by the definition of 8 .

2.4.17

Exercise

Prove that $2 + 2 = 4$.

If we were keen to show that all the elementary school math we've learned follows from these axioms we would go on to prove that addition is commutative (i.e. that for all $a, b \in N$, $a + b = b + a$) and associative (i.e. that for all $a, b, c \in N$, $(a + b) + c = a + (b + c)$). For $a, b \in N$, we can define $a \leq b$ if there is an $m \in N$ such that $a + m = b$. If there is such an m , we say that $b - a = m$. We would then want to show that if $a \leq b$ and if $c \in N$, then $a + c \leq b + c$. Similarly, if $a + c \leq b + c$ then $a \leq b$. As you can imagine, those proofs can be quite involved and should really wait until after we've explained logic and proof techniques more thoroughly! In this text, however, we won't spend any more time developing basic arithmetic from axioms – we have better things to do! I assure you, however, that it can be done! See [41, Chapter 1.2] or [101, Chapter 1], where these issues are put into a larger philosophical context.

2.5 Application: Symmetry Groups

"All of mathematics is the study of symmetry, or how to change a thing without really changing it ... It is symmetry, then, in its various forms, which underlies the orderliness, laws, and rationality of the universe, and thereby also the language of mathematics."

- H.S.M. Coxeter¹

What does it mean for an object to be symmetric? Is there more than one way for an object to be symmetric? How many symmetries does a square have? How many symmetries does a circle have? Does a sphere have more symmetries than a circle? Is it more symmetric? In what sense? We can use the notion of a group to investigate symmetries mathematically².

To give the most general definition of a symmetry, we need to leave mathematics³ to give a definition in which not every term is precisely defined:

2.5.1

Informal Definition

Suppose that X is an object with some sort of structure. A **symmetry** of X is an invertible structure-preserving transformation of X . Two symmetries are **the same** if they transform each point of X in exactly the same way. By saying that transformation is "invertible," we mean that there is always another structure-preserving transformation returning the object to its original state.

Metric spaces provide a natural setting for discussing symmetries, as we can consider all invertible transformations of the metric space which preserve distance. We'll wait until we have discussed abstract functions in more detail before taking up that idea, however. For now, we will consider only transformations of subsets of the plane \mathbb{R}^2 which preserve Euclidean distance. For example, the symmetries of a square consist of four counter-clockwise rotations (by 0° , 90° , 180° , and 270°) and four reflections, as in Figure 2.7.

Symmetries play an important role in chemistry. For example, if a molecule admits a reflection as a symmetry then it is **achiral**⁴. Molecules that are not achiral are **chiral**. A chiral molecule may have very different properties from the molecule which is its mirror image. For example, the mirror image of a sugar molecule is used as a sugar substitute and the symmetries and asymmetries of naturally occurring and synthetic molecules play an important role in the Dorothy L. Sayers mystery *The Documents in the Case*.

¹H.S.M. Coxeter (1907 - 2003) was responsible for mathematicians' rediscovery of the joy of Euclidean geometry and symmetry. He wrote and published research papers up until his death, proving by example that age need not be an obstruction to being a mathematician.

²In what follows, we'll assume some familiarity with functions whose domain and codomain are the plane \mathbb{R}^2 and with function composition. Anyone who has taken two semesters of Calculus should be okay. Otherwise, come back to this section after reading Chapter 8.

³Don't worry! We'll be back momentarily.

⁴More precisely, if a reflected version of the molecule can be translated and rotated through space to coincide with the original then the molecule is achiral.

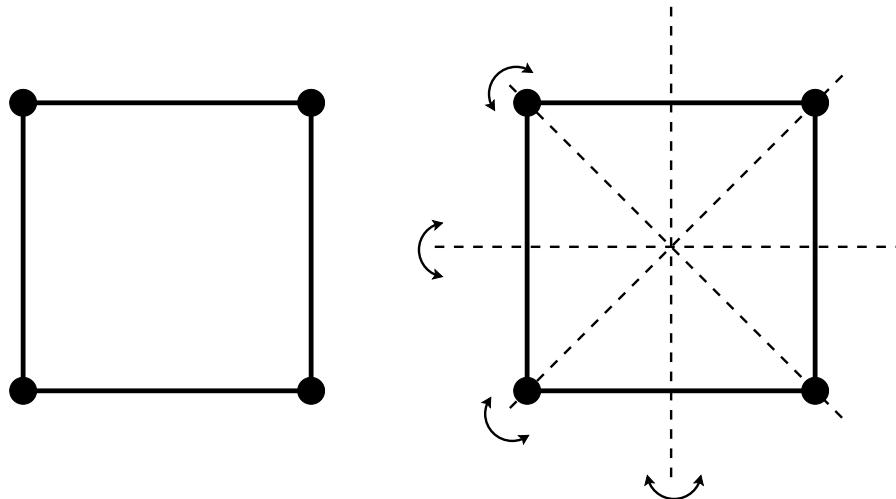


Figure 2.7: The four bilateral symmetries of a square

2.5.2 Example

Symmetry also plays an important role in art, both decorative and otherwise. What symmetries are present in Figure 2.8?

While symmetry in decorative art can lend a pleasing calmness, too much symmetry in non-decorative art leads to monotony. Artists will naturally find ways to suggest the presence of symmetry and then break the pattern. For example, Figure 2.9 shows circular ripples expanding outwards. Of course, we observe the rotational symmetries inherent in the picture, but the expanding ripples also seem to imbue the picture with a sense of symmetry. The symmetry of the ripples is “broken” by angle at which the photo is taken, so that the ripples do not appear as circles (with their many symmetries) but rather as ellipses (with their many fewer symmetries.)

Observe that whatever our object X is, if we “do nothing” we have a transformation preserving the structure of X . It is its own inverse. If S and T are symmetries of X , then the transformation $S \circ T$ obtained by first performing the symmetry T and then performing the symmetry S will also preserve the structure of X . Finally, notice that we are only considering *invertible* transformations of X and so axioms (G1) - (G3) hold for the set $\text{SYM}(X)$ of symmetries of X . Once we formalize this by discussing functions, we will also be able to conclude that the operation \circ is associative and so $\text{SYM}(X)$ is a group with operation \circ .

2.5.3 Example

Let X be the subset of \mathbb{R}^2 consisting exactly of all the points which lie on a circle centered at the origin and of radius 2^n for some n . A portion of the set X is depicted in Figure 2.9. Every symmetry of X is either a rotation of \mathbb{R}^2 about the origin, a reflection of \mathbb{R}^2 across a line through the origin, or a function of the form $f(x, y) = (2^n x, 2^n y)$ for some $n \in \mathbb{Z}$, or a combination

2.5.3

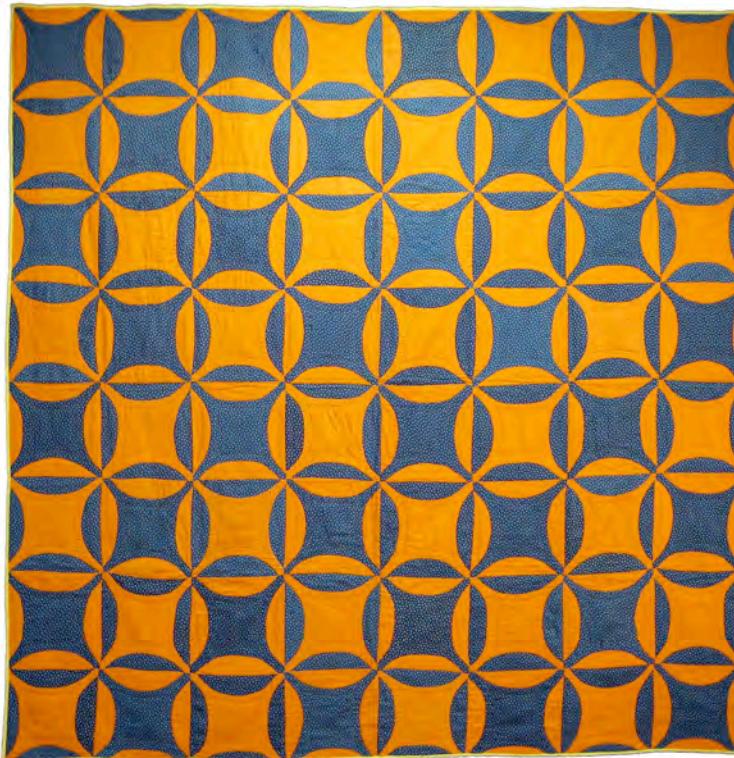


Figure 2.8: A quilt from the Pilgrim/Roy collection. Photo from quiltmuseum.org

of these.

2.5.4

Exercise

Let G be the set of functions of \mathbb{R}^2 to itself of the form $f(x, y) = (2^n x, 2^n y)$ for some $n \in \mathbb{Z}$. Verify that G is a group with function composition as the operation. (For the purposes of this exercise, you may omit verifying that associativity holds.) The group G is a subgroup of the group of symmetries of the set X from the previous example.

Given an object X (perhaps a work of art or piece of music or a molecule) we can attempt to determine the group of the symmetries of X . But we can also use groups to *create* interesting objects. For example, if G is a group whose elements are functions of \mathbb{R}^2 to itself (with group operation function composition), then we can create a design by starting with a point $(x_0, y_0) \in X$ and then defining the set X whose elements are all points $(x, y) \in \mathbb{R}^2$ such that there is some function $g \in G$ with $g(x_0, y_0) = (x, y)$.

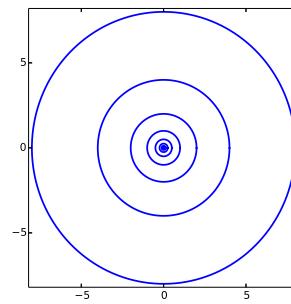


Figure 2.9: Concentric circles exhibit symmetry under scaling. The photo on the left is by Gian Luigi Perrella on Flickr. Used by permission under the creative commons license.

2.5.5 Example

Let G be the set of functions of \mathbb{R}^2 to itself, such that if $g \in G$, then there exist $n, m \in \mathbb{Z}$ such that $g(x, y) = (x + n, y + m)$. Letting $(x_0, y_0) = (0, 0)$, observe that, for all $n, m \in \mathbb{Z}$, $g(x_0, y_0) = (n, m)$. Then $X = \mathbb{Z} \times \mathbb{Z} \subset \mathbb{R}^2$, as on the left of Figure 2.10.

Of course, this image X is not terribly interesting. But then we have not chosen a particularly interesting group. The next example gives a hint of what we can obtain if we choose a more interesting group. The resulting design gives the sense of symmetry, but does not admit any of the usual translation, reflection, or rotation symmetries of \mathbb{R}^2 .

2.5.6 Example

Define the following functions. Let f be the function which rotates \mathbb{R}^2 by an angle of $\pi/12$ and then scales in the x coordinate by .9 and in the y coordinate by .85. Let g be the rotation by an angle of $\pi/12$. We let G be group whose elements consist of all functions that are the composition of the result of composing f , g , and their inverses some number of times. A portion of the resulting design X , for an initial starting point (x_0, y_0) , is shown on the right of Figure 2.10.

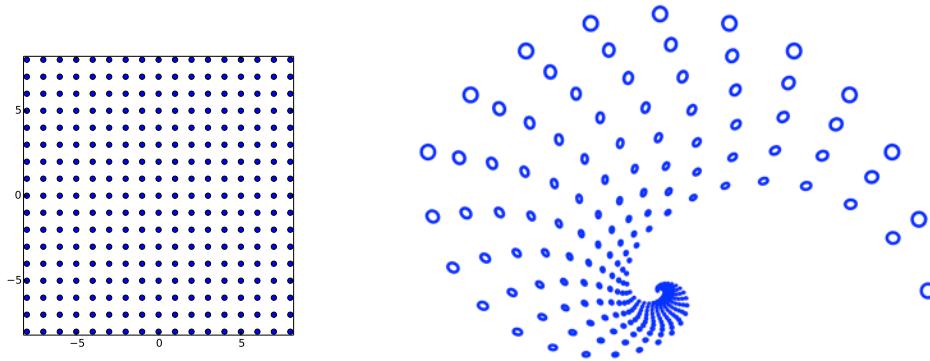


Figure 2.10: On the left is the integer lattice X in \mathbb{R}^2 from Example 2.5.5. On the right is a design obtained by applying f and g from Example 2.5.6 to a small circle some distance from the origin.

2.6 Appendix: Euclidean metric

In this appendix, we prove that \mathbb{R}^n with the euclidean metric is actually a metric space. We will not use the methods of proof elsewhere in the text. Throughout we let $\mathbf{x} = (x_1, \dots, x_n)$, $\mathbf{y} = (y_1, \dots, y_n)$ and so forth. Each entry in the list is a real number and $\mathbf{x} = \mathbf{y}$ if and only if $x_1 = y_1, x_2 = y_2$, etc.

The **euclidean metric** on \mathbb{R}^n is defined by:

$$d(\mathbf{x}, \mathbf{y}) = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2 + \dots + (x_n - y_n)^2}.$$

Observe that it is immediate from the definition that the euclidean metric on \mathbb{R}^n is positive, definite, and symmetric. We need to show that it satisfies the triangle inequality. We begin with some lemmas that simplify the situation.

2.6.1

Lemma ▶ Translation doesn't change distance

Suppose that $\mathbf{a} \in \mathbb{R}^n$. Then for all $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$,

$$d(\mathbf{x}, \mathbf{y}) = d(\mathbf{x} - \mathbf{a}, \mathbf{y} - \mathbf{a})$$

Recall that for vectors $\mathbf{a} = (a_1, \dots, a_n)$ and $\mathbf{b} = (b_1, \dots, b_n)$, we define

$$\mathbf{a} \cdot \mathbf{b} = a_1 b_1 + \dots + a_n b_n$$

The following facts are straightforward to prove from the definition:

2.6.2

Lemma

Suppose that $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{R}^n$ and that $k \in \mathbb{R}$ then

- $\mathbf{a} \cdot \mathbf{b} = \mathbf{b} \cdot \mathbf{a}$
- $(k\mathbf{a}) \cdot \mathbf{b} = k(\mathbf{a} \cdot \mathbf{b}) = \mathbf{a} \cdot (k\mathbf{b})$.
- $\mathbf{a} \cdot (\mathbf{b} + \mathbf{c}) = \mathbf{a} \cdot \mathbf{b} + \mathbf{a} \cdot \mathbf{c}$
- $\mathbf{a} \cdot \mathbf{a} = (d(\mathbf{a}, \mathbf{0}))^2$
- $\mathbf{a} \cdot \mathbf{b} = d(\mathbf{a}, \mathbf{0})d(\mathbf{b}, \mathbf{0}) \cos \theta$ where $\theta \in [0, \pi]$ is the angle between the vectors \mathbf{a} and \mathbf{b} , measured in the plane containing them and $\mathbf{0}$.
- $(d(\mathbf{a}, \mathbf{b}))^2 = (\mathbf{a} - \mathbf{b}) \cdot (\mathbf{a} - \mathbf{b}) = d(\mathbf{a} - \mathbf{b}, \mathbf{0})$.

2.6.3

Lemma

Suppose that $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{R}^n$, then

$$d(\mathbf{x}, \mathbf{z}) \leq d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z}).$$

Proof. Let $\mathbf{a} = \mathbf{x} - \mathbf{y}$ and $\mathbf{b} = \mathbf{z} - \mathbf{y}$. By Lemma 2.6.2,

$$\begin{aligned} d(\mathbf{a}, \mathbf{0}) &= d(\mathbf{x}, \mathbf{0}) \\ d(\mathbf{a}, \mathbf{b}) &= d(\mathbf{x}, \mathbf{z}) \\ d(\mathbf{0}, \mathbf{c}) &= d(\mathbf{y}, \mathbf{z}). \end{aligned}$$

Thus, it suffices to show that $d(\mathbf{a}, \mathbf{b}) \leq d(\mathbf{a}, \mathbf{0}) + d(\mathbf{0}, \mathbf{b})$.

We have

$$\begin{aligned} (d(\mathbf{a}, \mathbf{b}))^2 &= (\mathbf{b} - \mathbf{a}) \cdot (\mathbf{b} - \mathbf{a}) \\ &= \mathbf{b} \cdot \mathbf{b} - 2\mathbf{a} \cdot \mathbf{b} + \mathbf{a} \cdot \mathbf{a} \\ &\leq (d(\mathbf{0}, \mathbf{b}))^2 + (d(\mathbf{a}, \mathbf{0}))^2 \\ &\leq (d(\mathbf{0}, \mathbf{b}) + d(\mathbf{a}, \mathbf{0}))^2 \end{aligned}$$

Taking the square roots of both sides,

$$d(\mathbf{a}, \mathbf{b}) \leq d(\mathbf{0}, \mathbf{b}) + d(\mathbf{a}, \mathbf{0}),$$

as desired. □

2.6.4

Corollary

The euclidean metric on \mathbb{R}^n is a metric.

3 | Logic

Key Terms

- statement, predicate, free variable
- existential and universal quantifiers
- negation, conjunction, disjunction
- implication, hypothesis, conclusion, contrapositive, converse, equivalent statements
- Russell's paradox

"Logic inquires into the form of thought, as separable from and independent of the matter thought on."

- Augustus De Morgan [37]

In the previous chapter we encountered some of the basic structures of mathematics: sets, the natural numbers, groups, metric spaces, and graphs. As we began to explore those structures, we encountered words like "unique" and phrases like "if ... then" Before we can go any further in our explorations, we need to set out the basic elements constituting a logical argument. In this chapter we briefly summarize the essential concepts from logic that we need. In the interests of clarity for the beginning mathematician, we do not give completely thorough definitions.

3.1 Statements, predicates, and quantifiers

“To put this idle time to use and at the same time to occupy faculty members who were themselves idle, many of the troops were sent to colleges ... One day, one of them had a question: ‘I don’t understand what x is.’ The question was far more profound than he suspected, but I did not attempt to explain why.”

-André Weil¹, describing teaching elementary mathematics in the U.S. in 1943-44. [132]

- 3.1.1 A **statement** is a sentence that is unambiguously true or false but not both. A **free variable** is a symbol that can take on different meanings (usually representing the possible elements of a particular specified set). If we remove ambiguity from the free variable by saying exactly what it is, we say that we **specify** or **bind** the free variable. A sentence with free variables that becomes a statement once the free variables are bound is called a **predicate** or **conditional statement**.

3.1.2 Example ► (Examples of Statements and Predicates)

The sentence “Colby College is an academic institution.” is a statement (subject to some potential minor ambiguity about what the words “academic” or “institution” mean). The sentence “Colby is a boy” is a predicate since there are many people named Colby. However, if the speaker has a particular person named Colby in mind, then the variable “Colby” is bound to that individual.

The sentence “The number 5 is even” is a statement. The sentence “The number x is even” is a predicate.

The sentence “The number 17 is ugly” is not a statement or a predicate since “ugly” is ambiguous.

- 3.1.3 If x is a free variable, then we can denote a predicate with free variable x by writing $P(x)$ (or $Q(x)$, etc.). Apart from specifying a particular value for a free variable, there are two other common ways of binding a free variable: the **universal quantifier** \forall (pronounced “for all”) and the **existential quantifier** \exists (pronounced “there exists”). If $P(x)$ is predicate, then “ $\forall x, P(x)$ ” is the statement that, no matter how we bind x , the statement $P(x)$ is true. If $P(x)$ is a predicate, then “ $\exists x$ such that $P(x)$ ” is the statement that there is some x such that $P(x)$ is true.

¹André Weil (1906-1998) was one of the most influential mathematicians of the twentieth century. Weil himself went to great lengths to avoid serving in the military during the war, so his disdain for teaching those who did sit poorly. His sister Simone Weil was a well-known philosopher and mystic. She is quoted elsewhere in this text.

3.1.4

Example ▶ (Universal and Existential Quantifiers)

The statement: “For all real numbers x , $x^2 \geq 0$ ” is a true statement which contains the universal quantifier. We can rephrase it by saying “For every real number x , $x^2 \geq 0$.”

The statement: “There is a real number x , such that $x^2 = 0$ ” is a true statement which contains the existential quantifier. We can rephrase it as: “Some real number x has the property that $x^2 = 0$ ”.

The statement: “Every natural number is the sum of three prime numbers” is a statement which contains the universal quantifier. It is false, since the number $n = 1$ is a natural number which is not the sum of three prime numbers.

The statement: “Some natural number n has the property that $n^2 < 0$ ” is a statement with an existential quantifier. It is false, since *every* natural number n has the property that $n^2 \geq 0$.

3.2 Conjunctions, and Disjunctions

“Now logic while it is the science of reasoning in general is in a more especial sense the science of reasoning by signs. It investigates the forms and expressions to which correct reasoning may be reduced and the laws upon which it is founded.”

- George Boole¹

Given one or more statements, we can combine them to create new statements.

- If P and Q are statements, the statement $P \wedge Q$ (read P **and** Q) is the statement which is true exactly when both P and Q are true. (This is called the **conjunction** of P and Q)
- If P and Q are statements, the statement $P \vee Q$ (read P **or** Q) is the statement which is true exactly when *at least one and possibly both* of P and Q are true. (This is called the **disjunction** of P and Q .)

3.2.1

Example

Let P be the statement “Douglas Adams writes a book” and Q be the statement “I eat lunch at the restaurant at the end of the universe.”

- The conjunction of P and Q is: “Douglas Adams writes a book and I eat lunch at the restaurant at the end of the universe.”

¹George Boole (1815-1864) studied the nature of logic and developed analogies with arithmetic. His work forms the basis of the theory underlying electronic circuits, such as those in computers. The quotation is from [19]

- The disjunction of P and Q is: “Douglas Adams writes a book or I each lunch at the restaurant at the end of the universe.”

3.2.2

Example

Let P be the statement “Some sperm whales eat giant squid” and let Q be the statement “Some scientists eat giant squid.” Both P and Q are true statements.

- Thus the conjunction $P \wedge Q$, which is “Some sperm whales eat giant squid and some scientists eat giant squid,” is a true statement.
- Also, the disjunction $P \vee Q$, which is “Some sperm whales eat giant squid or some scientists eat giant squid,” is a true statement.

3.2.3

Example

Let P be the statement “Some tube worms live in environments toxic to humans.” Let Q be the statement “The author of this textbook has eaten a tube worm for breakfast.” The statement P is true while the statement Q is false.

- The conjunction $P \wedge Q$ is “Some tube worms live in environments toxic to humans and the author of this textbook has eaten a tube worm for breakfast.” It is a false statement since Q is false.
- The disjunction $P \vee Q$ is “Some tube worms live in environments toxic to humans or the author of this textbook has eaten a tube worm for breakfast.” It is a true statement since P is true.

3.2.4

Example

Let P be the statement “All porpoises live in an aquarium.” Let Q be the statement “Porpoises write self-help books in English.” Both P and Q are false.

- The conjunction $P \wedge Q$ is “All porpoises live in an aquarium and porpoises write self-help books in English.” It is a false statement since P is false. We could equally well say it is a false statement since Q is false.
- The disjunction $P \vee Q$ is “All porpoises live in an aquarium or porpoises write self-help books in English.” It is also a false statement since both P and Q are false.

We can summarize the relationship between the truth values of the original statements and the truth values of the new statements in a table (called a **truth table**). In a truth table we list all possible truth values of the original statements and

then deduce the corresponding truth values of the composite statements. Observe that no matter what the statements P and Q are the truth value of $P \wedge Q$ will be the same as the truth value of $Q \wedge P$ and the truth value of $P \vee Q$ will be the same as the truth value of $Q \vee P$. This helps us be slightly more concise when analyzing truth values. In the truth table below, we consider the combinations of 3 statements, P , Q , and R .

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

3.2.5 Exercise

Fill in the missing spots in the truth table above.

In completing the previous exercise, you should have discovered that $(P \wedge Q) \vee R$ and $(P \vee R) \wedge (Q \vee R)$ always have the same truth values as each other, no matter what the truth values of P , Q , and R . We say that the statements $(P \wedge Q) \vee R$ and $(P \vee R) \wedge (Q \vee R)$ are **logically equivalent**.

3.2.6 Exercise

In the previous truth table, find another pair of logically equivalent statements.

3.2.7 Exercise

Determine the truth value of the following statements and give as complete an explanation as you can for your answer.

1. $-7 < 0$ and $7^2 > 0$.
2. $-7 \geq 0$ or $7^2 \leq 0$.
3. For all real numbers x , $-x < 0$ and $x^2 > 0$.
4. $7 < 0$ or $7^2 > 0$.
5. For all real numbers x , $x < 0$ or $x^2 > 0$.

6. There exists a real number x such that $x < 0$ and $x^2 > 0$.

3.2.8

Exercise

Do the following two statements have the same truth values? Why or why not? What does this say about the relationship between quantifiers and conjunctions and disjunctions?

- There exists $n \in \mathbb{N}$ such that n is even and n is odd.
- There exists $n \in \mathbb{N}$ such that n is even and there exists $n \in \mathbb{N}$ such that n is odd.

3.2.9

Warning

In the statement

- There exists $n \in \mathbb{N}$ such that n is even and there exists $n \in \mathbb{N}$ such that n is odd.

the two occurrences of n can refer to different numbers. It would be much better to use different symbols to refer to them. Like so:

- There exists $n \in \mathbb{N}$ such that n is even and there exists $m \in \mathbb{N}$ such that m is odd.

This will help ensure that if we use the statement later, we don't get confused and start working with some n that we believe to be both even and odd.

3.2.10

Exercise

Do the following two statements have the same truth values? Why or why not? What does this say about the relationship between quantifiers and conjunctions and disjunctions?

- For every $x \in \mathbb{R}$, $x > 0$ or $x \leq 0$.
- For every $x \in \mathbb{R}$, $x > 0$ or for every $x \in \mathbb{R}$, $x \leq 0$.

We conclude with one other warning about the word “and.”

3.2.11

Warning ▶ English vs. Mathematese

Not every use of the word “and” indicates the conjunction of two statements.

3.2.12

Example

Consider the statement:

- For every a, b , and c which are elements of \mathbb{R} , $a + b + c$ is an element of \mathbb{R} .

This statement can be rephrased as:

- For every $a, b, c \in \mathbb{R}$, $a + b + c$ is an element of \mathbb{R} .

We can even rewrite it as:

- $\forall a, b, c \in \mathbb{R}, a + b + c \in \mathbb{R}$.

Either of these ways of rewriting the original indicate that the “and” was not signifying the conjunction of two statements. Furthermore, the phrase “For every a, b ” is not a statement nor is

$$“c \in \mathbb{R}, a + b + c \in \mathbb{R}.”$$

This is another indication that the “and” is not the conjunction of two statements.

3.2.13

Example

Consider the statement (considering f to be some fixed function, not a free variable):

- The function f is increasing and differentiable.

The word “differentiable” is not by itself a statement, so at first glance it seems that the “and” does not indicate a conjunction. However, the statement can be rephrased as:

- The function f is increasing and the function f is differentiable,

which indicates that our original statement is the conjunction of two other statements.

The previous two examples concern the relationship between the English word “and” and the logical notion of “conjunction.” They show that thought is always required when working mathematically or logically with statements phrased in English. There is no hard-and-fast rule for determining when the English word “and” indicates a conjunction, but the follow rules-of-thumb may help:

- Can the statement be rephrased without the use of “and”? If so, it might not be a conjunction.

- Does the “and” show up after a quantifier, indicating the last item of a list? If so, it might not be a conjunction.
- How would the statement be disproved? Consider the statement (where f is some unspecified but fixed function):
 - The function f is increasing and differentiable.

If f strictly decreases at some point, the statement would be false. If f is not differentiable at some point, the statement would also be false. It could be that f is both non-increasing and non-differentiable, in which case the statement is also false. Since a conjunction $P \wedge Q$ is false whenever at least one of P or Q is false, this indicates that the “and” indicates a conjunction.

3.2.14

Exercise

Determine if the “and”s in the following statements indicate conjunctions, determine the truth values of each statement, and give a reason for your answer of “true” or “false.”

1. There exist real numbers x and y such that $x^2 + y^2 = 0$.
2. There exist $x, y \in \mathbb{R}$ such that $x > 0$ and $xy \leq 0$.
3. $7 > 0$, $-3 < 0$, and $7 + (-3) < 0$.
4. There exist real numbers x and y such that $x > 0$, $y < 0$, and $x+y < 0$.
5. For every choice of real numbers x and y such that $x > 0$ and $y < 0$, we have $x+y < 0$.

3.3 Negations

“Question 1: Do you want to reject the parts of a new law that would delay the use of ranked-choice voting in the election of candidates for any state or federal office until 2022, and then retain the method only if the constitution is amended by December 1, 2021, to allow ranked-choice voting for candidates in state elections?”

-Ballot question in Maine on June 12, 2018 [3]



Negations of simple statements

If P is a statement, then the **negation** of P , denoted $\neg P$ and pronounced “not P ”, is the statement with the opposite truth value of P .

3.3.1 Example

Let P be the statement:

- The Loch Ness Monster lives in the Mississippi River.

The statement $\neg P$ is the statement:

- It is not the case that the Loch Ness Monster lives in the Mississippi River.

We can rephrase $\neg P$ slightly more helpfully as:

- The Loch Ness Monster does not live in the Mississippi River.

3.3.2

Exercise

Complete the following truth table:

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

Negations of conjunctions and disjunctions

In many mathematical arguments, we need to be able to write the negation of a statement in a useful way. For example, if we claim that it is not the case that there exists an x such that $x > 0$ and $x < 7$, then we might do better to simply claim that for every x , $x \leq 0$ or $x \geq 7$. We note the following:

- If P and Q are statements, then the statement “ $\neg(P \text{ and } Q)$ ” is logically equivalent to the statement “ $(\neg P) \text{ or } (\neg Q)$.”
- If P and Q are statements, then the statement “ $\neg(P \text{ or } Q)$ ” is logically equivalent to the statement “ $(\neg P) \text{ and } (\neg Q)$.”

In other words, negating a statement toggles the “and”s and “or”s. This should be evident in your answers to Exercise 3.3.2. Generally, we will say that rephrasing $\neg(P \wedge Q)$ as $(\neg P) \vee (\neg Q)$ is writing “the negation of $P \wedge Q$ as positively as possible.” Likewise, rephrasing $\neg(P \vee Q)$ as $(\neg P) \wedge (\neg Q)$ is writing “the negation of $P \vee Q$ as positively as possible.”

3.3.3

Example

Consider the statement:

- R : $27 > 0$ and the function f is increasing,

where f is some fixed function. Writing the negation as positively as possible we obtain:

- $\neg R$: $27 \leq 0$ or the function f is non-increasing.

3.3.4

Exercise

Write the negations of the following statements as positively as possible. You do not have to know what all the mathematical terms refer to.

1. 26 is positive and $(-2, 16)$ is in the first quadrant of the Cartesian plane.
2. 6821 is prime or 6823 is composite.
3. The function $f(x) = \sin x$ has period $\pi/2$ and the function $g(x) = \cos x$ has period 2π .
4. The function $f(x) = x^2$ is concave up and increasing.
5. The unit disc is an open subset of the Cartesian plane or the unit disc is compact.
6. The real numbers e , π , and $\sqrt{2}$ are irrational, but the real number $27/3$ is rational.
7. $(26 > 0 \text{ or } 25 < 0)$ and $\sqrt{2}$ is rational.

Negations with quantifiers

While truth tables are helpful for analyzing the effect of negating conjunctions and disjunctions, they do not do a great job capturing the effect of negating statements with quantifiers. Nevertheless, some thought will show that negating also toggles “there exists” with “for all.”

- If $P(x)$ is a predicate, then $\neg(\forall x, P(x))$ is the statement $\exists x(\neg P(x))$.
- If $P(x)$ is a predicate, then $\neg(\exists x \text{ s.t. } P(x))$ is the statement $\forall x, (\neg P(x))$.

3.3.5

Warning

In everyday speech, people are often sloppy with the placement of the word “not” with respect to quantifiers. Consider the following two statements:

- All rectangles are not squares.
- Not all rectangles are squares.

The first statement is false because some rectangles are squares. The second statement is equivalent to the statement “There exists a rectangle that is not a square.” It is a true statement.

3.3.6

Example

Let P be the statement

- Every real number x is positive.

The statement $\neg P$ is:

- Some real number x is not positive.

3.3.7

Example

Let P be the statement

- There is a prime number larger than 20000.

The statement $\neg P$ is:

- All prime numbers are not larger than 20000.

3.3.8

Exercise

Negate the following statements, phrasing your answer as positively as possible. Consider x to be some fixed element.

1. $x \in A$ and $x \in B$
2. $x \in A$ or $x \in B$
3. For all $A \in \mathcal{A}$, $a \in A$.
4. There exists $A \in \mathcal{A}$, such that $a \in A$.

When negating a statement with multiple quantifiers, work from left to right, toggling the quantifiers.

3.3.9

Example

Negate the statement:

“For every $x \in X$ there exists $y \in Y$ such that for all $z \in Z$, $|xy| < z$.”

(Assume that X , Y , and Z are particular subsets of \mathbb{R} .)

Solution:

“There exists $x \in X$ such that for all $y \in Y$, there exists $z \in Z$ so that
 $|xy| \geq z$.”

Notice that the words “such that” are attached to “there exists”; indeed you should consider “there exists ... such that ...” to be one phrase. The words “for all” are not paired with “such that”.

3.3.10

Example

Negate the statement:

“For every $x > 0$ there exists $y < 0$ such that for all $z > 0$, $|xy| < z$.”

Solution:

“There exists $x > 0$ such that for all $y < 0$, there exists $z > 0$ so that
 $|xy| \geq z$.”

3.3.11

Warning

When you negate a statement with a quantifier, the kind of object being quantified does not change. In the solution to Example 3.3.9, the element x is still an element of X ; the element y is still an element of Y ; and the element z is still an element of Z . Likewise, in the solution to Example 3.3.10, we still have $x > 0$, $y < 0$ and $z > 0$.

When negating compound statements, work from the outside to the inside. Here are two examples involving both quantifiers and conjunctions and disjunctions.

3.3.12

Example

Negate the statement:

“For every $x \in X$, there exists $y \in Y$ such that $xy = 0$ and there exists $a \in X$ such that $a^2 > 100$.”

Of course, simply prefacing the previous statement with the words “It is not the case that”, gives a valid negation. To get something more useful, however, we progress in stages:

First attempt: We observe that the given statement is of the form $P \wedge Q$ where P is the statement:

P : “For every $x \in X$, there exists $y \in Y$ such that $xy = 0$ ”

and Q is the statement:

Q : “There exists $a \in X$ such that $a^2 > 100$.”

Since the negation of $P \wedge Q$ is $\neg P \vee \neg Q$, we arrive at:

“(It is not the case that for every $x \in X$, there exists $y \in Y$ such that $xy = 0$) or (it is not the case that there exists $a \in X$ such that $a^2 > 100$).”

Of course, the sentence is unwieldy, so we improve it by writing more useful negations of P and Q .

Second attempt:

“There exists $x \in X$ such that for all $y \in Y$, $xy \neq 0$ or for all $a \in X$, $a^2 \leq 100$.”

We can improve the readability by signalling to the reader at the beginning of the sentence that there will be an “or” later on. Making it read a little more naturally in English, we end up with:

“Either there is $x \in X$ such that for every $y \in Y$, $xy \neq 0$ or $a^2 \leq 100$, for every $a \in X$.”

3.3.13 Example

Negate the statement:

“Either there exists $n, m \in \mathbb{N}$ such that $n + m = 1000$ or $\frac{1}{n} < 15$ for every $n \in \mathbb{N}$; additionally for every $n \in \mathbb{N}$, $n^2 < 0$.”

Solution: The given statement is somewhat convoluted. To clarify the logical structure, we write it using logical symbols. The given statement is then:

$$\left((\exists n, m \in \mathbb{N}, n + m = 1000) \vee (\forall n \in \mathbb{N}, \frac{1}{n} < 15) \right) \wedge \left(\forall n \in \mathbb{N}, n^2 < 0 \right).$$

Negating, using logical symbols, we arrive at:

$$\left((\forall n, m \in \mathbb{N}, n + m \neq 1000) \wedge (\exists n \in \mathbb{N}, \frac{1}{n} \geq 15) \right) \vee \left(\exists n \in \mathbb{N}, n^2 \geq 0 \right).$$

Translating back into English, we arrive at:

“Either, for every $n, m \in \mathbb{N}$, $n + m$ is not equal to 1000 and there is some $n \in N$ such that $\frac{1}{n} \geq 15$, or there is some $n \in N$ such that n^2 is at least 0.”

which is unwieldy, but understandable.

3.3.14 Example

The point of this example is that when checking if an “and” is joining two statements, you may need to think about how the English sentence can be reworded to make it plain that an “and” is a conjunction. Consider:

“Some increasing function is continuous and differentiable.”

Obviously, the word “differentiable” is not, by itself a statement, but the statement can be reworded to make its logical structure plain:

“There exists an increasing function f such that f is continuous and f is

differentiable".

The negation of the statement is, therefore,

"For every increasing function f , either f is not continuous or f is not differentiable."

3.3.15 Exercise

Negate the following statements:

1. For all $x \in X$, there exists $H \in \mathcal{H}$, such that $x \in H$.
2. For all $x \in X$ and for all $H \in \mathcal{H}$, we have $x \in H$.
3. There exists $x \in X$ such that for all $H \in \mathcal{H}$, $x \in H$.
4. There exists $x \in X$ and there exists $H \in \mathcal{H}$, such that $x \in H$.

3.4 Implications

"While the contemplative trend of logical analysis does not represent all of mathematics, it has led to a more profound understanding of mathematical facts and their interdependence, and to a clearer comprehension of the essence of mathematical concepts."

- Courant and Robbins, *What is Mathematics? An elementary approach to ideas and methods.* [32]

Almost of all mathematics, both pure and applied, is about deducing the consequences of certain assumptions. While investigating the consequences of certain assumptions, we work under the presumption that those assumptions are true. If our work brings to light a consequence of our assumptions that is a false statement, then we may conclude that at least one of our assumptions was false. On the other hand, even if we deduce true statements, there is no guarantee that the assumptions themselves were true. For example, suppose, using tremendous feats of logic, we were able to deduce from the assumption "The moose is the largest of all aquatic creatures" the statement "The moose is a mammal". Although we have reached a true conclusion, our assumption is still false. But if we know that our assumption is true and that our assumption implies some conclusion, then we may be certain that our conclusion is also true.

We formalize this process with the notion of an implication. Implications are another way (besides conjunctions and disjunctions) of combining two statements to create a third.

Implications and their negations

- If P and Q are statements, the statement $P \Rightarrow Q$ (read P **implies** Q and called an **implication**) is the statement that is false exactly when P is true and Q is false. For the implication $P \Rightarrow Q$, the statement P is the **hypothesis** and the statement Q is the **conclusion**.
- If P and Q are statements, the **contrapositive** of $P \Rightarrow Q$ is $\neg Q \Rightarrow \neg P$.
- If P and Q are statements, the **converse** of $P \Rightarrow Q$ is $Q \Rightarrow P$.

If P and Q are statements, there are a variety of ways of reading the implication $P \Rightarrow Q$:

- $P \Rightarrow Q$ can be read as “ P implies Q .”
- $P \Rightarrow Q$ can be read as “if P then Q .”
- $P \Rightarrow Q$ can be read as “ P only if Q .”
- $P \Rightarrow Q$ can be read as “ P is sufficient for Q .”
- $P \Rightarrow Q$ can be read as “ Q is necessary for P .”

3.4.1 Exercise

Complete the following truth table:

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

Observe that the last two lines of the previous truth table confirm that $\neg(P \Rightarrow Q)$ is logically equivalent to $P \wedge (\neg Q)$. In particular, *the negation of an implication is not an implication; it is a conjunction!*

3.4.2 Example

Let P be the statement “Douglas Adams writes a book” and Q be the statement “I eat lunch at the restaurant at the end of the universe”.

- The implication $P \Rightarrow Q$ is: “If Douglas Adams writes a book, then I eat lunch at the restaurant at the end of the universe.” or “Douglas

Adams writes a book only if I eat lunch at the restaurant at the end of the universe.”

- 3.4.2
- The contrapositive of $P \Rightarrow Q$ is: “If I don’t eat lunch at the end of the universe then Douglas Adams doesn’t write a book.”
 - The converse of $P \Rightarrow Q$ is: “If I eat lunch at the restaurant at the end of the universe, then Douglas Adams writes a book.”
 - The negation of $P \Rightarrow Q$ is: “Douglas Adams writes a book and I don’t eat lunch at the restaurant at the end of the universe.”

3.4.3

Exercise

For each of the following implications, determine the truth value and write the converse and the contrapositive.

1. If $20 > 0$ then $3^2 + 4^2 = 5^2$.
2. If $20 < 0$ then $3^2 + 4^2 = 5^2$.
3. If $20 > 0$ then $3^2 + 4^2 \neq 5^2$.
4. If $20 < 0$ then $3^2 + 4^2 \neq 5^2$.

3.4.4

Exercise

Determine the truth values of the following statements and write their negations.

1. $27 > 0$ implies 19 is odd.
2. The fact that the function $f(x) = x$ is an increasing function implies that $g(x) = \cos x$ is differentiable. (You may assume that f and g are defined on all of \mathbb{R} and have the well-known properties from Calculus.)
3. If the moon is made of green cheese then 19 is a prime number.
4. If 19 is a prime number then the moon is made of green cheese.

3.4.5

Warning ▶ Negating and Implication

Some people find the method for negating an implication to be counter-intuitive. So we stress that *the negation of an implication is not an implication*, it is a conjunction.

Implication and predicates

In math, we often say things like: “If p is prime then p is odd” is a false statement. And yet, at face-value this is a ludicrous thing to say, since the sentence:

“If p is prime then p is odd.”

is not a statement, but a predicate with a free variable p . If we specify that $p = 3$, then it becomes a true statement and if we specify that $p = 2$ then the statement is false. Thinking about normal usage, it becomes apparent that when the mathematician says

“If p is prime then p is odd.”

what she means is really something along the lines of:

“For every natural number p , if p is prime then p is odd.”

The statement is false, as $p = 2$ is a counterexample. We (as most mathematicians) will thus make the following convention:

3.4.6

Warning ▶ Predicates and Implications

If P and Q are predicates, then $P \Rightarrow Q$ is, by convention, the *statement* obtained by using the universal quantifier to bind all the variables of P and Q . That is, $P(x) \Rightarrow Q(x)$ means $\forall x, P(x) \Rightarrow Q(x)$. For example, $(x \geq 0) \Rightarrow (x^3 \geq 0)$ is short hand for the statement

$$\forall x \in \mathbb{R}, (x \geq 0) \Rightarrow (x^3 \geq 0)$$

which is true.

Consequently, the negation of an implication involving predicates will be a conjunction containing an existential quantifier.

3.4.7

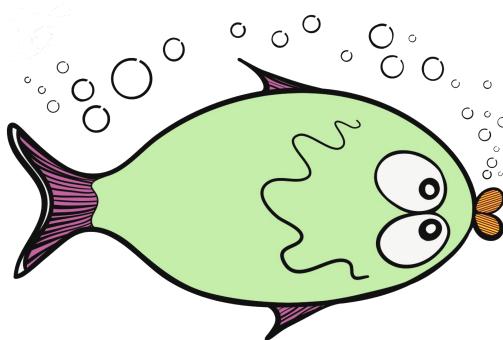
Example

The negation of the statement:

“If a fish lives in fresh-water, then it is a trout.”

is

“There is a fish that lives in fresh-water and is not a trout.”



3.4.8

Exercise

Write negations of the following implications. You do not need to know what all the terms mean.

1. If f is an increasing function, then f is differentiable.
2. If $x^2 < 0$, then x is not a real number.
3. If lines L and M are not parallel, then L and M intersect in exactly one point or $L = M$.
4. If $I \subset \mathbb{R}$ is a closed and bounded interval, then every continuous function $f: I \rightarrow I$ has a fixed point.

Implications and natural language

Example 3.4.7 is a good reminder that we use the language of implications frequently in every-day speech¹:

- “If I stay up late, then I fall asleep in class.”
- “If the earth is flat, then I am taking a math class.”
- “If I finish my homework, then I will call you.”

But as is always the case, we must be very careful when thinking about the relationship between mathematics and natural world. In particular, the conventions for handling implications in everyday language can be very different from the conventions in logic. Take the previous three statements in turn.

- “If I stay up late, then I fall asleep in class.” This sentence in everyday language communicates a causal relationship between staying up late and falling asleep in class. In mathematics and logic, however, the use of “if ... then ...” is not intended to communicate a causal relationship, only a logical one. Thus, a logician who ignores everyone else’s speech conventions,

¹I am heavily indebted to the excellent article [44] for these observations.

would say that the statement “If I stay up late, then I fall asleep in class.” is true even in the situation where she falls asleep in class whether or not she stays up late. Similarly, she would admit “If I stay up late tomorrow night, then I fell asleep in class yesterday.” as a valid statement which might be true or might be false.

- “If the earth is flat, then I am taking a math class.” In everyday speech, this sentence is close to nonsensical since the flatness (or not) of the earth has nothing to do with whether or not I am taking a math class. A logician, however, would say that the statement is true (indeed vacuously true) since the hypothesis is false and any implication with a false hypothesis is a true statement.
- “If I finish my homework, then I will call you.” In addition to the issues of causality and temporality mentioned in our first example, in everyday speech, this statement might well be taken to also include the sentiment that “If I don’t finish my homework, then I won’t call you.” That is, in everyday speech, implications stated in the form “ $P \Rightarrow Q$ ” are often understood to be logical equivalences $P \Leftrightarrow Q$. Unfortunately, in mathematics, this convention has lingered in the way definitions are often presented. For instance:

“We define q to be **rational** if there exists $a \in \mathbb{Z}$ and $b \in \mathbb{N}$ such that
$$q = a/b.$$
”

What we mean to say, however, is:

“We define q to be **rational if and only if** there exists $a \in \mathbb{Z}$ and $b \in \mathbb{N}$ such that $q = a/b.$ ”

How to prove an implication is true

The next observation is helpful when it comes time to prove implications.

3.4.9

Example

Suppose that P and Q are statements. The statement “ $P \Rightarrow Q$ ” is logically equivalent to “ $\neg P \text{ or } Q$.”

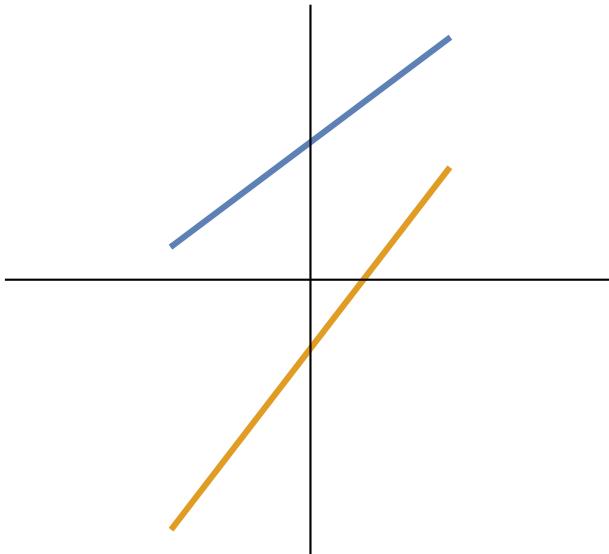


Figure 3.1: Portions of two lines L_1 and L_2 in \mathbb{R}^2 . Theorem 3.4.10 claims that since the lines L_1 and L_2 have different slopes, they will intersect at a unique point (x_0, y_0) .

3.4.9

Proof. We can show that “ $P \Rightarrow Q$ ” and “ $\neg P \vee Q$ ” always have exactly the same truth values by using a truth table where we list all the possible truth values for the two statements according to the truth values of P and Q .

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

Since the last two rows always take the same value, the two statements are logically equivalent. \square

The fact that $P \Rightarrow Q$ is logically equivalent to $(\neg P) \vee Q$ helps explain why the negation of $P \Rightarrow Q$ is $P \wedge (\neg Q)$. Furthermore, if we want to show that $P \Rightarrow Q$, we need only show that $\neg P \vee Q$. If $\neg P$ is true, we are done, so it suffices to *assume* P is true and show that from that assumption, we can deduce that Q is true. There are, however, other ways of proving an implication. We will explore these in next Chapter, but here is an example from Algebra to tide you over. See Figure 3.1 for an example.

3.4.10

Theorem

Let $m, b, a, c \in \mathbb{R}$ and let L_1 be the line in \mathbb{R}^2 with the equation $y = mx + b$ and let L_2 be the line in \mathbb{R}^2 with the equation $y = ax + c$. If $a \neq m$, then there is a unique point $(x_0, y_0) \in \mathbb{R}^2$ belonging to both L_1 and L_2 .

Proof. Assume that $a \neq m$. Let $x_0 = \frac{c-b}{m-a}$ and $y_0 = \frac{mc-ba}{m-a}$. We claim that (x_0, y_0) belongs to both L_1 and L_2 .

To see that $(x_0, y_0) \in L_1$, observe:

$$\begin{aligned} mx_0 + b &= \frac{m(c-b)}{m-a} + b \\ &= \frac{m(c-b) + b(m-a)}{m-a} \\ &= \frac{mc - ba}{m-a} \\ &= y_0. \end{aligned}$$

Since (x_0, y_0) satisfies the equation of L_1 , $(x_0, y_0) \in L_1$.

To see that $(x_0, y_0) \in L_2$, observe:

$$\begin{aligned} ax_0 + c &= \frac{a(c-b)}{m-a} + c \\ &= \frac{a(c-b) + c(m-a)}{m-a} \\ &= \frac{-ab + cm}{m-a} \\ &= y_0. \end{aligned}$$

Thus, $(x_0, y_0) \in L_2$.

Finally, we need to confirm that (x_0, y_0) is the unique point of \mathbb{R}^2 belonging to both L_1 and L_2 . To that end, assume (x, y) belongs to both L_1 and L_2 . We will show that $(x, y) = (x_0, y_0)$.

⟨ Do it! ⟩

□

3.4.11

Exercise

Suppose that C_1 is the circle with equation $x^2 + y^2 = 1$. Let C_2 be the circle with equation $(x - a)^2 + y^2 = 1$ for some $a \in \mathbb{R}$. Prove that if $a \in [0, 1]$ then there exists a point (x_0, y_0) belonging to both C_1 and C_2 . For what values of $a \in [0, 1]$, is the point (x_0, y_0) unique?

Equivalent statements

3.4.12

Previously we said that two statements P and Q were **equivalent** if they have the same truth values. Another way of saying this is that $P \Rightarrow Q$ and $Q \Rightarrow P$. We combine this to say that P and Q are equivalent statements if $P \Leftrightarrow Q$. We can read this as “ P if and only if Q ” or “ P is necessary and sufficient for Q .” The phrase “if and only if” is often abbreviated when writing as “iff.”

To prove that two statements P and Q are equivalent, we usually show that $P \Rightarrow Q$ and $Q \Rightarrow P$.

3.5 A remark on uniqueness

“The power which language gives us of generalizing our reasonings concerning individuals by the aid of general terms, is nowhere more eminent than in the mathematical sciences, nor is it carried to so great an extent in any other part of human knowledge.”

-Charles Babbage¹[11]

Finally, we observe that the uniqueness of a certain kind of element in a set can be expressed in logical terms. Look back over the proof of Theorem 3.4.10 for an example of how this definition is used in proofs.

3.5.1

Definition ▶ unique

If X is a set and if $a \in X$ and if $P(x)$ is a predicate, then to say that a is the **unique** element of X satisfying $P(x)$ means:

- $P(a)$ is true, and
- If $b \in X$ and $P(b)$ is true, then $a = b$.

The negation of the statement

Q : “ $x_0 \in X$ is the unique element of X with property P ”

(where x_0 is some fixed element of X) is thus

$\neg Q$: “Either x_0 does not have property P or there exists $y_0 \in X$ such that y_0 has property P and $x_0 \neq y_0$.”

¹Charles Babbage (1791-1871) is widely credited as the inventor of the computer, though he never saw a working one built.

3.6 Basic exercises in logic

“[W]hoever has attempted anything of this kind must be convinced, how difficult it is to hit upon such a method as shall have sufficient degree of perspicuity, and simplicity, omitting everything superfluous, and yet retaining all that is useful and necessary...”

-Maria Agnesi¹

We could spend a great deal of time discussing all the various ways of writing and rewriting statements and predicates, but the best thing to do is to simply do a number of practice problems and then trust your careful thinking and good judgement when encountering new situations.

1. Show that if $P(x)$ and $Q(x)$ are predicates, then $\neg(P(x) \Rightarrow Q(x))$ is logically equivalent to $\exists x$ s.t. $P(x) \wedge (\neg Q(x))$.
2. Invent and write down three examples of implications from life outside of mathematics. Identify the hypothesis and the conclusion and discuss the truth value of each statement.
3. Invent and write down three examples of mathematical statements that are implications. Identify the hypothesis and conclusion of each and discuss the truth value of each statement.
4. Find an example of a (possibly non-mathematical) predicate $Q(x, y)$ in two free variables x and y such that $\forall x \exists y Q(x, y)$ is a true statement but $\exists y \forall x Q(x, y)$ is a false statement.
5. For each of the following implications, write down the (i) negation, (ii) the converse, and (iii) the contrapositive (each phrased as positively as possible). Finally, (iv) attempt to determine the truth value of the original implication. Explanatory comments are in parentheses and are not part of the statement you are to work with.
 - (a) If n is positive, then $\sqrt{n} = n$.
 - (b) (x is a fixed real number.) If $x^2 \geq 2$, then $x \geq 1$.
 - (c) If n is a natural number and n^2 is even, then n is even.
 - (d) If n is a natural number, then $5n^2 + 5n + 1$ is a prime number. A **prime number** is a natural number other than 1 whose only natural number divisors are 1 and itself. Finally, for natural numbers, “being odd” means “not being even” and “even” means being a multiple of 2.

(Hint for (iv): look at a table of prime numbers. You can find one online.)

¹Maria Gaetana Agnesi (1718-1799) was a prodigy and genius best known for her textbook on Calculus, entitled *Analytical Institutions*. The quotation is from her introduction to that book, translated by John Colson. For more on Agnesi, see [126].

- (e) If T_1 and T_2 are triangles with the same area, then their sides are the same length.
- (f) If $f: [0, 1] \rightarrow \mathbb{R}$ is a function then there is a real number M such that for all $x \in [0, 1]$, we have $f(x) \leq M$. (Here, $[0, 1]$ is the interval $\{x \in \mathbb{R} : 0 \leq x \leq 1\}$)

(Hint for (iv): if a function is continuous on a closed and bounded interval, the extreme value theorem from calculus can be applied to it. Thus, if you try to show that the statement is true, you are, in essence, attempting to extend the extreme value theorem to all functions. If you try to show the statement is false, on the other hand, you need to show that there is a discontinuous function for which the conclusion of the extreme value theorem does not hold.)

6. Which of the following statements¹ (if any) is true? Are they logically equivalent? Why or why not?

P : “There is a positive real number b such that for all positive numbers a , $b < a$.”

Q : “For all positive real numbers a , there is a positive number b , such that $b < a$.”

7. For each of the following implications (which are variants of statements elsewhere in this text) write the (i) converse, (ii) contrapositive, and (iii) negation (remembering that the negation of an implication is a conjunction.) You do not need to know all the terms in the statements and not all of the statements are true. Explanatory comments are in parentheses and you do not need to manipulate them when writing the converse, contrapositive, or negation.

- (a) If A is a subset of B then B^c is a subset of A^c .
- (b) If $X = \emptyset$ and Y is a set, then $X \times Y = \emptyset$.
- (c) If every element $H \in \mathcal{H}$ is a convex set, then $\bigcap_{H \in \mathcal{H}} H$ is convex.
- (d) If $a, b \in \mathbb{N}$, then there exists $q, r \in \mathbb{N}^*$ such that $b = aq + r$ and $r < a$.
- (e) If $a \sim b$ and $b \sim c$, then $a \sim c$.
- (f) If $f(x) = f(y)$, then $x = y$.
- (g) (We have a function $f: X \rightarrow Y$.) If $y \in Y$, there exists $x \in X$ such that $f(x) = y$.
- (h) If $f: X \rightarrow Y$ is injective and $g: Y \rightarrow Z$ is injective, then $g \circ f: X \rightarrow Z$ is injective.
- (i) If $n \in \mathbb{Z}$, then there exists $k \in \mathbb{Z}$ such that $n = 2k$ or $n = 2k + 1$.
- (j) If $n \in \mathbb{N} \setminus \{1\}$, then there exists a prime number p such that n is a multiple of p .

¹Taken from [44]

- (k) (For every $n \in \mathbb{N}$, $x_n \in \mathbb{R}$.) If $|x_n - x_{n+1}| < (1/2)^n$, then for all $\epsilon > 0$, there exists $N \in \mathbb{N}$ such that for all $n, m \geq N$, $|x_n - x_m| < \epsilon$.
- (l) (For every $n \in \mathbb{N}$, $x_n \in \mathbb{R}$.) If $|x_n| < 100$, then there exists $a \in \mathbb{R}$ such that for all $\epsilon > 0$, there exists $N \in \mathbb{N}$ such that for all $n \geq N$, $|x_n - a| < \epsilon$.
8. Negate the following statements. Phrase your answer as positively as possible (meaning: don't simply write the word "not" in front of the given statement - try to write something that is potentially useful!) Explanatory comments are in parentheses and are not part of what you are to negate. Remember that predicates which are implications are considered to be statements by the invisible addition of a universal quantifier. You need to take that into consideration when negating. You do not need to know all the terms in the statement.
- (a) If a is an even natural number, then there exist natural numbers m, n, p, q such that
- $$a = m^2 + n^2 + p^2 + q^2.$$
- (b) There exists a natural number a and there exists a natural number b such that $ab = 5$.
- (c) For every real number $\epsilon > 0$ and for every natural number N , there exists a natural number $n \geq N$ with $|x_n - x| > \epsilon$.
 (Here (x_n) is a sequence of real numbers and x is a fixed real number.)
- (d) The sum of three odd numbers is always an odd number. (Hint: try rephrasing this so as to use quantifiers.)
- (e) For all $r \in \mathbb{R}$ and for all $s \in \mathbb{R}$ there exists $q \in \mathbb{R}$ such that $rs = q$.
- (f) $((x_n))$ is some fixed sequence and L is some fixed real number.
 For all $\epsilon > 0$, there exists $N \in \mathbb{N}$, such that for all $n \geq N$, $|x_n - L| < \epsilon$.
- (g) $((x_n))$ is a fixed sequence.
 There exists $L \in \mathbb{R}$, such that for all $\epsilon > 0$, there exists $N \in \mathbb{N}$, such that for all $n \geq N$, $|x_n - L| < \epsilon$ or for all $L \in \mathbb{R}$, there exists $N \in \mathbb{N}$, such that for all $n \geq N$, $x_n \geq L$.
- (h) ($f: \mathbb{R} \rightarrow \mathbb{R}$ is a fixed function and $a \in \mathbb{R}$ is a fixed number.)
 For all $\epsilon > 0$, there exists $\delta > 0$, such that if $|x - a| < \delta$, then $|f(x) - f(a)| < \epsilon$.
- (i) Every open cover of X has a finite subcover.
 (Hint: there are two quantifiers in this statement. Also, the negation of "finite" is "infinite".)
- (j) Every sequence (x_n) in X has a convergent subsequence.

- (k) The number 0 in \mathbb{Z} is the unique number such that if $x \in \mathbb{Z}$, then $x + 0 = x$.

(Hint: there are two ways 0 can fail to be the unique number with a given property: it might not have the property or it might not be the only number with the property.)

- (l) (For $\alpha \in \mathbb{R}$, let $[\alpha]$ denote the distance to the nearest integer. The statement is known as Roth's theorem.)

For all irrational, algebraic numbers $\alpha \in \mathbb{R}$ and every $\epsilon > 0$, there exists $C \in \mathbb{R}$ such that for all $N \in \mathbb{N}$

$$\min\{[\alpha n] : 1 \leq n \leq N\} \leq \frac{C}{N^{1+\epsilon}}.$$

- (m) (The next statement is known as Fermat's Little Theorem. It was stated by Fermat in 1640 and proved by Euler in 1736.)

If $p \in \mathbb{N}$ is prime, then for all $a \in \mathbb{Z}$, there exists $k \in \mathbb{Z}$ such that $a^p - a = kp$.

- (n) (The next statement is known as Fermat's Last Theorem. It was stated by Fermat in 1637 and dramatically proved by Andrew Wiles in 1995.)

For all natural numbers $N \geq 3$ and all $a, b, c \in \mathbb{N}$, $a^N + b^N \neq c^N$.

- (o) (The next statement is known as the Twin Prime Conjecture. It was first stated in a more general form in 1849, but is likely considerably older. It is still unproven.)

For all $N \in \mathbb{N}$, there exist prime numbers $p, q \geq N$ such that $|p - q| = 2$.

- (p) (The next statement was proved by Yitang Zhang in 2013 to the great astonishment of the mathematical community.)

There exists $M \in \mathbb{N}$ such that for all $N \in \mathbb{N}$, there exist prime numbers $p, q \geq N$ such that $|p - q| \leq M$.

- (q) (The next statement is related to the card game *Set* and dates to at least 1971. It was proved [43] in 2016. See [81] for an explanation of the connection to *Set*.)

(Let $n \in \mathbb{N}$ and suppose that there are n attributes (such as color, shape, smell, etc.) which a card may have. Each attribute can take one of three values. For example, color might be red, blue, or green and shape might be a diamond, square, or circle. Suppose that a deck X consists of all of the 3^n possible cards. A **match** is a set of three cards such that there is an attribute where they all have the same value. For example, if three cards have the same color, then those three form a match. For $A \subset X$, let $|A|$ denote the number of elements of A .)

For all $\epsilon > 0$, there exists $N \in \mathbb{N}$ such that for all $n \geq N$ if $A \subset X$ has the

property that no subset of A is a match, then

$$\frac{|A|}{2.756^n} < \epsilon.$$

- (r) (The next statement was proved in 2016 by Maryna Viazovska, to great acclaim [83, 128].)

No packing of unit balls in Euclidean space \mathbb{R}^8 has density greater than that of the E_8 -lattice packing.

9. (These examples are taken from [116]. See that book for more highly entertaining, imaginatively expressed puzzles.)

- (a) John has an identical twin. One of them always lies and the other always tells the truth. You meet the brothers and you wish to find out which one is John. You may ask only one question to one of them. The catch is that the question will be answered with only a “yes” or “no” and your question may not contain more than three words. What question should you ask?
- (b) The March Hare, the Mad Hatter, and the Dormouse were arrested on suspicion of stealing the Queen of Hearts’ jam. The Queen holds a trial to determine which of them stole the jam. Under interrogation, the March Hare and the Dormouse did not both speak the truth. The March Hare says, “I never stole the jam!” The Hatter says, “One of us stole it, but it wasn’t me!” The Dormouse says, “At least one of the March Hare and the Hatter told the truth.” Who stole the jam?

3.7 Russell’s Paradox

“Hardly anything more unfortunate can befall a scientific writer than to have one of the foundations of his edifice shaken after the work is finished. This was the position I was placed in by a letter of Mr. Bertrand Russell, just when the printing of this volume was nearing its completion.”

- Gottlob Frege¹

“It is bad luck to title a book ‘Volume One.’”

- Gian-Carlo Rota [108]

In the remainder of the text we’ll use a combination of logic and set theory to approach a wide variety of interesting mathematical topics. We will do so, however, without using a precise definition of “set” (or “element” for that matter.)

¹Gottlob Frege (1848 - 1925) was a philosopher and mathematician, best known for his efforts to base mathematics on formal logic. The quotation is from the second volume of his work *The Basic Laws of Arithmetic* and is oft quoted.

Although we will accomplish a lot without a precise definition of set, we should have some idea of what we are missing. The purpose of this chapter is to use logic to show that the informal definition of “set” we’ve used in previous chapters can lead to logical contradictions. The purpose of a formal definition of “set” (see Chapter 6) is to attempt to ensure that we can do everything we need to do with sets, without encountering logical contradictions. The final portion of this chapter gives an interesting application of these rather abstruse considerations to Computer Science.

In the 19th century, a number of mathematicians and logicians sought to base mathematics on precisely stated logical principles. As part of this quest, Gottlob Frege (1848–1925) thoroughly developed set theory. He published the first volume of his *magnum opus*, but as he was preparing the second volume for publication he received a letter from Bertrand Russell (1872 – 1970) which shattered his entire project. In the letter, Russell points out a logical contradiction in Frege’s work arising from not being careful enough with the definition of “set.” The ultimate resolution of this paradox was eventually accomplished through what is now called Zermelo-Frankel set theory. With modern eyes, Russell’s paradox is a “paradox” only in the sense that it contradicts our intuitive sense that we can form any kind of set that we want; it is actually a theorem that rules out the existence of a certain kind of set.

One way of escaping from the paradox is to claim that because we are appealing to terminology from everyday language we can’t be precise enough to strictly apply logical principles. However, there are more sophisticated versions of the paradox which raise serious philosophical issues. See [69] for a fun introduction to these, as well as to some of the other concepts from logic and set theory which will be important in this text. As far as set theory goes, however, Russell’s paradox needn’t cause us too much worry since rather than getting enmeshed in a philosophical trap, we can simply conclude that the object in question isn’t a set and then begin the quest for a more precise definition of “set.”



The version of Russell’s paradox we present here, centers on the question:

What sets are elements of themselves?

On the one hand, there is at least one set that is *not* an element of itself, since \emptyset does not have any elements at all. (Remember though that it does have a subset! Indeed, $\emptyset \subset \emptyset$ although $\emptyset \notin \emptyset$.) The question of whether or not there is a set A such that $A \in A$ is more difficult.

Thinking of sets as boxes makes it difficult to conceive how we could even parse a statements like $A \in A$. This is a limitation of our analogy. A better way of thinking of sets to try to make sense of these statements is to think of a set as a folder on a

computer. Clicking or tapping on the folder opens it and shows its contents (i.e. its elements). We can conceive of a special kind of folder such that examining the contents of the folder show us that the folder itself is one of the elements of the folder; potentially, other folders are also elements of the folder.

As a warm-up consider the following paradox (taken from [113]). Call a word “self-referential” if it describes itself and “non-self-referential” if not. For instance, “short” is a short word and so is self-referential. On the other hand, “long” is a short word and so is non-self-referential. Here is the question: Is “non-self-referential” a self-referential word or a non-self-referential word? It certainly can’t be self-referential since the word itself is “non-self-referential”. On the other hand, it can’t be non-self-referential for then it would be self-referential, which is a contradiction.

As another analogy, consider the real number defined¹ by the expression:

$$r = \sqrt{2 + \sqrt{2 + \sqrt{2 + \sqrt{2 + \sqrt{2 + \dots}}}}}$$

Observe that $r = \sqrt{2 + r}$ and is, in some sense², a real number that contains itself. Maybe there is a set-theory version of this?

Russell’s paradox concerns an (ultimately non-existent) set R whose elements are precisely the sets x such that $x \notin x$. It could be thought of a folder which behaves like this: When we open it, we see folders. No matter which folder x we examine, when we open x we will not see x as a folder inside x . Thus, for example, we would have $\emptyset \in R$ since $\emptyset \notin \emptyset$. Furthermore, crucially, R contains every single folder with this property. Our proof will show that this is logically impossible.

3.7.1

Theorem ▶ Russell’s Paradox

There does not exist a set R , whose elements are all sets, such that $x \in R$ if and only if $x \notin x$.

The proof is a “proof-by-contradiction”: we pretend the theorem is false and show that we encounter a logical contradiction. Since the theorem can’t be false, it must be true. We’ll explore proofs-by-contradiction more in the next chapter.

Proof. Suppose that there is a set R whose elements are precisely all those sets which are not elements of themselves. There are exactly two possibilities: either R is an element of itself or R is not an element of itself.

If R is an element of itself (i.e. $R \in R$) then, by the definition of R , $R \notin R$. Thus,

$$(R \in R) \Rightarrow (R \notin R)$$

which is a logical contradiction. Hence, it is not the case that $R \in R$.

If R is not an element of itself (i.e. $R \notin R$) then R , by definition, meets the

¹It is a question best addressed by Calculus as to why this expression does define a real number

²but not in a set theoretic sense

entrance criterion for elements of R and so $R \in R$. Thus,

$$(R \notin R) \Rightarrow (R \in R)$$

which is a logical contradiction. Hence, it is not the case that $R \notin R$.

We have shown, therefore that neither $R \in R$ nor $R \notin R$ but that is a contradiction as one of those must hold. Hence, there is no such set R . \square

An important consequence of this theorem is that there is no “set of all sets”:

3.7.2

Theorem ▶ There is no universal set

There does not exist a set U such that $A \in U$ if and only if A is a set.

Proof. Suppose, to obtain a contradiction, that there is such a set U . Then $R = \{x \in U : x \notin x\}$ would be a subset (see the Axiom of Subset Selection in Chapter 6.) However, the previous theorem shows that R is not a set and so U cannot be a set either. \square

Remark 3.7.1. Examining the proof of Theorem 3.7.2 raises the question of why we insist that if U is a set then $R = \{x \in U : x \notin x\}$ is a set. Rather than denying the existence of the set U , we could deny our ability to create a subset of a given set in this way. That is, we could choose to deny the Axiom of Subset Selection (which we haven’t discussed yet.) This axiom, however, is one of the major links between set theory and logic and denying it, rather than the existence of a universal set, would create far more problems than it solves.

Russell’s paradox leaves us with the question: How can we tell, in a particular instance, if we have defined a set? How do avoid logical contradictions? The answer to the first question is that we restrict ourselves only to sets whose existence is guaranteed by the axioms of set theory. The answer to the second question has a long interesting story, but is essentially: “We can’t guarantee that there are no logical contradictions, but none (to the best of our knowledge) have been found.” Mathematics, like everything else in human knowledge, ultimately depends on some faith and hope. For those of us who are becoming mathematicians, we would, of course, also add “love.”

3.8 Application: The Halting Problem

"[I]t has been shown that there are machines theoretically possible which will do something very close to thinking. They will, for instance, test the validity of a formal proof in the system of *Principia Mathematica*, or even tell of a formula of that system whether it is provable or disprovable. ... [O]ne can show that however the machine is constructed there are bound to be cases where the machine fails to give an answer, but a mathematician would be able to. On the other hand, the machine has certain advantages over the mathematician."

-Alan Turing¹

If you have ever done any computer programming, you have undoubtedly spent vast amounts of time debugging your code. The Fields Medallist William P. Thurston, comparing the level of detail necessary to write a correct proof with the level of detail required to write a correct computer program, says [124]:

I have spent a fair amount of effort during periods of my career exploring mathematical questions by computer. In view of that experience, I was astonished [at the view] that mathematics is extremely slow and arduous, and that it is arguably the most disciplined of all human activities. The standard of correctness and completeness necessary to get a computer program to work at all is a couple of orders of magnitude higher than the mathematical community's standard of valid proofs. Nonetheless, large computer programs, even when they have been very carefully written and very carefully tested, always seem to have bugs.

In light of this, we might despair at our ability to write correct proofs. Thurston, reminds us, however that the goal is ultimately that of understanding and that communicating understanding is of primary importance:

Mathematics as we practice it is much more formally complete and precise than other sciences, but it is much less formally complete and precise for its content than computer programs. The difference has to do not just with the amount of effort: the kind of effort is qualitatively different. In large computer programs, a tremendous proportion of effort must be spent on myriad compatibility issues: making sure that all definitions are consistent, developing "good" data structures that have useful but not cumbersome generality, deciding on the "right" generality for functions, etc. The proportion of energy spent on the working part of a large program, as distinguished from the bookkeeping part, is surprisingly small. ...

A very similar kind of effort would have to go into mathematics to make it formally correct and complete. ... If we were to continue to cooperate,

¹Alan Turing (1912-1954) did foundational work in probability, logic, genetics, cryptography. His most influential work was in the theory of computation. The theoretical abstraction of modern computers is called a "Turing machine." The argument that the halting problem is unsolvable is credited to Turing.

much of our time would be spent with international standards commissions to establish uniform definitions and resolve huge controversies.

Mathematicians can and do fill in gaps, correct errors, and supply more detail and more careful scholarship when they are called on or motivated to do so. Our system is quite good at producing reliable theorems that can be solidly backed up. It's just that the reliability does not primarily come from mathematicians formally checking formal arguments; it comes from mathematicians thinking carefully and critically about mathematical ideas.

One way of “thinking carefully and critically” about mathematical ideas is to test them against real world problems. Sometimes the results can be quite surprising. Here is an example arising from an application of mathematics to computer science. Although, the ideas of what follows can be formalized in a much more precise way, here we simply outline the relevant ideas and defer the details to another course.

There is an especially pernicious type of bug in software: an infinite loop. Modern computer programs are exceedingly complex and can run for days before producing their output. If a computer program enters into an infinite loop it will never¹ terminate, but the user may wait expectantly for a long time before giving up on it. “Maybe my program will stop in 5 minutes? ... Maybe it just needs 5 more minutes ...” and so on.

Wouldn't it be great if there were a computer program HALT available that could read the code for *any* other computer program X and determine if X will enter into an infinite loop or if it is guaranteed to halt (i.e. stop running or terminate)?

It turns out that no such computer program HALT can exist! To explain why, recall that a computer program consists of two parts: the code and the executable. The code is (more-or-less) human readable and exists independently of the executable, which is the set of instructions actually carried out by the computer's CPU. The executable is what is produced from the code by a compiler. (In some modern languages, you may never see the executable and the work of the compiler may be carried out automatically.) Additionally, computer programs may take a file as input – in particular they can take their own code as input. This is reminiscent of Russell's Paradox where we ask if a certain set is an element of itself, and thereby encounter a contradiction to the existence of a universal set. We can apply a similar idea here.

Suppose, for a contradiction, that there is a computer program HALT which can read the code (without running it!) for any other computer program X and determine if X is guaranteed to halt. We may assume, without loss of generality, that if X halts, the program HALT prints out “ X halts!” and terminates. If X might enter into an infinite loop, HALT prints out “ X infinitely loops!” and then terminates. We write a new computer program Q . The program Q takes the code for any computer program X as input. It then tells HALT to read the code for X . If HALT prints out “ X halts!” then we write Q so that Q enters into an infinite loop. On

¹well, at least not until the hardware fails

the other hand, if HALT prints out “ X infinitely loops!”, then we write Q so that Q prints out “Success!” and terminates. In particular if X halts, then Q loops and if X infinitely loops, then Q terminates.

We now compile Q and, to the executable for Q , input the code for Q itself. Let’s see what happens. If Q infinitely loops, then by design Q terminates (a contradiction) and if Q halts, then Q by design infinitely loops – also a contradiction. Hence the program HALT cannot exist.

If the previous argument seems like it could be made more exciting, I encourage you to consult [103].

Carnot’s theorem in thermodynamics has the corollary that it is impossible to build a perfectly efficient engine. Carnot’s theorem, however, does not mean that engineers shouldn’t try to keep making engines more efficient (even as they know perfection is impossible). Similarly, the solution to the Halting Problem shows that it is impossible to write a computer program which is perfect at detecting whether or not code will enter into an infinite loop. This does not mean, however, that it is impossible to make improved bug checkers. In fact, there are computer programs which can determine if certain limited classes of computer programs will loop or halt. The argument showing that the Halting problem is impossible shows that if such a computer program MINI-HALT can determine if all programs having certain characteristics \mathcal{C} are guaranteed to halt, then MINI-HALT does not itself have those characteristics \mathcal{C} .

4 | Proof Techniques I

Key Concepts

- direct proof
- proof by contraposition
- proof by contradiction
- proving existence
- proving uniqueness

“A proof is a proof. What kind of a proof? It’s a proof. A proof is a proof. And when you have a good proof, it’s because it’s proven.”

–Jean Chrétien²

This chapter covers the most common types of proofs, other than induction. Induction will be discussed in Chapter 9.

4.1 Direct Proof

“Begin at the beginning,” the King said gravely, “and go on till you come to the end: then stop.”

-Lewis Carroll, *Alice in Wonderland*

In a direct proof, you should usually start by stating whatever it is you are assuming. If you are proving that an implication holds, then the hypothesis of the implication is one of the initial assumptions which you should state. You should then say what it is you are to prove and, through a sequence of tightly reasoned steps, explain why what you are to prove is true. Each step should make use of only previously stated definitions, previously proved theorems (or lemmas,

²Jean Chrétien was prime minister of Canada from 1993 - 2003. This quote can be found at [26].

etc.), and the standard rules of logic. Throughout you should explicitly point out where you have used the initial assumptions. At the end of the proof you should conclude by summarizing what it is you have proved.

DIRECT PROOF OF AN IMPLICATION

To show: $P \Rightarrow Q$

Structure of Proof:

We assume P and we will show that Q holds.

(Sequence of tightly reasoned statements, each following from what has already been done. At some point, possibly at the beginning, possibly later on, the assumption that P is true is used. Usually at the end we encounter a statement which shows us, without any additional work that Q is true.)

Thus, Q is true. \square .

The element arguments we saw in the first chapter were all direct proofs. Here is a relatively simple example. We assume some basic well-known properties of the integers. Recall that $n \in \mathbb{Z}$ is a **multiple** of $m \in \mathbb{Z}$ if there exists $a \in \mathbb{Z}$ such that $n = am$. A lemma is simply a theorem used primarily to prove another theorem. We will use this result in the proof of Theorem 4.3.1.

4.1.1

Lemma

Suppose that $n \in \mathbb{Z}$. If there exists $m \in \mathbb{Z}$ such that both n and $n + 1$ are multiples of m , then $m \in \{-1, 1\}$.

Proof. Let $n \in \mathbb{Z}$. Assume that $n = km$ and $n + 1 = \ell m$ for some $k, \ell \in \mathbb{Z}$. We will show that $m \in \{-1, 1\}$.

Subtracting the first equation from the second, we obtain:

$$1 = (\ell - k)m.$$

Taking absolute values, we see that

$$1 = |\ell - k| \cdot |m|.$$

Since $|m|$ and $|\ell - k|$ are integers, by the properties of multiplication, we have $0 \leq |m| \leq 1$. Thus, $|m| = 0$ or $|m| = 1$. In the first case, $m = 0$. However, this is impossible as there is no number $|\ell - k|$ such that $1 = |\ell - k| \cdot (0)$. In the second case $m = \pm 1$, as desired. \square

4.2 Proof by Contraposition

"If I can't raise a little diversionary attack, my name's not Sergeant Jackrum. And since it *is* Sergeant Jackrum, that proves it."

- Terry Pratchett, *Monstrous Regiment*

Recall that the contrapositive of an implication $P \Rightarrow Q$ is the statement $\neg Q \Rightarrow \neg P$ and that the contrapositive is logically equivalent to the original implication. Consequently, instead of giving a direct proof of an implication, we can give a direct proof of its contrapositive. This style of proof is called a "proof by contraposition." We always begin such a proof by saying what kind of proof it is.

PROOF BY CONTRAPOSITION

To show: $P \Rightarrow Q$

Structure of Proof: We prove the statement by contraposition. We assume that Q is false and will show that P is also false.

(Sequence of tightly reasoned statements, each following from what has already been done.)

Thus, P is false. Since we have shown that $\neg Q \Rightarrow \neg P$, it must be the case that $P \Rightarrow Q$.

For our example we will use, without proof, the fact that a number $n \in \mathbb{N}^*$ is not even (i.e. **odd**) if and only if there exists $m \in \mathbb{N}^*$ such that $n = 2m + 1$.

4.2.1

Lemma

A number $n \in \mathbb{N}^*$ is even if and only if n^2 is even.

Since the theorem is an "if and only if" statement we have two implications to prove. The first one is proved directly; the second by contraposition.

Proof. (\Rightarrow) Let $n \in \mathbb{N}^*$ be even. We will show n^2 is even.

Since n is even, by definition of even, there exists $m \in \mathbb{N}$ such that $n = 2m$. Elementary arithmetic shows that

$$n^2 = 4m^2 = 2(2m^2).$$

Since n^2 is a multiple of 2, it is even.

(\Leftarrow) Let $n \in \mathbb{N}^*$. We will prove the implication by contraposition. That is, we will show that if n is not even then n^2 is not even.

Assume n is not even. By our stated assumption, this implies that there exists $m \in \mathbb{N}^*$ such that $n = 2m + 1$. By elementary algebra:

$$n^2 = (2m + 1)^2 = 4m^2 + 4m + 1 = 2(2m^2 + 2m) + 1.$$

Since n^2 is one more than an even number it is not even. Hence, if n is not

| even then n^2 is not even, as desired. □

4.3 Proof by Contradiction

“Reductio ad absurdum, which Euclid loved so much, is one of a mathematician’s finest weapons. It is a far finer gambit than any chess play: a chess player may offer the sacrifice of a pawn or even a piece, but a mathematician offers the game.”

- G.H. Hardy¹, *A Mathematician’s Apology*

A proof by contradiction (or *reductio ad absurdum*) begins by asserting the negation of what is trying to be proved and then shows that the assumption produces a logical contradiction. Since the negation cannot be true, the statement itself must be true². A proof by contradiction should always begin by saying what kind of proof it is.

PROOF BY CONTRADICTION

To show: P is true.

Structure of Proof: We prove the statement by contradiction and so assume that P is false.

(Sequence of tightly reasoned statements, each following from what has already been done and concluding with a contradiction.)

Since we have encountered a contradiction, P cannot be false. Hence, P is true.

Here are two famous examples. For the first example we need the definition of prime number and a fact whose proof will be deferred. A number $p \in \mathbb{N}$ is **prime** if $p \neq 1$ and if whenever p is a multiple of some $a \in \mathbb{N}$, either $a = 1$ or $a = p$. The fact we need is that every number $n \in \mathbb{N}$ such that $n \geq 2$ is a multiple of a prime number; see Theorem 9.2.3.

4.3.1

Theorem ▶ Infinitude of Primes

There are infinitely many prime numbers.

The proof is essentially due to Euclid³.

¹G.H. Hardy (1877-1947) was a prominent mathematician, working primarily in number theory. His book *A Mathematician’s Apology* is a classic, though deeply frustrating in the way it creates and perpetuates false myths regarding who can do mathematics and how it should be done.

²This is the occasionally controversial logical principle known as the “law of the excluded middle.”

³Euclid (325 BCE? - 265 BCE?) compiled *The Elements*, one of the most influential books of all time. In his proof of the infinitude of primes Euclid did not use a proof by contradiction. He showed that for every $N \in \mathbb{N}$, there exists a prime number p such that $p > N$. In my experience, almost all beginning math students prefer the proof by contradiction. The main issue with this, however, is that we do not have a precise definition of “infinitely many” or “finitely many”. We will explore this in Chapter 10. For now, we rely on our perhaps vague sense of what this should mean.

Proof. Suppose, for a contradiction, that there are only finitely many prime numbers. Let them be:

$$p_1, p_2, p_3, \dots, p_m.$$

Let $n = p_1 p_2 \cdots p_m$ be their product. Observe that n is a multiple of p_i for each $i \in \{1, \dots, m\}$. Also, for all i , $p_i \neq 1$, by the definition of prime. Thus, by Lemma 4.1.1, $n+1$ is not a multiple of p_i , for any $i \in \{1, \dots, m\}$. That is, $n+1$ is not a multiple of any prime number. However, $n+1 \geq 2$ and so we contradict the (still unproved) fact that every natural number other than 1 is a multiple of a prime number. This contradiction shows that there must be infinitely many prime numbers. \square

Our second famous example shows that there is a real number (namely $\sqrt{2}$) that is not rational. Recall that $\sqrt{2}$ is defined to be the positive real number x with the property that $x^2 = 2$. Why must there be such a number? That is a vexing question that depends on the exact definition of the real numbers. Those waters are too deep for us at present. Additionally, our proof will also need one other deep fact (see Theorem 9.3.7): every rational number $r \in \mathbb{Q}$ can be written in lowest terms. In other words, if $r \in \mathbb{Q}$, there exists $a \in \mathbb{Z}$ and $b \in \mathbb{N}$ such that $r = a/b$, and so that the only common factors of a and b are ± 1 .

4.3.2

Theorem ▶ Irrationality of $\sqrt{2}$

The number $\sqrt{2}$ is irrational. That is, there do not exist $a, b \in \mathbb{Z}$ with $b \neq 0$ so that $\sqrt{2} = a/b$.

Proof. We prove this by contradiction. Suppose that there does exist $a \in \mathbb{Z}$ and $b \in \mathbb{N}$ such that $\sqrt{2} = a/b$. By our preliminary assumption, we may assume that a/b is in lowest terms. Then, $\sqrt{2}b = a$ and so $2b^2 = a^2$. Thus, a^2 is even. By Lemma 4.2.1, a must be even. That is, there exists $m \in \mathbb{Z}$ such that $a = 2m$. Consequently,

$$2b^2 = (2m)^2 = 4m^2.$$

Hence, $b^2 = 2m^2$ and so b^2 is even. By Lemma 4.2.1, this implies that b is even. However, since both a and b are even, they are both multiples of 2, contradicting the fact that we chose a/b in lowest terms. \square

4.3.3

Exercise

Prove that $\sqrt{3}$ is irrational. When you write your solution, you should list all elementary number facts that you need (some of which you may not be able to prove.) Any portion of the proof that can be separated out as a separate lemma should be.

(This is your chance to adapt the previous example to prove something rather sophisticated. You should focus on writing something coherently organized and logically correct. At this point you may have gaps in your argument or statements you don't know how to justify. These should be clearly marked as such. You should base your work on the proof above that $\sqrt{2}$ is irrational. Rather than discussing even numbers, you will need to discuss numbers that are multiples of

3. Also, this is certainly a proof that you can find online – but you shouldn't do that! Instead work hard to construct it for yourself.)

Since a proof by contradiction begins by asserting something that is ultimately shown to be false, proofs by contradiction can have an unsettling quality to them and may not produce as much understanding as one would like from a proof. Here is an historically important example.

4.3.4 Example

In Euclid's *Elements*, Euclid states five axioms from which he deduces all of what is now called "planar euclidean geometry." The first four of the axioms were relatively non-controversial, saying things like "Given a point (x_0, y_0) in the plane and a radius $r > 0$, there is a circle of radius r centered at (x_0, y_0) ." The fifth axiom, however, seemed much more like it should be a theorem rather than an axiom. That is, it seemed like it should be possible to prove the fifth axiom using only the first four axioms; there should be no need to take it as an unproved assumption. One mathematician to attempt this was Giovanni Saccheri (1667– 1733). He tried using a proof by contradiction. He assumed the first four axioms were true and also assumed that the negation of the fifth axiom was true. Saccheri then attempted to work his way to a contradiction. Along the way he proved a number of results based on these assumptions, many of which seemed very counter-intuitive. Eventually he gave up when he encountered a result which he claimed was "repugnant to the nature of straight lines." It was not until late in the 19th century when Eugenio Beltrami showed (though he did not phrase it this way) that Saccheri's quest was impossible.

If a theorem can be proved by both a direct proof and a proof by contradiction then, unless the direct proof is much harder to understand, the direct proof is preferable. After you have written a proof by contradiction, check to be sure that you actually needed to write it that way. In particular, a proof by contradiction of an implication can often be rewritten as a proof by contraposition.

4.4 Existence

“But there was yet another thing which I affirmed, and which, from having been accustomed to believe it, I thought I clearly perceived, although, in truth, I did not perceive it at all; I mean the existence of objects external to me...”

– René Descartes¹, *Meditationes de prima Philosophia*

Many of the most significant results in mathematics are statements of existence. An existence proof can have the feeling of magician’s trick since there is no (logical) need for the writer to explain to the reader how the object in question was found. Often, though, one of these magical existence proofs will be preceded or succeeded by a brief discussion describing how the object was found. In this text, we will not often feel the need to provide this additional explanation as either the construction is classical (i.e. the method of discovery is either not known or would require too great a diversion from the task at hand to explain it) or relatively simple algebraic manipulations will produce the required object. We gave a few examples of proofs of existence using element arguments in Chapter 1. Here is a reminder of how it works.



¹René Descartes (1596 - 1650) was a scientist, mathematician, and philosopher. His *Meditations* is one of the most influential philosophical works. This quotation is from a translation by Veitch.

PROOF OF EXISTENCE

To show: There exists a satisfying property P .

Structure of Proof: Let $a = \dots$

(State exactly what a is.)

We now show that a has property P .

(Do work to show that a has the required property P)

The work required to show that a has the required property may involve one or more direct proofs, proofs by contradiction, or some other kind of proof.

Although the proof structure above is fairly typical of existence proofs, there are many existence proofs that depart from it. For instance, in many cases it may not be possible to give a brief definition of a . For example, the Intermediate Value Theorem (typically encountered in a beginning calculus class) affirms that if a continuous real-valued function f is defined on the interval $[a, b]$ of real numbers and if y is between $f(a)$ and $f(b)$ then there exists c so that $a \leq c \leq b$ and $f(c) = y$. The Intermediate Value Theorem (IVT) does not say what the number c is (i.e. does not give a formula for it in terms of the function or the numbers a , b , and y .) It only says that the number c exists. Thus, if an existence proof of some other theorem needs to use the IVT it will not be possible for the existence proof to give a simple description of the object whose existence is being proved. Nevertheless, even in that case the first part of the existence proof should explain how the IVT is being used to find the object a and then the second part of the proof should show that a satisfies the requirements of the theorem being proved.

4.4.1

Theorem ▶ 1-dimensional Brouwer Fixed Point Theorem

Suppose that f is a continuous function defined on $[0, 1]$ such that for every $t \in [0, 1]$, we have $0 \leq f(t) \leq 1$. Then there exists $t_0 \in [0, 1]$ such that $f(t_0) = t_0$.

The proof uses some basic facts from Calculus, including the IVT. The generalization of this theorem to higher dimensions is one of the most significant theorems of topology.

Proof. We assume that f is a continuous function defined on the interval $[0, 1]$ such that for every $t \in [0, 1]$, we have $0 \leq f(t) \leq 1$. We will show that there exists a fixed point $t_0 \in [0, 1]$ such that $f(t_0) = t_0$.

Let $g(t) = t - f(t)$ for every $t \in [0, 1]$. Standard results from Calculus ensure that g is a continuous function defined on $[0, 1]$. Observe that $g(0) = -f(0) \leq 0$ and $g(1) = 1 - f(1) \geq 0$. Thus, 0 is contained in the interval $[g(0), g(1)]$. Since g is continuous, by the Intermediate Value Theorem, there exists $t_0 \in [0, 1]$ such that $g(t_0) = 0$. By the definition of g , this implies:

$$t_0 - f(t_0) = 0.$$

| That is, $f(t_0) = t_0$, as desired. □

Similarly, it is sometimes possible to prove the existence of an object by contradiction: assume the object does not exist and show that we encounter a logical contradiction. For instance, we could rewrite Theorem 4.3.2 and its proof to be a proof by contradiction that irrational numbers exist. Often, however, such proofs are overly convoluted.

Existence proofs are often paired with uniqueness proofs, described in the next section.

4.5 Uniqueness

“What *does* logic contribute to mathematics? Logic does a number of things that are essential for mathematics. In the first place, logic stabilizes mathematical ideas. Without logic mathematics would be in a continual state of flux, so it would be impossible to build up the intricate mathematical structures and arguments that characterize the subject. ... [Secondly,] logic helps us to communicate mathematics by creating a common language in which mathematical ideas may be expressed.”

– William Byers, *How Mathematicians Think* [22]

In Chapter 1, we explained that often a proof of uniqueness follows the basic outline below.

PROOF OF UNIQUENESS (VERSION 1)

To show: The object a is the unique object satisfying property P .

Structure of Proof: First, we show that a has property P .

(Do work to show that a has property P)

Now we show that a is unique. Suppose that a and b both satisfy property P . We will show that $a = b$.

(Do work to show that $a = b$.)

Sometimes, however, it is better to prove uniqueness by contradiction:

PROOF OF UNIQUENESS (VERSION 2)

To show: The object a is the unique object satisfying property P .

Structure of Proof: First, we show that a has property P .

⟨Do work to show that a has property P ⟩

Now we show that a is unique. We do a proof by contradiction. Suppose that a satisfies property P , but is not unique. Then there exists $b \neq a$ also satisfying property P .

⟨Do work to encounter a contradiction.⟩

Since we have encountered a contradiction, if a satisfies property P , then it is the unique object satisfying property P .

Here is an example.

4.5.1

Theorem

The real number $x = 0$ is the unique solution in the set of real numbers to the equation $x(x^2 + 1) = 0$.

Proof. Observe, first, that $x = 0$ is a solution to the equation $x(x^2 + 1) = 0$. Suppose, then, for a contradiction that there exists a non-zero $z \in \mathbb{R}$ such that $z(z^2 + 1) = 0$. Since $z \neq 0$, we may divide by z to obtain

$$z^2 + 1 = 0.$$

Subtracting 1 shows that

$$z^2 = -1.$$

There is no such real number z , and so 0 is the unique real number solution to $z(z^2 + 1) = 0$. \square

4.6 Application: p -values and Scientific Reasoning

“Researchers often wish to turn a p-value into a statement about the truth of a null hypothesis, or about the probability that random chance produced the observed data. The p-value is neither. It is a statement about data in relation to a specified hypothetical explanation, and is not a statement about the explanation itself.”

-American Statistical Association, *ASA Statement on Statistical Significance and P-Values* [130]

In both the natural and social sciences, natural or behavioural phenomena are

studied by collecting measurements from some subset of the population of interest. For instance, an economist might randomly select some, but not all, members of a community for an interview. Or a chemist might select certain flakes of paint from a painting in order to subject them to chemical analysis to determine the materials used in the paint. After analyzing the data they've collected, the economist or chemist reports their findings. For the findings to be of interest, however, the scientist needs to claim that the findings apply not only to the people or paint flakes they've sampled, but to all the people in the community or to all the paint in the painting. How do we know that their findings are not just an artifact of the particular people or paint flakes chosen for analysis?

Statistics has numerous methods available for scientists to make the argument that their findings apply to the entire population of interest and not just to that subset that was analyzed. One of the most prevalent (and most problematic) methods is the method of *p*-values. To understand how *p*-values are used, we need to realize that there are two reasons why findings concerning a subset of the population may not apply to the entire population:

1. *Selection Bias*, and
2. *Statistical Error*.

Selection bias arises when the sample is systematically chosen in a way that does not accurately reflect the entire population. For instance, perhaps the economist is interested in studying local attitudes toward property tax increases. If the economist only interviews people who are in their homes between the hours of 9 AM and 5 PM during the weekday, the sample will be biased as it will not include the opinions of people who are at work during those hours. The views of people who are at home during the workday (such as retirees) may not be representative of the people who are at work (and may have an income). Similarly, if the chemist only selects paint flakes from one corner of the painting, she may be testing only paint that was applied during an attempted restoration, rather than original paint.

Statistical error, on the other hand, arises even when a sample *is* representative of the population. If the economist randomly selects 1000 people from a city of population 15,000 (and those people agree to be interviewed and answer the questions honestly) those thousand people will still not exactly reflect the opinions of all 15,000 residents. Likewise, even if the chemist randomly selects paint flakes from a dozen different locations on the painting the chemical properties of those flakes will not exactly coincide with the chemical properties of all the paint on the painting.

The method of *p*-values allows us to understand the effects of *statistical error* on our conclusions. It does nothing to address any kind of selection bias. The way it works is this. The scientist establishes a null hypothesis (typically denoted H_0) which she will attempt to refute with her analysis. For instance, the economist might claim:

$$H_0: \text{The majority of city residents do not favor increasing property taxes.}$$

The chemist might claim:

H_0 : The mean (i.e. average) age of the paint on the canvas is less than 500 years.

The scientist then randomly selects a subset of the population to analyze, arriving at measurements X . Suppose that the economist determines that 55% of the *sampled* population does not favor increasing property taxes and that the chemist determines that the mean age of the *sampled* paint flakes is 450 years. Statistics gives a method, using the size of the population, the size of the sample, and X to determine a probability, denoted $p(X|H_0)$, that H_0 being true would result in the measurements X being observed. Suppose, for instance that the majority of residents do not favor increasing property taxes and that 70% of the *sampled* residents do not favor increasing property taxes. The probability $p(X|H_0)$ will likely be large as it is likely that 70% of the sampled residents do not favor increasing property taxes if the majority of all residents do. Conversely, if the majority of residents do not favor increasing property taxes but only 10% of the sampled residents do not favor increasing property taxes, then $p(X|H_0)$ will likely be small. Similarly, if the mean age of the paint is less than 500 years and if the sampled paint flakes have a mean age of 510 years, then $p(X|H_0)$ will be large, while if the sampled paint flakes have a mean age of 800 years, then $p(X|H_0)$ will be small. This is because if the average age of the paint on the canvas is less than 500 years it is *unlikely* that our sample will have a mean age of 800 years.

In practice, the scientist compares the probability $p(X|H_0)$ to a pre-determined threshold (often .05). If $p(X|H_0)$ is less than the threshold then the null-hypothesis is rejected. Thus, if $p(X|H_0) < 0.05$ then the economist would conclude that the majority of city residents are okay with increasing property taxes. The chemist would conclude that the mean age of the paint on the canvas is at least 500 years. Again, this is because if H_0 is true, then it is unlikely that $p(X|H_0)$ will be small.

This kind of reasoning is a version of a proof by contraposition. The scientist thinks:

“If H_0 is true, then $p(X|H_0) \geq 0.05$. However, I have discovered that $p(X|H_0) < 0.05$, therefore H_0 is (likely to be) false.”

For more about notions of statistical proof and some of the issues surrounding the use of *p*-values, see [71] and [130].

4.7 Writing Well

“With all proofs, there are many levels of confidence. At first, you see a solution, and that is very good. But it is a huge proof, so you may have overlooked something. Then you sit down and write notes. After you have done that, you are more confident. And then you sit down and write a paper, and you feel even more confident. And then you start giving talks and people think about what you said. And there is the refereeing process. By now, we are pretty confident. With such a large proof, I don’t know how to tell one hundred percent that it is true. Probably someone by now would have found a mistake, as it is something that people care about.”

-Maria Chudnovsky¹ [18]

Here are a few pieces of advice for writing proofs well. For more on good proof writing style, check out [60, 72, 119]. Some of the following suggestions are inspired by those resources.

Think of your reader. If you have to do extra work to make your proof clearer, do it. If a picture helps to explain your notation or proof strategy, include one. If you have irrelevant details, take them out. If a proof by contraposition would be clearer, but you’ve written a proof by contradiction, rewrite it. In general, you should assume that your reader is a mathematician not quite as advanced as yourself. Consider the final words of a book review written by one prominent mathematician concerning a mathematics text written by another prominent mathematician:

“Those who can understand the book will be indebted to [the author of the text] for having brought together in one volume the important results contained in it. How much greater thanks would he have earned if the book had been written in such a way that more of it could have been more easily comprehended by a larger class of readers! It is to be hoped that someone will undertake the task of writing such a book.” - L.J. Mordell [94]

Write multiple drafts. After you’ve written a version of your solution ask yourself: Can I make this clearer? Will my intended reader understand it? Should I put more steps in? Have I included too much detail? Do I ramble? Do I have logical gaps? Have I ever assumed what I am trying to prove? Did I prove the statement I was asked to prove? Use your answers to write a better draft, if possible.

Later in the text we will encounter other methods of proof, most of which are versions of the proofs described above. In all cases, it is crucial that you **clearly articulate what you are assuming** at the start of the proof **and what you are trying to prove**. As proofs get more complex, you will have smaller proofs em-

¹Maria Chudnovsky (b. 1977), speaking about her co-authored proof of the Strong Perfect Graph Conjecture

bedded inside larger proofs. If these smaller proofs are too long or complex, it may be helpful to pull them out as their own lemmas.

In your initial drafts, **include too many details rather than too few**. You can always remove details later, but if you don't ever write them down you may have made an error or missed an important piece of reasoning without ever realizing it. Many a mathematical research paper has been rejected by a journal referee who discovered a significant gap in the argument! Even worse, sometimes the referee doesn't see the gap and other mathematicians begin relying on results which have been incompletely proven or are false!

Be clear about what you are *assuming* versus what your are *concluding*. There's little more frustrating to a reader than not being sure whether a statement or equation is something being assumed or something being proven.

Take special care with proofs of existence. If you are asked to show that something exists, you must actually say what that thing is, either by directly constructing it or by appealing to previously proved existence theorems. Simply giving the object a name isn't enough to show that it exists. For example, if you are asked to show that there is an element of a set A which is (for example) positive, you can't just say "Let $a \in A$ be positive" – for how do you know such an a exists? To simply assert its existence is to assume what you are trying to prove. You must actually appeal to the definition of A or to previously proved theorems concerning A (or both!) to explain why such an a exists. Perhaps at the moment, this seems clear and you wonder why anyone would make this mistake. All I can say in response is that this is one of the most common mistakes in proving theorems. I encourage you, after every existence proof you write, to reread it and ask yourself if you have actually said what the object is.

Use words to help your reader understand equations. If you are moving from one equation to another using elementary algebra, tell the reader that's what you are doing. Don't assume that a string of equations communicates anything meaningful to the reader about why the claimed statement is true.

Use transition words and phrases to guide your reader. Words like *consequently*, *therefore*, *hence*, *thus* provide clues to the reader that you are not introducing a new thought but are rather deducing a conclusion from what you've just been discussing.

Introduce notation, but not too much. If you are going to refer to an object (set, function, etc.) multiple times, give it a name if it doesn't already have one. When choosing notation, be sure you don't use the same symbol (for example, x) to stand for multiple objects simultaneously¹. Also, if an object isn't actually necessary for the proof, try to avoid giving it a name or introducing notation for it. Readers find it difficult to keep track of lots of notation. The following quote from Charles Babbage (1791 - 1871) is to the point [11]:

¹My colleague Fernando Gouvêa refers to this as "notational bigamy."

“The plan of accenting letters, in order to represent quantities which stand in similar relations, adds, when employed with discretion, much to the perspicuity of the formulae in which it is used; but like many other innovations, whose tendency is on the whole decidedly beneficial, an attempt to extend it beyond its proper limits, has been productive of inconveniences as considerable as those which its introduction was proposed to remove. Indices in various positions have been substituted in many cases for the system of accentuation, and the admirers of this scheme, pursuing it with equal ardor, have not been more fortunate in avoiding the confusion, which a multitude of signs, differing but by the slightest shades, can scarcely fail of producing.”

Choose your notation wisely. Often in a proof there will be several objects with closely related but distinct functions. For example, if both n and m are even, then there exist $k, \ell \in \mathbb{Z}$ such that $n = 2k$ and $m = 2\ell$. The numbers k and ℓ are potentially distinct numbers, but their functions are very similar - they help witness the fact that n and m are even. In situations like this, we choose notation that helps the reader keep in mind that the objects are related, but potentially distinct. In our example, k and ℓ are adjacent letters of the alphabet. Alternatively, we might also choose to use k and k' . Often (but not always), we'll denote sets using capital letters (such as A) and elements using lowercase letters (such as a). However, in this text we will often need to work with sets whose elements we will need to remember are sets. In this case, we will often denote the set whose elements are sets using a caligraphic typeface, for example \mathcal{A} or \mathcal{U} . A representative element of the set is then denoted with the same letter, but in a different typeface, for example A or U . If we need to discuss two elements of the set \mathcal{A} , for example, we could then use A and A' to denote those elements. We might then refer to $a \in A$ and $a' \in A'$. We can also decorate variable names with other symbols, for example: \hat{a} , \tilde{a} , or \bar{a} . Don't, however, use symbols that are difficult to distinguish from each other! For instance, using the Greek letter Ξ and then putting a bar on top of it to get $\bar{\Xi}$ is a bad idea [78, p. 547]. However you choose your notation, you want to make it as easy as possible for the reader to remember what the notation represents.

Avoid beginning a sentence with a math symbol. Sentences beginning with math symbols can be difficult for the reader to parse quickly, especially if the math symbol isn't a capital letter. Similarly, don't put too many math symbols close together if you can help it.

4.8 Additional Proofs

“When you can prove a theorem, it basically captures infinitely many examples that you could never individually check on your own – even with the most powerful computers. And often, the essence of what is needed for a proof to work gives insight into the key features that make the phenomenon tick.”

-Carina Curto¹ [107]

Most of the proofs in this section are relatively simple adaptations of proofs in this chapter. Many of them can, of course, be found online. It is crucial, however, that you work through them for yourself, figuring out how to adapt the model proofs.

1. Prove, using a direct proof, the following theorem. Model your proof on the proof of Lemma 4.1.1

Theorem. Suppose that $n, m \in \mathbb{N}$ and that both n and $n + 3$ are multiples of m . Prove that $m \in \{1, 3\}$.

2. Use a proof by contraposition to prove the following theorem. Model your proof on the proof of Lemma 4.2.1. You may use the fact that every $m \in \mathbb{N}$ is either a multiple of 3, one more than a multiple of 3, or two more than a multiple of 3.

Theorem. For every $n \in \mathbb{N}$, if n^2 is a multiple of 3, then n is a multiple of 3.

3. Prove that $\sqrt[3]{2}$ is irrational. When you write your solution, you should list all elementary number facts that you need (some of which you may not be able to prove.) Any portion of the proof that can be separated out as a separate lemma should be.
4. Let p be a prime number. Prove that \sqrt{p} is irrational. When you write your solution, you should list all elementary number facts that you need (some of which you may not be able to prove.) Any portion of the proof that can be separated out as a separate lemma should be.
5. Adapt the proof that there are infinitely many primes to show that for every $N \in \mathbb{N}$ with $N \geq 2$, there exists a prime number p such that

$$N \leq p < N!$$

(Recall that $N!$ means $N(N - 1)(N - 2) \cdots 3 \cdot 2 \cdot 1$.) Can you find a smaller lower bound than $N!$?

¹Carina Curto is a mathematician working at the interface of theoretical mathematics and neuroscience.

6. Let A_r be the open interval $(-r, r) \subset \mathbb{R}$ for every $r > 0$. Prove that there exists a unique element x which is an element of A_r , for all $r > 0$.
7. How many points of intersection are there between two parabolas? Suppose that there are $(a, b, c) \in \mathbb{R}^3$ and $(a', b', c') \in \mathbb{R}^3$ such that there is no $k \in \mathbb{R}$ with $(a, b, c) = (ka', kb', kc')$. Let S be the set of all $(x, y) \in \mathbb{R}^2$ such that

$$\begin{aligned}y &= ax^2 + bx + c, \text{ and} \\y &= a'x^2 + b'x + c'.\end{aligned}$$

Prove that S has at most two points. Can you find conditions on (a, b, c) and (a', b', c') that guarantee that S has a unique element?

8. Recall that S^1 is the unit circle. Suppose that $\theta \in \mathbb{R}$. Let $x_0 = (1, 0) \in S^1$ and, for each $n \in \mathbb{N}$, define $x_n \in S^1$ to be the result of rotating the point x_0 counter-clockwise by an angle of $n\theta$.
- (a) Prove that there exists $n \in \mathbb{N}$ such that $x_n = x_0$ if and only if there exists $q \in \mathbb{Q}$ such that $\theta = \pi q$.
 - (b) Prove that there exist distinct $n, m \in \mathbb{N}$ such that $x_n = x_m$ if and only if there exists $q \in \mathbb{Q}$ such that $\theta = \pi q$.

5 | Building Sets

Key Terms

- complement and relative complement of a set
- intersection
- union
- power set
- cartesian product

“Don’t be intimidated! I have seen many people get discouraged because they see mathematics as full of deep incomprehensible theories. There is no reason to feel that way. In mathematics whatever you learn is yours and you build it up – one step at a time. It’s not like a real-time game of winning and losing. You win if you benefit from the power, rigor, and beauty of mathematics. It is a big win if you discover a new principle or solve a tough problem”

- Fan Chung Graham², *Advice to Young Women* [104]

In this chapter, we’ll investigate ways of creating new sets from old sets. After encountering Russell’s paradox (Section 3.7), we might wonder why these methods create legitimate sets (rather than just looking like sets!) The ZFC axioms of set theory, explained in Chapter 6, are designed to guarantee that these methods actually do create sets. These new methods of creating sets will also provide us with many opportunities to practice element arguments.

²Fan Chung Graham (b. 1949 -) has done major work in combinatorics and graph theory. She is a member of the American Academy of Arts and Sciences

5.1 Subsets

Heisenberg: “What something means is what it means in mathematics.”

Bohr: “You think that so long as the mathematics works out, the sense doesn’t matter.”

Heisenberg: “Mathematics *is* sense! That’s what sense is!”

Bohr: “But in the end, in the end, remember, we have to be able to explain it all to Margrethe!”

Margrethe: “Explain it to me? You couldn’t even explain it to each other! You went on arguing into the small hours every night! You both got so angry!”

– Michael Frayn, *Copenhagen*¹

Recall that if A and B are sets, we say that $A \subset B$ if and only if for all $a \in A$, we also have $a \in B$. Predicates give us a powerful method for creating subsets. If $P(x)$ is a predicate and if B is a set, then

$$A = \{x \in B : P(x)\}$$

will be a subset of B with the property that $x \in A$ if and only if $x \in B$ and $P(x)$ is true. Several of the methods for building sets that we will introduce later are particular versions of this subset construction.

¹ *Copenhagen* is a play that imagines an after-death conversation between the physicists Werner Heisenberg and Niels Bohr. Margrethe is Bohr’s wife. [49]

5.1.1

Example

The set $A = \{x \in \mathbb{R} : x^2 - x \geq 7\}$ is a subset of \mathbb{R} since every $a \in A$ is a real number and " $x^2 - x \geq 7$ " is a predicate. Similarly, the set $X = \{x \in \mathbb{R} : |x| > 1\}$ is also a subset of \mathbb{R} . We can verify that $A \subset X$, using an element argument as follows. See Figure 5.1 for a diagram¹. Notice that our proof uses element arguments.

Proof. Suppose that $a \in A$. We will show that $a \in X$.

By the definition of A , $a^2 - a \geq 7$. This implies that $a^2 - a - 7 \geq 0$. Using the quadratic formula to factor, we see that

$$\left(a - \frac{1 + \sqrt{29}}{2}\right)\left(a - \frac{1 - \sqrt{29}}{2}\right) \geq 0.$$

The product of two real numbers is non-negative exactly when both are non-negative or both are non-positive. Since $\frac{1+\sqrt{29}}{2} > \frac{1-\sqrt{29}}{2}$, we conclude that either

$$a \geq \frac{1 + \sqrt{29}}{2} = 3.19\dots$$

or

$$a \leq \frac{1 - \sqrt{29}}{2} = -2.19\dots$$

In either case, observe that $|a| > 1$. Thus, by the definition of X , $a \in X$. Since $a \in A$ was arbitrary, $A \subset X$. □

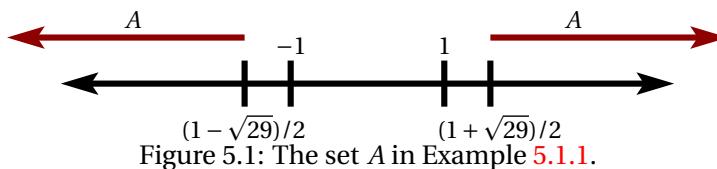


Figure 5.1: The set A in Example 5.1.1.

¹But remember a diagram isn't a proof!

5.2 Complements

Bill Bailey: “What is the opposite of nothing? Is it anything, something, or everything?”

Frank Close: “The answer is ‘yes.’ ”

- *The Museum of Curiosity* 1.4.

The most foundational statement in mathematics (for a fixed x and A) is: $x \in A$. Its negation, of course, is: $x \notin A$. These statements have analogues for sets.

5.2.1

Definition ▶ Complement

Suppose that A is a set and that $A \subset U$ for some set U . The **complement** of A (in U) is the subset, denoted A^C , such that $x \in A^C$ if and only if $x \notin A$ and $x \in U$.

Figure 5.2 shows a picture of a complement. Such a picture is an example of a **Venn diagram**¹. Venn diagrams can be helpful, but unless you are literally proving a theorem about dots on a page, drawing a Venn diagram does not constitute an adequate method of proof.

We must have a superset U in mind when taking the complement of A , since the object $\{x : x \notin A\}$ is not a set². Notice that, although the complement A^C of A is defined in terms of the superset U , the “ U ” doesn’t show up in the notation A^C . We could rectify this by using A_U^C instead (or something similar) but in almost all circumstances the superset U will be clear from the context or will not matter much. Nonetheless – when using complements, be sure you know what the superset is!

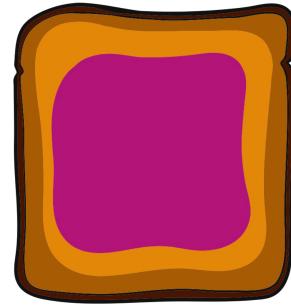


Figure 5.2: The complement of the region of the toast covered in jam is the region of the toast without any spread together with the region of the toast covered in peanut butter, but not in jam.

Remark 5.2.1. Set complements are directly related to negations of predicates. Suppose that U is a set and that A is the subset of all elements x of U satisfying some predicate $P(x)$. Then A^C is the subset of all elements x of U satisfying the predicate $\neg P(x)$.

5.2.2

Example

The complement of the interval $(-1, 3) \subset \mathbb{R}$ is the set

$$\{x \in \mathbb{R} : x \leq -1 \text{ or } x \geq 3\}.$$

¹Although, we should say that not everyone draws them to look like toast!

²The proof is like the proof of Russell’s paradox.

5.2.3

Example

Consider the set $A \subset \mathbb{R}^2$ defined by $A = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 < 1\}$. The set A is the unit disc centered at the origin, not including the boundary circle S^1 . The set A^C is the set of all points $(x, y) \in \mathbb{R}^2$ such that $x^2 + y^2 \geq 1$. This is the set of all points outside the unit disc, but including the circle S^1 .

5.2.4

Exercise

Prove that $(A^C)^C = A$. Remember that you need to show $(A^C)^C \subset A$ and $A \subset (A^C)^C$.

5.2.5

Exercise

Prove that if $A \subset B$ then $B^C \subset A^C$ (where the complement is taken relative to any set U such that $A \subset U$ and $B \subset U$). Notice that you are asked to prove an implication involving sets! You should use the appropriate proof structure for an implication and, inside that, use element arguments.

If A and B are sets, it also makes sense to look at just the elements of A that are not in B , even if B is not a subset of A . We call this set the “relative complement” of B in A .

5.2.6

Definition ▶ Relative Complement

Suppose that A and B are sets. The **complement** of B relative to A is:

$$A \setminus B = \{x \in A : x \notin B\}$$

The complement of B in A is also called the **set difference** of A and B and can also be denoted $A - B$. Figure 5.3 shows a Venn diagram of a relative complement.

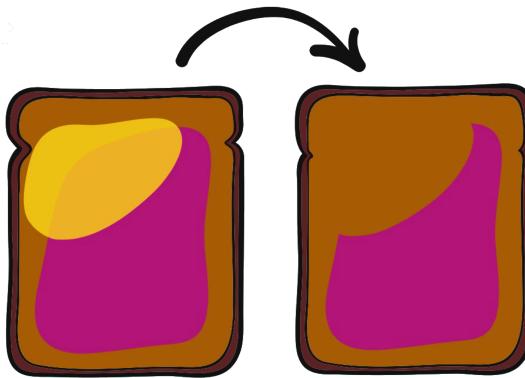


Figure 5.3: The left shows a piece of toast, part of which is covered with butter (call that part B) and part of which is covered in jam (call that part J). Some portions are covered in both. The set difference $J \setminus B$ is shown on the right. It is the portions of the toast that are covered in jam, but not in butter.

5.3 Intersections

“Using intersection overlay: Sometimes, you want to know which polygon features are shared by each of the polygons you’re searching. In other words, instead of combining pieces of land for sale with lands that are agricultural, you only want to know which agricultural lands you can buy. You can get this information by using a logical AND search, which needs both categories to exist before it returns a value to the output map. This search typically reduces the size of the area retrieved . . .”

– Michael M. DeMers, *GIS for Dummies*¹ [34]

Some students at a college are math majors; some are computer science majors; some are art majors. Perhaps some are even all three! The set of students who triple majoring in math, computer science, and art is the intersection of the set of students who are math majors, the set who are computer science majors, and the set who are art majors. More generally, whenever we have a set \mathcal{A} such that each element $A \in \mathcal{A}$ is a set we can consider those elements that are elements of every one of the sets $A \in \mathcal{A}$. Informally, the intersection of a bunch of sets consists of those elements common to *all* the sets in the bunch. Just as complements correspond to negations, intersections correspond to the universal quantifier.

5.3.1

Definition ▶ Intersection

Suppose that A_λ is a set for every $\lambda \in \Lambda$ (where Λ is some nonempty index set). The **intersection** of all the A_λ is the set, denoted by $\bigcap_{\lambda \in \Lambda} A_\lambda$, such that $x \in \bigcap_{\lambda \in \Lambda} A_\lambda$ if and only if, for all $\lambda \in \Lambda$, we have $x \in A_\lambda$.

5.3.2

Example

Suppose that $A_1 = \{1\}$, $A_2 = \{1, 2\}$, and, more generally, $A_n = \{1, 2, 3, \dots, n\}$ for all $n \in \mathbb{N}$. Then

$$\bigcap_{n \in \mathbb{N}} A_n = \{1\}$$

since 1 is the only element common to every A_n .

5.3.3

Example

Define:

$$\begin{aligned} A_1 &= \{1, 2, 3, 4, 5\} \\ A_2 &= \{3, 4, 5, 6, 7, 8\} \\ A_3 &= \{4, 5, 10, 15\} \end{aligned}$$

¹GIS stands for “Geographic Information Systems;” these are software used throughout the social and natural sciences for making maps.

5.3.3

Then

$$\bigcap_{\lambda \in \{1, 2, 3\}} A_\lambda = \{4, 5\}.$$

To see this, we check that both 4 and 5 are elements of A_1 , A_2 , and A_3 and that nothing else is an element of all three sets.

If we are interested in the intersection of just two sets, say A_1 and A_2 , we will write $A_1 \cap A_2$ instead of $\bigcap_{n \in \{1, 2\}} A_n$. Figure 5.4 shows a Venn diagram of the intersection of two sets.

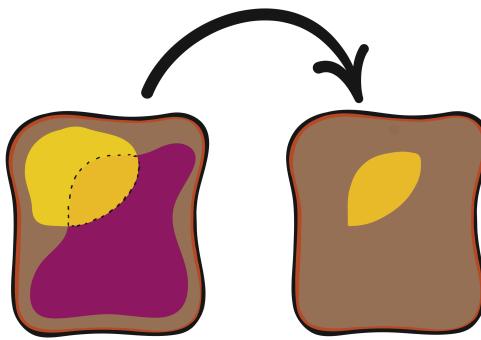


Figure 5.4: Part of the toast (call it B) is covered in butter and part of it (call it J) is covered in jam. The intersection $J \cap B$ is shown on the right.

Similarly, if we have a finite number of sets A_1, A_2, \dots, A_n , we can write their intersection as $A_1 \cap \dots \cap A_n$ or $\bigcap_{j=1}^n A_j$. Going one step further, if we have a set A_j for every $j \in \mathbb{N}$, we can write the intersection of all those sets as

$$\bigcap_{j \in \mathbb{N}} A_j \text{ or } \bigcap_{j=1}^{\infty} A_j \text{ or } A_1 \cap A_2 \cap \dots$$

This is much like how infinite sums are written in Calculus. Not every intersection can be written out as a list, however. Here is one typical example.

5.3.4

Example

For each $r \in \mathbb{R}$, let $A_r = (r - \frac{1}{2}, r + \frac{1}{2}) \subset \mathbb{R}$. Then

$$\bigcap_{r \in \mathbb{R}} A_r = \emptyset$$

since no real number is an element of **every** open interval of length 1.

The next example adapts the notation to deal with the case where we want to index by just the positive real numbers. We include the full proof for completeness and to give another example of element arguments and a proof by contraposition.

5.3.5

Example

For each $r > 0$, let A_r be the interval $(-1 - r, 1 + r) \subset \mathbb{R}$. Then

$$\bigcap_{r>0} A_r = [-1, 1].$$

To see this, we do two element arguments. Before starting, observe that the statement $x \notin \bigcap_{r>0} A_r$ is equivalent to the statement: “There exists $r > 0$ such that $x \notin A_r$.” Also, for notational convenience, let $A = \bigcap_{r>0} A_r$ and recall that some element $x \in A$ if and only if $x \in A_r$ for every $r > 0$.

Proof. \supseteq : We will show that $A \supseteq [-1, 1]$.

Suppose that $x \in [-1, 1]$. We will show that $x \in A$. We do this by showing that $x \in A_r$ for every $r > 0$.

For all $r > 0$, we have:

$$\begin{aligned} -1 - r &< -1, \text{ and} \\ 1 &< 1 + r \end{aligned}$$

Thus, by definition of interval notation, we have $[-1, 1] \subset (-1 - r, 1 + r)$ for every $r > 0$. Since $x \in [-1, 1]$, by definition of subset, we also have $x \in (-1 - r, 1 + r) = A_r$ for every $r > 0$. Thus, $x \in A$. Since we chose $x \in [-1, 1]$ arbitrarily, $[-1, 1] \subset A$.

\subseteq : We will show that $A \subseteq [-1, 1]$. We need to show that if $x \in A$ then $x \in [-1, 1]$. We prove the contrapositive.

Suppose that x is a real number such that $x \notin [-1, 1]$. We will show that $x \notin A$. That is, we must show that there exists an r such that $x \notin A_r$.

If $x > 1$, let $r = (x - 1)/2$ and, as in Figure 5.5, notice that

$$1 < 1 + r < x.$$

Thus, for this value of r ,

$$x \notin (-1 - r, 1 + r)$$

and so $x \notin A$. Similarly, if $x < -1$, let $r = (-x - 1)/2$. Notice that $r > 0$ and that

$$x < -1 - r < -1.$$

Thus, for this value of r ,

$$x \notin (-1 - r, 1 + r)$$

and so $x \notin A$.

Consequently, if $x \notin [-1, 1]$, then $x \notin A$. Therefore, if $x \in A$, then $x \in [-1, 1]$. We conclude that $\bigcap_{r>0} A_r = [-1, 1]$ as desired. \square

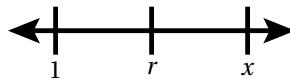


Figure 5.5: The number r when $x > 1$, for the second half of the proof in Example 5.3.5.

5.3.6 Exercise

In Example 5.3.5, identify all the different types of proof that are used and compare the written proof to the proof-outlines for each type.

Here are a few to try for yourself.

5.3.7 Exercise

For each $p \in \mathbb{N}$, let $p\mathbb{Z}$ be the set of those integers that are multiples of p . Prove that

$$\bigcap_{p \in \mathbb{N}} p\mathbb{Z} = \{0\}.$$

5.3.8 Exercise

For each $t \in (2, \infty) \subset \mathbb{R}$, let $A_t = [1, t] \subset \mathbb{R}$. Prove that

$$\bigcap_{t \in (2, \infty)} A_t = [1, 2]$$

5.3.9 Exercise

For a point $a = (a_0, a_1) \in \mathbb{R}^2$, let $B_1(a)$ be the closed disc in \mathbb{R}^2 of radius 1 centered at a . That is,

$$B_1(a) = \{(x, y) \in \mathbb{R}^2 : (a_0 - x)^2 + (a_1 - y)^2 \leq 1\}.$$

Find $\bigcap_{a \in \mathbb{R}^2} B_1(a)$.

5.3.10 Exercise

For $\theta \in [0, 2\pi]$, let

$$H_\theta = \{(x, y) \in \mathbb{R}^2 : y \sin \theta \leq 1 - x \cos \theta\}.$$

Find $\bigcap_{\theta \in [0, 2\pi]} H_\theta$.

(Hint: the tangent line to the unit circle at the point $(\cos \theta, \sin \theta)$ has equation $y \sin \theta = 1 - x \cos \theta$.)

Sometimes, it is inconvenient to have to write intersections using an index set. There is a way around it. Suppose that \mathcal{H} is a non-empty set such that every

element $H \in \mathcal{H}$ is a set. Then we denote the intersection of all the sets $H \in \mathcal{H}$ by

$$\bigcap_{H \in \mathcal{H}} H.$$

Observe that $x \in \bigcap_{H \in \mathcal{H}} H$ if and only if, for every $H \in \mathcal{H}$, $x \in H$.

5.3.11 Example

Let \mathcal{H} be the set whose elements are the graphs of the equations $y = x^2 + 1$, $y = 1$, and $y = -x^2 + 1$ in \mathbb{R}^2 . Then

$$\bigcap_{H \in \mathcal{H}} H = \{(0, 1)\}$$

since the point $(0, 1)$ is an element of each of those graphs and is, in fact, the only point of \mathbb{R}^2 common to all those graphs.

5.3.12 Warning

The notation

$$\bigcap_{H \in \mathcal{H}} H$$

has two dangers. The first is simply conceptual while the second is logical. The conceptual danger is that it is easy to confuse the set \mathcal{H} with the sets H . It is best to think of \mathcal{H} as a backpack containing the sets H which are to be intersected. For example, if $\mathcal{H} = \{H_1, H_2, H_3\}$, then

$$\bigcap_{H \in \mathcal{H}} H = H_1 \cap H_2 \cap H_3.$$

This notation is analogous to notation such as the following, which is much like that typically seen in Calculus:

$$\sum_{k \in \{1, 2, 3\}} 5^k = 5 + 5^2 + 5^3.$$

Secondly, when we write

$$\bigcap_{H \in \mathcal{H}} H$$

it is important that the set \mathcal{H} be non-empty. That is, to find the intersection of some sets, we should actually have some sets to intersect. It is fine, however, for one or more of the elements of \mathcal{H} to be the empty set. Indeed, if one or more of the elements of \mathcal{H} is empty, then the intersection

$$\bigcap_{H \in \mathcal{H}} H.$$

will be the empty set.

5.3.13

Theorem

Suppose that \mathcal{H} is a nonempty set such that each $H \in \mathcal{H}$ is a set. Then for all $A \in \mathcal{H}$,

$$\bigcap_{H \in \mathcal{H}} H \subset A.$$

Consequently, if $A \subset X$ for some set $A \in \mathcal{H}$ and some set X , then also

$$\bigcap_{H \in \mathcal{H}} H \subset X$$

5.3.14

Theorem

Suppose that \mathcal{H} is a non-empty set such that each $H \in \mathcal{H}$ is a set. Let U be any set. Prove that

$$U \subset \bigcap_{H \in \mathcal{H}} H$$

if and only if $U \subset H$ for all $H \in \mathcal{H}$.

5.4 Unions

“We the People of the United States, in Order to form a more perfect Union ...”

- Preamble to the Constitution of the United States.

In the previous section, we defined the intersection of sets to be the set of elements appearing in *every* one of the sets. The union of the sets is defined by replacing the “every” with “some”. That is, we replace the universal quantifier with the existential quantifier.

5.4.1

Definition ▶ Unions of Sets

Suppose that A_λ is a set for every element λ of some index set Λ . The **union** of all the A_λ is the the set, denoted by $\bigcup_{\lambda \in \Lambda} A_\lambda$, such that $x \in \bigcup_{\lambda \in \Lambda} A_\lambda$ if and only if there exists $\lambda \in \Lambda$ such that $x \in A_\lambda$.

Figure 5.6 shows a Venn diagram of the union of two sets.

5.4.2

Example

Let $A_1 = \{1, 3, 5\}$, $A_2 = \{3, 5, 9\}$, and $A_3 = \{25\}$. Then,

$$\bigcup_{n \in \{1, 2, 3\}} A_n = \{1, 3, 5, 9, 25\}.$$

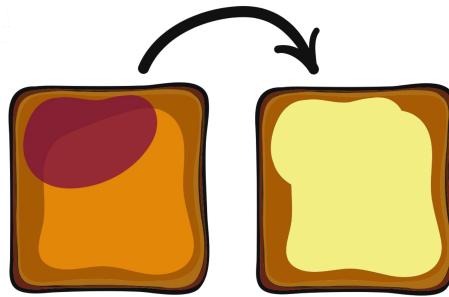


Figure 5.6: On the left piece of toast, part (call it J) is covered with jam and part (call it PB) with peanut butter. The union $J \cup PB$ is the yellow region on the right piece of toast.

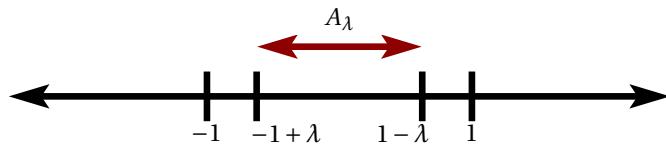


Figure 5.7: The sets A_λ in Example 5.4.6.

As with intersections, we will sometimes vary our notation. If A_1 and A_2 are two sets we will write $A_1 \cup A_2$ for their union. If A_1, \dots, A_n are sets we will write either $A_1 \cup \dots \cup A_n$ or $\bigcup_{j=1}^n A_j$ for their union. If A_n is a set for each $n \in \mathbb{N}$, we will write either $A_1 \cup A_2 \cup \dots$ or $\bigcup_{n \in \mathbb{N}} A_n$ or $\bigcup_{n=1}^{\infty} A_n$ for their union.

5.4.3 Example

Suppose that $A_n = \{2n - 1, 2n + 1\}$ for each $n \in \mathbb{N}$. Then $\bigcup_{n \in \mathbb{N}} A_n$ is equal to the set of odd natural numbers.

5.4.4 Example

Let $A_n = \{-n, -(n-1), \dots, -3, -2, -1, 0, 1, 2, 3, \dots, n\}$. (So, for instance, $A_3 = \{-3, -2, -1, 0, 1, 2, 3\}$.) Then $\bigcup_{n \in \mathbb{N}} A_n = \mathbb{Z}$.

5.4.5 Example

For each $r \in \mathbb{R}$, let $A_r = (r - \frac{1}{2}, r + \frac{1}{2}) \subset \mathbb{R}$. Then

$$\bigcup_{r \in \mathbb{R}} A_r = \mathbb{R}$$

since every real number is an element of **some** open interval of length 1.

We give a more complete proof for the next example. It is similar to Example 5.3.5.

5.4.6

Example

Let $\Lambda = (0, 1)$. For each $\lambda \in \Lambda$, let $A_\lambda = [-1 + \lambda, 1 - \lambda]$. We claim that

$$\bigcup_{\lambda \in \Lambda} A_\lambda = (-1, 1).$$

We use two element arguments to show this. See Figure 5.7. For notational convenience, let $A = \bigcup_{\lambda \in \Lambda} A_\lambda$. Recall that $x \in A$ if and only if $x \in A_\lambda$ for some $\lambda \in (0, 1)$.

\supseteq : We will show that $A \supset (-1, 1)$.

Suppose that $x \in (-1, 1)$. We wish to show that $x \in A$. By the definition of union, it suffices to show that there is $\lambda \in (0, 1)$ such that

$$x \in [-1 + \lambda, 1 - \lambda].$$

We will choose our λ so that $\pm(1 - \lambda)$ is the number halfway between x and ± 1 .

If $x \geq 0$, let $\lambda = (1 - x)/2$. If $x < 0$, let $\lambda = (x + 1)/2$. In either case, observe that $\lambda \in (0, 1)$. If $x \geq 0$, by elementary algebra, we have

$$0 \leq x \leq 1 - \lambda.$$

If $x < 0$, we have, by elementary algebra,

$$-1 + \lambda \leq x < 0.$$

Thus, in either case, $x \in [-1 + \lambda, 1 - \lambda]$ for our choice of $\lambda \in \Lambda$. Hence, $x \in A$.

\subseteq : We will show that $\bigcup_{\lambda \in \Lambda} A_\lambda \subseteq (-1, 1)$.

Suppose that $x \in A$. We wish to show that $x \in (-1, 1)$. By the definition of union, there exists $\lambda \in \Lambda$, such that $x \in [-1 + \lambda, 1 - \lambda]$. Since $\Lambda = (0, 1)$,

$$-1 < -1 + \lambda < 0 \text{ and } 0 < 1 - \lambda < 1.$$

Hence, $x \in (-1, 1)$, as desired.

Therefore, $\bigcup_{\lambda \in \Lambda} A_\lambda = (-1, 1)$. □

5.4.7

Exercise

Let $\Lambda = (0, \infty) \subset \mathbb{R}$. Let $B_\lambda = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 \leq \lambda^2\}$. Find $\bigcup_{\lambda \in \Lambda} B_\lambda$ and $\bigcap_{\lambda \in \Lambda} B_\lambda$.

5.4.8

Exercise

Suppose that $a, b, c, d \in \mathbb{R}$ with $a < b$ and $c < d$. Prove that either $(a, b) \cap (c, d) = \emptyset$ or that there exists $e, f \in \mathbb{R}$ with $e < f$ and

$$(a, b) \cup (c, d) = (e, f)$$

5.4.9

Exercise

For each $r \in \mathbb{Q}$, let $A_r = (r - \frac{1}{2}, r + \frac{1}{2}) \subset \mathbb{R}$. Show that

$$\bigcup_{r \in \mathbb{Q}} A_r = \mathbb{R}$$

(Hint: You need to explain why every real number is within $1/2$ of some rational number. You might like to use the fact that all real numbers have decimal representations.)

5.4.10

Theorem

Let X be a set. Suppose that for all $\lambda \in \Lambda$, the set $A_\lambda \subset X$. Then

$$\bigcup_{\lambda \in \Lambda} A_\lambda \subset X.$$

5.4.11

Theorem

Suppose that \mathcal{H} is a set and that for some $H' \in \mathcal{H}$, we have a subset $V \subset H'$. Then

$$V \subset \bigcup_{H \in \mathcal{H}} H.$$

5.4.12

Exercise

Suppose that \mathcal{H} is a set and that there is a subset

$$V \subset \bigcup_{H \in \mathcal{H}} H.$$

Must it be the case that there exists $H' \in \mathcal{H}$ such that $V \subset H'$? Why or why not?

We can combine unions, intersections, and complements in interesting ways. The following exercises and theorems are good opportunities to practice element arguments.

5.4.13

Exercise ▶ (Distributive Properties)

Let A, B , and C be sets. Prove the following distributive laws:

1. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

5.4.13

$$2. A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Can you formulate and prove versions of these results that involve arbitrarily many sets?

5.4.14

Theorem ▶ DeMorgan's Laws

Suppose that \mathcal{A} is a set such that each element $A \in \mathcal{A}$ is a subset of some fixed set. Then:

$$1. \left(\bigcup_{A \in \mathcal{A}} A \right)^c = \bigcap_{A \in \mathcal{A}} (A^c)$$

$$2. \left(\bigcap_{A \in \mathcal{A}} A \right)^c = \bigcup_{A \in \mathcal{A}} (A^c)$$

5.5 Power Sets

“Modern mathematics has emerged from a long series of conceptual reforms tending towards greater generality and rigour, as well as from more radical conceptual inventions opening up altogether new perspectives. The acceptance of such conceptual innovations is a self-modifying mental act in search of a truer intellectual life.”

—Michael Polanyi [102]

Power sets are a convenient tool for turning subsets into elements. Our ability to create power sets turns out to have a number of surprising consequences, some of which we explore in Chapter 10.

5.5.1

Definition

If X is a set then the **power set** $\mathcal{P}(X)$ of X is the set such that $A \in \mathcal{P}(X)$ if and only if $A \subset X$.

Observe that no matter what the set X is, the empty set \emptyset is an element of $\mathcal{P}(X)$.

5.5.2

Example

Here are several examples of power sets:

- $\mathcal{P}(\emptyset) = \{\emptyset\}$ (Observe $\mathcal{P}(\emptyset) \neq \emptyset$.)
- $\mathcal{P}(\{a\}) = \{\emptyset, \{a\}\}$
- $\mathcal{P}(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$
- $\mathcal{P}(\{a, b, c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$

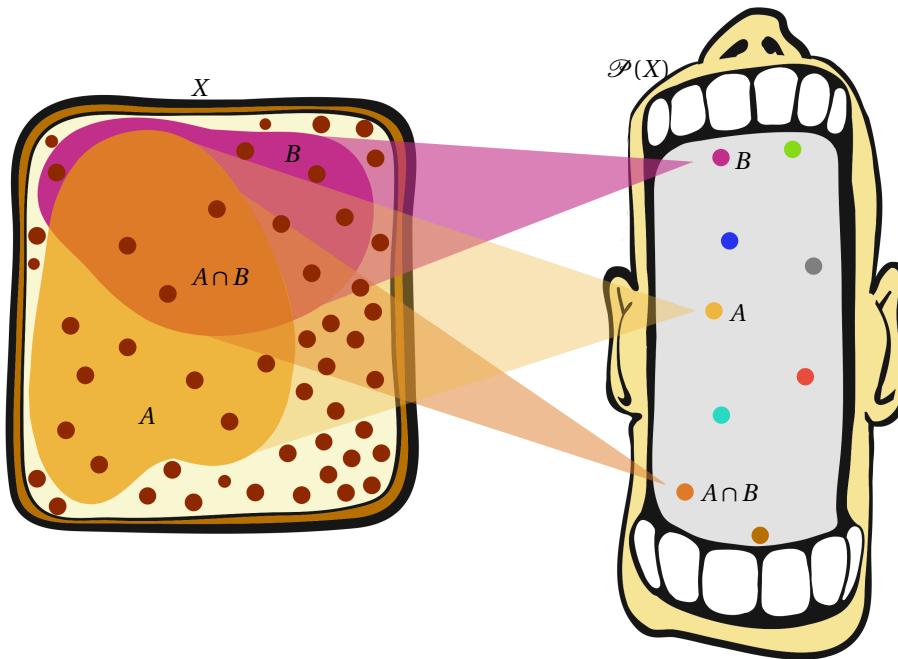


Figure 5.8: One way to attempt to visualize the power set is that if we zoom in on a point of the power set $\mathcal{P}(X)$ we see a subset of X . For every subset of X (including the empty set) there is a point of $\mathcal{P}(X)$ such that zooming in on the point gives us the subset.

In Figure 5.8, we present an attempt at visualizing the power set of a set X : zooming in on a point of $\mathcal{P}(X)$ lets us see a subset of X and for every subset $A \subset X$ there is some point of $\mathcal{P}(X)$ such that zooming in on it shows us the set A .

5.5.3 Exercise

Let $X = \{a, b, 1, 2\}$. Write down all the elements of $\mathcal{P}(X)$. Also write down 7 elements of $\mathcal{P}(\mathcal{P}(X))$.

5.5.4 Exercise

If X has $n \in \mathbb{N}$ elements, how many elements do you think $\mathcal{P}(X)$ will have? Can you prove it?

5.5.5 Exercise

Suppose that \mathcal{H} is a set such that each element $H \in \mathcal{H}$ is a set. Prove the following:

1. $\bigcup_{H \in \mathcal{H}} \mathcal{P}(H) \subset \mathcal{P}\left(\bigcup_{H \in \mathcal{H}} H\right)$.
2. $\bigcap_{H \in \mathcal{H}} \mathcal{P}(H) = \mathcal{P}\left(\bigcap_{H \in \mathcal{H}} H\right)$.

3. If $\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)$, then either $A \subset B$ or $B \subset A$.

Can you generalize this last fact to more than two sets?

5.6 Cartesian Products

“I would encourage any young mathematician thinking of working on applications to learn as much pure mathematics as possible, limited only by appetite and time, not by how applicable they think it might be. I believe that I have used in my own career all the mathematics I understand, I just wish I knew more, and that I still had the time to learn more. On the other hand, I have also found that great joy comes from working with others. Experiencing the give-and-take of half-baked ideas that then are given substance through the collaborative effort is exhilarating.”

– Ingrid Daubechies¹, *Advice to Young Women* [104]

The plane \mathbb{R}^2 is the natural setting for much of Calculus and the Cartesian coordinates (x, y) of a point in \mathbb{R}^2 play an important role. In many mathematical settings, it is natural to consider pairs of elements from two, possibly different, sets, much as \mathbb{R}^2 is the set of pairs of real numbers.

5.6.1

Definition ► Ordered Pairs and the Cartesian Product

If X and Y are sets and if $x \in X$ and $y \in Y$, then (x, y) is an **ordered pair** of elements from X and Y . We define $(x, y) = (a, b)$ if and only if $x = a$ and $y = b$. The **Cartesian product** $X \times Y$ is the set of all ordered pairs of (x, y) with $x \in X$ and $y \in Y$. That is, $z \in X \times Y$ if and only if there exist $x \in X$ and $y \in Y$ so that $z = (x, y)$.

5.6.2

Example ► (The annulus)

Let S^1 denote the unit circle $\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$. The **annulus** or cylinder is the set $S^1 \times [0, 1]$, where $[0, 1]$ is the closed interval in \mathbb{R} . The top of the cylinder is the set $S^1 \times \{1\}$ and the bottom of the cylinder is the set $S^1 \times \{0\}$. A pair (θ, t) gives us a position θ on the circle and a height t . Figure 5.9 visualizes the cylinder in \mathbb{R}^3 .

¹Ingrid Daubechies (b. 1954) is an applied mathematician whose work is important to JPEG2000 image compression standard. She has received many awards and is currently President of the International Mathematical Union.

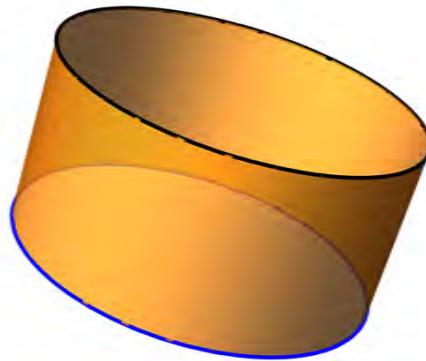


Figure 5.9: The annulus (or cylinder) is the Cartesian product $S^1 \times [0, 1]$. The blue curve on the rim is $S^1 \times \{0\}$ and the black curve on the rim is $S^1 \times \{1\}$.

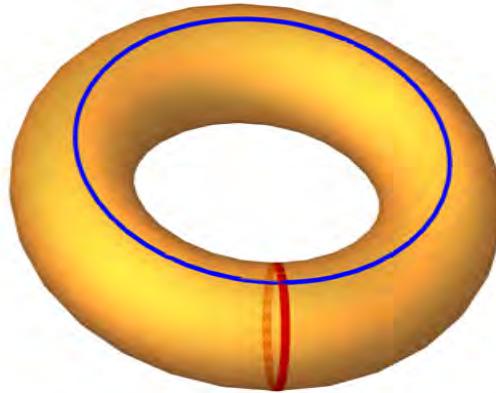


Figure 5.10: A 2-dimensional picture of a torus in \mathbb{R}^3 . The red and blue curves represent $S^1 \times \{(1, 0)\}$ and $\{(1, 0)\} \times S^1$.

5.6.3 Example ▶ (The torus)

Let S^1 denote the unit circle $\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$. The **torus** is the set $T^2 = S^1 \times S^1$. It is a subset of $\mathbb{R}^2 \times \mathbb{R}^2$. The element $((\sqrt{2}/2, \sqrt{2}/2), (\sqrt{3}/2, 1/2))$, for example, is an element of T^2 .

Even though T^2 , according to the definition above, naturally lives in a 4-dimensional space, with some distortion we can visualize it in \mathbb{R}^3 as in Figure 5.10. Incidentally, observe that technically $\mathbb{R}^4 \neq \mathbb{R}^2 \times \mathbb{R}^2$ because $((1, 2), (3, 4)) \in \mathbb{R}^2 \times \mathbb{R}^2$ is not an element of \mathbb{R}^4 and, on the other hand, $(1, 2, 3, 4) \in \mathbb{R}^4$ is not an element of $\mathbb{R}^2 \times \mathbb{R}^2$. However, as the only difference between the elements of $\mathbb{R}^2 \times \mathbb{R}^2$ and the elements of \mathbb{R}^4 is the placement of parentheses, most mathematicians are content to ignore the distinction. In particular, any useful result for $\mathbb{R}^2 \times \mathbb{R}^2$ can be converted into a corresponding result for \mathbb{R}^4 and vice versa.

Why is the set of ordered pairs called a product? Does it bear any relationship

to the multiplication of numbers? It turns out that taking the Cartesian product with the empty set is sort of like multiplying a real number by 0:

5.6.4

Theorem

Let Y be any set. Prove that $\emptyset \times Y = \emptyset$ and $Y \times \emptyset = \emptyset$.

The analogue of multiplying a real number by 1 is taking the Cartesian product with a set containing one element. For example, for any non-empty set X , the elements of $X \times \{1\}$ are all ordered pairs of the form $(x, 1)$ for some $x \in X$. Given a result for X , it is easy to translate it into a result for $X \times \{1\}$ and vice versa. The analogy between the product of real numbers and the Cartesian product of sets breaks down at this point since there are many different one-element sets, while there is only one real number 1. The analogy also breaks down when we consider commutativity.

5.6.5

Theorem

Suppose that X and Y are non-empty sets. Prove that $X \times Y = Y \times X$ if and only if $X = Y$.

If the Cartesian product of two sets is like (in a very limited way) the multiplication of real numbers, is there any operation which is like a sum? There is - it's called the disjoint union of two sets.

5.6.6

Definition

Suppose that X and Y are sets, possibly with $X \cap Y \neq \emptyset$. Let $X' = X \times \{0\}$ and $Y' = Y \times \{1\}$, then $X' \cap Y' = \emptyset$. (Prove this!). The set $X' \cup Y'$ is sometimes called the **disjoint union** of X and Y with X' and Y' considered as copies of the sets X and Y respectively. The disjoint union of X and Y is sometimes denoted $X \sqcup Y$.

Notice that, for any set X , the set $X \sqcup \emptyset = X \times \{0\}$. We previously argued that the Cartesian product of X with any one element set produces a set functionally equivalent to X . Thus, \emptyset is a type of additive identity for sets under the operation of disjoint union.

5.6.7

Exercise

Let A , B , and C be sets. Explain why the set $A \times (B \sqcup C)$ is essentially the same set as $(A \times B) \sqcup (A \times C)$. Thus, a version of the distributive property holds for the Cartesian product and disjoint union.

There is a close connection between Cartesian products and functions, which we explore more in Chapter 8. For now, consider the kind of functions studied in pre-calculus and calculus. These are functions f which have \mathbb{R} as their domain and which also produce values in \mathbb{R} (that is, \mathbb{R} is also the codomain). We express this by writing $f: \mathbb{R} \rightarrow \mathbb{R}$. For example, the function $f: \mathbb{R} \rightarrow \mathbb{R}$ defined by $f(x) = x^3 + 5$ is such a function. You learned to graph such functions by making marks

on the Cartesian plane $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$. To graph the function f , we mark a point $(x, y) \in \mathbb{R} \times \mathbb{R}$ if and only if $y = f(x)$. For example, if $f(x) = x^3 + 5$ for every $x \in \mathbb{R}$, then the points $(0, 5)$, $(-1, 4)$, and $(1, 6)$ (among many others) would be marked, whereas the points $(0, 7)$, $(2, -3)$, $(-3, 0)$ (among many others) remain unmarked. Thus, the **graph** of a function $f: \mathbb{R} \rightarrow \mathbb{R}$ is the subset $G \subset \mathbb{R}^2$ such that $(x, y) \in G$ if and only if $y = f(x)$. In calculus, you likely also studied function $f: \mathbb{R}^2 \rightarrow \mathbb{R}$. These are functions like $f(x, y) = \cos(xy) + y^2$ which have \mathbb{R}^2 as their domain and \mathbb{R} as their codomain. The graph of such a function is the subset $G \subset \mathbb{R}^2 \times \mathbb{R}$ such that $((x, y), z) \in G$ if and only if $z = f(x, y)$. The graph of such a function is visualized by identifying \mathbb{R}^3 with $\mathbb{R}^2 \times \mathbb{R}$ and marking those points (x, y, z) such that $z = f(x, y)$. Inspired by our work in Calculus, we can also consider functions $f: X \rightarrow Y$ between any two sets X and Y . The graph of f is then the subset $G \subset X \times Y$ such that $(x, y) \in G$ if and only if $y = f(x)$.

5.6.8 Exercise

Let $f: [0, 1] \rightarrow [0, 1]$ be the function defined by $f(x) = \frac{2x}{x^2+1}$ for every $x \in [0, 1]$. Draw the graph of f in $[0, 1] \times [0, 1]$.

5.6.9 Exercise

Let $f: ([0, 1] \times [0, 1]) \rightarrow ([0, 1] \times [0, 1])$ be the function defined by

$$f(x, y) = \left(\frac{2x}{x^2+1}, \sin(\pi y) \right).$$

List six elements in the graph of f and two elements not in the graph of f . Explain why each is or is not an element of the graph of f .

5.7 The persistence of structure

"If this argument frustrates you, if your reaction is that the argument is much ado about nothing or if the argument is too abstract for you, you have a point. In fact I am taking a chance in using this example, because I may just succeed in "turning off" my reader just as so many students are turned off in theoretical courses in pure mathematics. It is difficult to understand what is going on in this proof precisely because this kind of argument is all at the formal, logical level. The point of the example is that one can follow the logic of the definitions and argument without knowing anything about the subject, with no experience with anything connected to the subject, and therefore certainly no intuition of 'feel for the subject.' ... Verification is one thing, understanding is quite another."

– William Byers, *How Mathematicians Think* [22]

We saw in Chapter 1 that to study number systems and different kinds of spaces, we can put additional structure (i.e. impose additional axioms) on sets. In this

section we explore a few ways that intersections, unions, and Cartesian products interact with some of those structures, as well as some new structures. At a first read through these examples will all seem very different from each other (and, perhaps, very difficult). With multiple rereadings, however, you should start to see how similar the proofs in each of the following subsections are, even though the definitions and contexts change. The opening quote from William Byers concerns Theorem 5.7.8 below. Despite his claim that its proof is completely formal, its proof, as well as the others in this section, does contain important ideas. Those ideas are:

1. The properties of mathematical objects will sometimes persist to combinations of those objects,
2. Unless we verify that those properties persist, using the precise definitions defining those properties and objects, there is no guarantee that they persist.

But we are best off, jumping in and seeing the examples. If you master the proofs in this subsection, you will have a coherent deep understanding of how to use unions and intersections.

Convexity

One goal in all of mathematics and science is to explain complicated things in terms of simpler things. Subsets of \mathbb{R}^2 don't get much simpler than half planes. In this section, we explore which subsets of \mathbb{R}^2 are the intersection of half planes. This will lead us into a discussion of convex subsets of \mathbb{R}^2 . Convex sets (in both \mathbb{R}^2 and other metric spaces) are important in their own right and play an important role in mathematics; especially in geometry, analysis, and optimization theory.

A **line** in \mathbb{R}^2 is a set of points of the form $\{(x, y) \in \mathbb{R}^2 : Ax + By = C\}$ for some $A, B, C \in \mathbb{R}$, with at least one of A or B not equal to 0. Every line ℓ in \mathbb{R}^2 divides \mathbb{R}^2 into two half planes Π_1 and Π_2 such that $\Pi_1 \cap \Pi_2 = \ell$. If we orient the line ℓ (by placing an arrow on it) we can talk about the left and right half planes for ℓ . Let \mathcal{L} denote the set of *oriented* lines in \mathbb{R}^2 . For an oriented line $\ell \in \mathcal{L}$, let $R(\ell)$ denote the right half plane for ℓ . See Figure 5.11. Observe that if we reverse the orientation on ℓ then the right half plane becomes the left half plane and vice versa.

5.7.1

Exercise

For each of the following sets X , find a subset $\mathcal{L}' \subset \mathcal{L}$ such that $X = \bigcap_{\ell \in \mathcal{L}'} R(\ell)$.

1. The solid unit square $X = \{(x, y) \in \mathbb{R}^2 : (|x| \leq 1) \text{ and } (|y| \leq 1)\}$
2. The disc $X = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 \leq 1\}$.

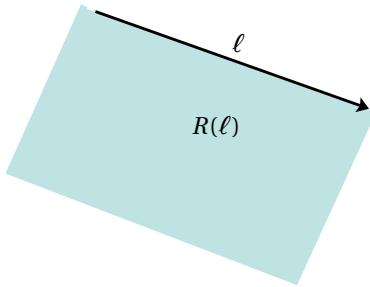


Figure 5.11: An example of an oriented line ℓ and its associated half-plane $R(\ell)$.

Consider the following problem. Let $X = \{(x, y) \in \mathbb{R}^2 : (|x| \geq 1) \text{ or } (|y| \geq 1)\}$. This is the region outside the unit square, as in Figure 5.12. Is there a subset $\mathcal{L}' \subset \mathcal{L}$ such that $X = \bigcap_{\ell \in \mathcal{L}'} R(\ell)$?

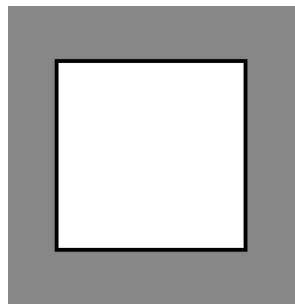


Figure 5.12: The region outside the unit square.

To answer this question, we take a detour.

5.7.2

Definition

For two distinct points $a, b \in \mathbb{R}^2$, let \overline{ab} denote the line segment between them. A subset $H \subset \mathbb{R}^2$ is **convex** if for every two distinct points $a, b \in H$, the line segment $\overline{ab} \subset H$.

Figure 5.13 shows an example of a convex region and a non-convex region. Note also that every half plane is convex. (Can you prove this?)

5.7.3

Theorem ▶ Intersection of convex sets is convex

Suppose that \mathcal{H} is a nonempty set such that each element $H \in \mathcal{H}$ is a convex subset of \mathbb{R}^2 . Then $\bigcap_{H \in \mathcal{H}} H$ is a convex subset of \mathbb{R}^2 .

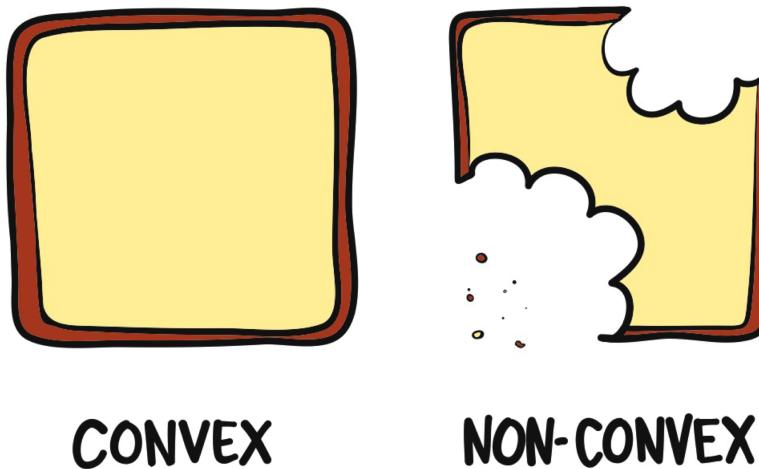


Figure 5.13: The region on the left is convex as any two points in the region are connected by a line segment lying entirely in the region. The region on the right is not convex as there is (at least one) pair of points connected by a line segment not lying entirely in the region.

Here is the beginning of the proof.

Proof. Assume that \mathcal{H} is a set such that each element $H \in \mathcal{H}$ is a convex subset of \mathbb{R}^2 . We will show that $\bigcap_{H \in \mathcal{H}} H$ is a convex subset of \mathbb{R}^2 . By Theorem 5.3.13, $\bigcap_{H \in \mathcal{H}} H \subset \mathbb{R}^2$. We need only show it is convex.

We must show that for every $a, b \in \bigcap_{H \in \mathcal{H}} H$, the line segment $\overline{ab} \subset \bigcap_{H \in \mathcal{H}} H$. Let $a, b \in \bigcap_{H \in \mathcal{H}} H$ be arbitrary.

(Show that \overline{ab} is a subset of $\bigcap_{H \in \mathcal{H}} H$.)

□

5.7.4 Exercise

Explain why if $X \subset \mathbb{R}^2$ is the intersection of some number of half planes, then X is convex. Use this to explain why $X = \{(x, y) \in \mathbb{R}^2 : (|x| \geq 1) \text{ or } (|y| \geq 1)\}$ is not the intersection of half planes of \mathbb{R}^2 .

5.7.5 Exercise

Give an example of two convex sets A and B such that $A \cup B$ is not convex. Thus, the theorem does not hold if we change the intersection to a union.

Finally, we use Theorem 5.7.3 to prove that, given *any* subset $X \subset \mathbb{R}^2$, we can turn X into a natural convex set, called the “convex hull” of X . See Figure 5.14 for an

example.

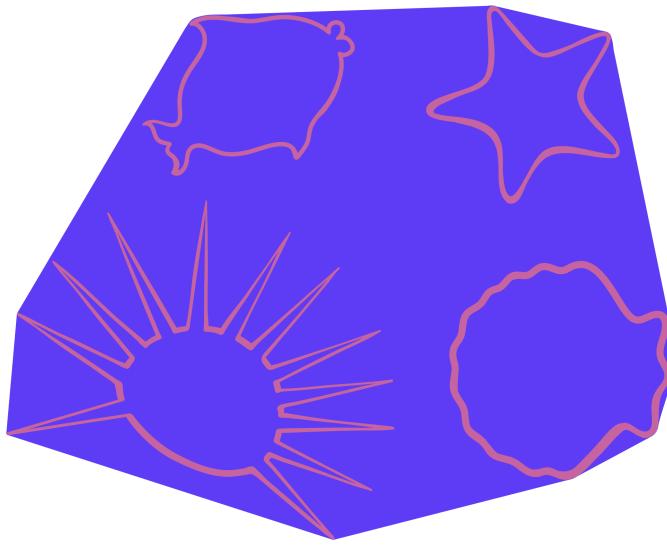


Figure 5.14: The light blue region is the convex hull of the pink regions. Observe that the blue region contains the pink set but that if we make the blue set smaller at all, it either ceases to contain the red/pink set or ceases to be convex.

Without our previous, rather abstract, work it is not obvious that we can do this. Since \mathbb{R}^2 is convex, every subset $X \subset \mathbb{R}^2$ is contained in a convex set, but is there a “smallest” convex set containing X ? If so, this is what we’ll call the “convex hull” of X . The convex hull should have the property that it is convex, but it should also have the property that we can’t take any points away from it to obtain a smaller convex set containing X . We call this set $C(X)$.

Given $X \subset \mathbb{R}^2$, one might attempt to turn X into a convex set by taking the union of X with all line segments in \mathbb{R}^2 having both endpoints in X . This creates a new set X_1 . But for X_1 , we would need to show that all line segments between those line segments lie in this new set. If they don’t we could take the union of X_1 with all line segments having both endpoints in X_1 to get a new set X_2 . If X_2 is not convex, we create an X_3 in a similar way. Are we ever guaranteed to stop? If not, how could we obtain a convex set¹? Theorem 5.7.3 is the needed tool.

5.7.6

Theorem

Suppose that $X \subset \mathbb{R}^2$. Then there exists a convex set $C(X) \subset \mathbb{R}^2$ (called the **convex hull of X**) such that:

- $C(X)$ contains X . That is, $X \subset C(X)$
- $C(X)$ is the smallest convex set containing X . That is, if $X \subset Q \subset \mathbb{R}^2$ and Q is convex, then $C(X) \subset Q$.

¹Actually, you might try taking the union of all those sets! But that is actually more difficult to work with than just applying Theorem 5.7.6.

Groups

In Section 2.1 we were introduced to the notion of a group. Recall that a **group** consists of a set G , an element $\mathbb{1} \in G$, and an operation \circ , such that the following axioms hold:

- (G1) (closure) For every $a \in G$ and $b \in G$ there is some element $c \in G$ such that $c = a \circ b$. Furthermore, this combination is unique. In other words, if $a = a'$ and $b = b'$, then:

$$a \circ b = a' \circ b'.$$

- (G2) (identity) The following hold:

- For every $a \in G$, $a \circ \mathbb{1} = a$.
- For every $a \in G$, $\mathbb{1} \circ a = a$.

- (G3) (inverses) For every $a \in G$ there exists $a^{-1} \in G$ such that the following hold:

- For every $a \in G$, $a \circ a^{-1} = \mathbb{1}$.
- For every $a \in G$, $a^{-1} \circ a = \mathbb{1}$.

- (G4) (associativity) For every $a, b, c \in G$

$$(a \circ b) \circ c = a \circ (b \circ c).$$

If $H \subset G$ is also a group with the same identity $\mathbb{1}$ and operation \circ we say that H is a **subgroup** of G . Initially, we might think that to verify H is a subgroup of G we need to verify that all four axioms hold for H . The next theorem shows that verifying a subset is a subgroup is easier than that. The proof doesn't directly use material from this chapter, but it is a good opportunity to practice using proof structures.

5.7.7

Theorem ▶ Subgroup characterization

Suppose that G is a group with identity $\mathbb{1}$ and operation \circ . Then a non-empty $H \subset G$ is a subgroup of G (with identity $\mathbb{1}$ and operation \circ) if

- For every $a, b \in H$, $a \circ b \in H$,
- For every $a \in H$, $a^{-1} \in H$.

We'll use Theorem 5.7.7, in the proof of the next theorem. It shows that the intersection of subgroups is a subgroup. Informally, we can use Venn diagrams to get a sense for what the theorem is saying, see Figure 5.15.

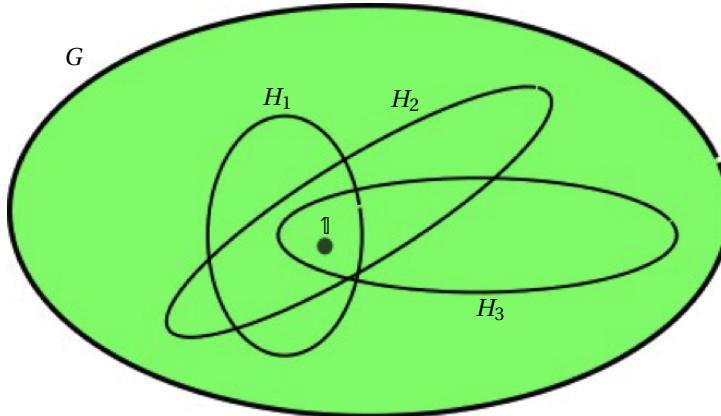


Figure 5.15: The large green ellipse represents a group G . The dot in the center represents the identity element $\mathbb{1}$ and the three smaller ellipses represent three subgroups H_1 , H_2 , and H_3 . Do you see why they must each contain $\mathbb{1}$? Theorem 5.7.8 shows that the intersection $H_1 \cap H_2 \cap H_3$ is also a subgroup of G .

5.7.8

Theorem ▶ Intersection of subgroups is a subgroup

Suppose that G is a group with identity $\mathbb{1}$ and operation \circ . Assume that \mathcal{H} is a non-empty set such that every $H \in \mathcal{H}$ is a subgroup of G . Then

$$\bigcap_{H \in \mathcal{H}} H$$

is a subgroup of G .

Proof. Suppose that G is a group with identity $\mathbb{1}$ and operation \circ . Also assume that \mathcal{H} is non-empty and that every $H \in \mathcal{H}$ is a subgroup of G . In particular, every $H \in \mathcal{H}$ satisfies axioms (G1) - (G4). We will show that

$$\bigcap_{H \in \mathcal{H}} H$$

is a subgroup of G . Observe that by Theorem 5.3.13, the intersection is a subset of G .

In principle, we need to show that $\bigcap_{H \in \mathcal{H}} H$ satisfies axioms (G1) - (G4). However, if we can show that $\bigcap_{H \in \mathcal{H}} H$ is non-empty, then Theorem 5.7.7 implies that we need only show (G1) and (G3).

First we show that $\bigcap_{H \in \mathcal{H}} H$ is non-empty. Since \mathcal{H} is non-empty, there exists $H_0 \in \mathcal{H}$. Since every element of \mathcal{H} is a subgroup of G , every $H \in \mathcal{H}$ satisfies axiom (G2). By Theorem 2.1.8, the identity in each H is equal to $\mathbb{1}$ (the identity in G). Thus, $\mathbb{1} \in H$ for every $H \in \mathcal{H}$. By definition, this implies that $\mathbb{1} \in \bigcap_{H \in \mathcal{H}} H$. Thus, $\bigcap_{H \in \mathcal{H}} H \neq \emptyset$.

Next we show that axiom (G1) holds for $\bigcap_{H \in \mathcal{H}} H$. Let $a, b \in \bigcap_{H \in \mathcal{H}} H$ be arbitrary.

We must show that $a \circ b \in \bigcap_{H \in \mathcal{H}} H$.

⟨ Do it! ⟩

Finally, we show that axiom (G3) holds for $\bigcap_{H \in \mathcal{H}} H$.

⟨ Do it! ⟩

□

Here is an important consequence of Theorem 5.7.8. Notice the similarity to Theorem 5.7.6 which says that every subset of \mathbb{R}^2 is contained in a “smallest” convex set (its convex hull.) Here we show that every subset of a group is contained in a “smallest” subgroup.

5.7.9

Theorem

Let G be a group with identity $\mathbf{1}$ and operation \circ . Suppose that $P \subset G$. Then there exists a subgroup $H(P) \subset G$ such that all of the following hold:

- $P \subset H(P)$
- if $H \subset G$ is any subgroup such that $P \subset H$, then $H(P) \subset H$.

We say that $H(P)$ is the subgroup of G **generated** by P and that $H(P)$ is the “smallest” subgroup of G containing P . The subgroup $H(P)$ may have infinitely many elements, so the term “smallest” only means that $H(P)$ is a subset of every other subgroup containing P .

5.7.10

Example

Let G be the set of all symmetries of \mathbb{R}^2 that preserve distance. For example, every rotation of the plane is an element of G , as is every reflection and translation. G is a group whose operation is function composition. For instance, if we rotate \mathbb{R}^2 by an angle of $\pi/8$ around the origin and then translate every point of \mathbb{R}^2 horizontally by 5 units, we have not changed the distance between any two points of \mathbb{R}^2 since neither the rotation nor the translation changes the distance. Can you give a complete proof that G is a group?

In Example 2.5.6, we considered two symmetries f and g of \mathbb{R} and all possible compositions of f and g and their inverses. The set X of all such symmetries of \mathbb{R}^2 forms a subgroup of G . This is relatively straightforward to prove: we just verify X satisfies axioms (G1) and (G3), but this is essentially the definition of X .

Set $P = \{f, g\}$. We claim that $X = H(P)$. That is, X is the smallest subgroup of G containing both f and g . We'll just sketch the idea behind the argument and omit the details. Since subgroups satisfy (G1) and (G3),

$X \subset H(P)$. Since $P \subset X$ and since $H(P)$ is the smallest subgroup of G containing P , we have $X = H(P)$.

In the previous example, we saw two different descriptions of a certain subgroup of G . The first, X , has a very “hands-on” description: we knew exactly that the elements of X were all compositions of f , g , and their inverses. The second description $H(P)$ is much more abstract, but shows us that X fits into a more general framework. Whatever we prove in the setting of the more general framework will apply to $H(P) = X$ without further additional work. Both descriptions are useful.

Open sets in \mathbb{R}^2

As you know from calculus, intervals play an important role in calculus (as in the definitions of “continuous function” and the statements of the Intermediate Value Theorem, Mean Value Theorem, and Fundamental Theorem of Calculus). The key to extending many of these important tools to other settings is to generalize the notion of open interval. To give us more practice working with sets, we take a brief excursion into topology (the study of continuous functions). We work in \mathbb{R}^2 which is familiar enough to not be scary but flexible enough to capture many of the important concepts. However, much of what we do has analogues for a general metric space. In a topology or real analysis course, these concepts are generalized to many other sets. Our focus is not on motivating the definitions, but on applying abstract definitions and the tools of set theory to prove a few introductory results in topology. Throughout we let d denote the Euclidean metric on \mathbb{R}^2 . That is, if $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$ then

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

In Section 2.6, we proved that d is a metric in the sense of Definition 2.2.1.

5.7.11

Definition

The **open disc** $D_r(a, b) \subset \mathbb{R}^2$ with center (a, b) and radius $r > 0$ is the set

$$D_r(a, b) = \{(x, y) \in \mathbb{R}^2 : d((x, y), (a, b)) < r\}$$

of points (a, b) less than a distance of r from the point (a, b) . A subset $U \subset \mathbb{R}^2$ is **open** if for every $(a, b) \in U$, there exists $r > 0$ such that $D_r(a, b) \subset U$.

One way of thinking about open sets is that their points are stable under small perturbations. That is, a very small change to a point in an open set will still produce a point in the open set. The next exercise shows that the complement of a single point p is always an open set. If you have a point $q \neq p$ and you perturb it a very small amount, then you will still have a point not equal to p . What counts as “very small” depends on the original distance from q to p .

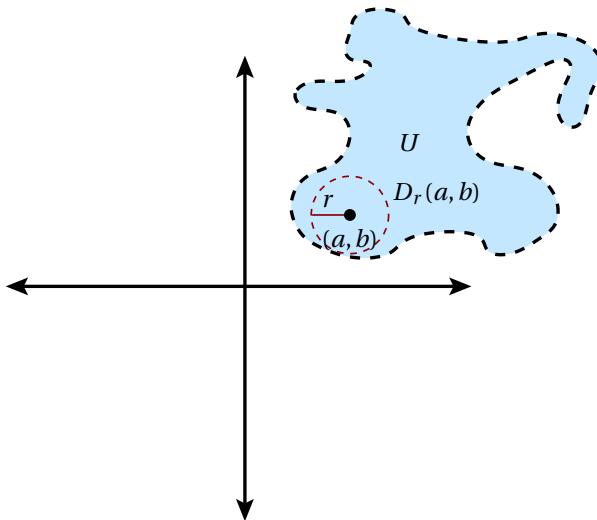


Figure 5.16: An example of an open set U containing the open disc $D_r(a, b)$ of radius r centered at the point (a, b) .

5.7.12 Exercise

Prove that if $p = (x_0, y_0) \in \mathbb{R}^2$, then the set $\mathbb{R}^2 \setminus \{p\}$ is open and the set $\{p\}$ is not open.

5.7.13 Exercise

Let $a, b, c, d \in \mathbb{R}$ with $a < b$ and $c < d$. Prove that the set $U = \{(x, y) \in \mathbb{R}^2 : x \in (a, b) \text{ and } y \in (c, d)\}$ is open.

The next theorem lists four important properties of open sets in \mathbb{R}^2 . These are the properties which, in a point-set topology course, provide the foundation for a very general setting where it makes sense to talk about “continuous function.” We won’t go very far in that direction, though. For us, open sets provide a convenient framework to practice writing proofs involving unions and intersections. In the proof, you will need to use the fact that d satisfies the definition of a metric.

5.7.14 Theorem ▶ Properties of open sets in \mathbb{R}^2

1. \emptyset is an open set.
2. \mathbb{R}^2 is an open set.
3. If \mathcal{U} is a set such that every element $U \in \mathcal{U}$ is an open set in \mathbb{R}^2 , then $\bigcup_{U \in \mathcal{U}} U$ is an open set in \mathbb{R}^2 .
4. If $U, V \subset \mathbb{R}^2$ are open, then $U \cap V$ is open.

In previous sections, we've seen how sometimes we can create the "smallest" sets with certain properties by intersecting all subsets with those properties. We can also, as the next theorem indicates, sometimes create the "largest" sets with certain properties by taking unions.

5.7.15

Theorem ▶ Interiors

Suppose that $V \subset \mathbb{R}^2$. Then there exists an open set $U \subset \mathbb{R}^2$ such that:

- U contains V . That is, $U \subset V$, and
- U is the largest open set contained in V . That is, if $U' \subset V$ and U' is open, then $U' \subset U$.

The set U in Theorem 5.7.15 is called the **interior** of V . Here are two statements regarding interiors for you to prove.

5.7.16

Theorem

1. Let $v \in \mathbb{R}^2$. The interior of the set $\{v\}$ is the empty set.
2. If $V \subset \mathbb{R}^2$ is open, then the interior of V is equal to V .

In \mathbb{R}^2 the open discs play the role of open intervals in \mathbb{R} and the open sets play the role of unions of open intervals in \mathbb{R} . We can also talk about closed sets. Perhaps contrary to what we expect, they are *not* defined by discussing the unions or intersections of closed discs.

5.7.17

Definition

A subset $V \subset \mathbb{R}^2$ is **closed** if its complement V^c is open.

5.7.18

Exercise

Use DeMorgan's Laws to rephrase Theorem 5.7.14 for closed sets, instead of open sets.

The next example is of a closed set of \mathbb{R}^2 which is the famous fractal known as the Sierpinski Carpet. See Figure 5.17. Informally, the Carpet can be defined by subdividing the unit square into 9 smaller squares, removing the middle one from each. Then subdivide each of the remaining 8 squares into 9 smaller squares and remove the middle one from each, etc. If we are always careful to remove open squares, then, at each stage, the complement of the squares we removed is a close set. The intersection of any number of closed sets is closed (Exercise 5.7.18) so the Carpet is a closed set.

Formalizing the definition of the Carpet requires us to work out the endpoints of the vertical and horizontal intervals that are being removed. That makes the definition somewhat technical. There are ways to avoid the technicality at the cost of becoming more abstract, but we won't pursue them here.

5.7.19

Example

Suppose that $n \in \mathbb{N}$. Let $I^n = \{1, 4, 7, 10, \dots, 3^n - 2\}$ be the set of natural numbers between 1 and 3^n that are one more than a multiple of 3. For $k \in I^n$, let $J_k^n = (k/3^n, (k+1)/3^n) \subset \mathbb{R}$. Observe that J_k^n is an interval of length $1/3^n$.

For every $k, \ell \in I^n$, let

$$U_{k,\ell}^n = \{(x, y) \in \mathbb{R}^2 : x \in J_k^n \text{ and } y \in J_\ell^n\}.$$

Notice that $U_{k,\ell}^n$ is an open square with sides of length $1/3^n$.

Let $U = \bigcup_{n \in \mathbb{N}} \bigcup_{k, \ell \in I^n} U_{k,\ell}^n$. Since each $U_{k,\ell}^n$ for all $n \in \mathbb{N}$ and $k, \ell \in I^n$ is an open set, their union U is also open. The complement of U

$$S = \{(x, y) \in \mathbb{R}^2 : (0 \leq x \leq 1) \text{ and } (0 \leq y \leq 1)\}$$

in the solid square is a closed set of \mathbb{R}^2 called the Sierpinski Carpet.

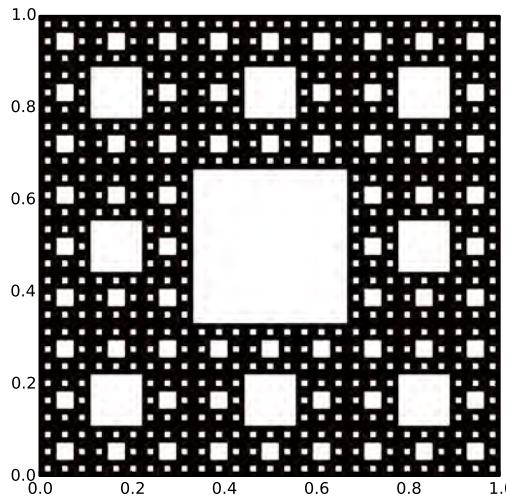


Figure 5.17: The white squares are the sets $U_{k,\ell}^n$ for $n = 1, 2, 3, 4$.

Event Spaces

Probability is the central tool of statistics and data analysis. The basic goal of probability is to begin with a set X (whose elements are called **outcomes**) and to certain subsets $E \subset X$ (called **events**) assign numbers $P(E) \in [0, 1]$, called the **probability of E** . In practice, the outcomes are the results (or potential results) of a random process. For instance, if the random process is “drawing a card from a standard deck of cards,” we can discuss the probability of drawing a 5 of hearts; the probability of drawing a spade, or the probability of drawing a 7 (of any suit).

The events under consideration are then

$$\begin{aligned} E &= \{5\heartsuit\}; \\ E &= \{A\spades, 2\spades, 3\spades, 4\spades, 5\spades, 6\spades, 7\spades, 8\spades, 9\spades, 10\spades, J\spades, Q\spades, K\spades\}; \\ E &= \{7\heartsuit, 7\spades, 7\diamondsuit, 7\clubsuit\} \end{aligned}$$

respectively. It is beneficial to have an abstract definition of probability space and to develop the general theory sufficiently far so as to give a common framework for understanding results concerning probabilities.

5.7.20

Definition ▶ Event Space

Let X be a set. An **event space** on X is a subset $\mathcal{E} \subset \mathcal{P}(X)$ such that the following hold:

- (E1) $\emptyset \in \mathcal{E}$
- (E2) If $A \in \mathcal{E}$ then $A^c \in \mathcal{E}$
- (E3) If $A_i \in \mathcal{E}$ for all $i \in \mathbb{N}$, then $\bigcup_{i \in \mathbb{N}} A_i \in \mathcal{E}$.

Elements of \mathcal{E} are called **events**.

Observe that the elements of an event space¹ are *subsets* of X ! The second condition can be summarized as saying that event spaces are closed under complements and the third condition is summarized by saying that event spaces are closed under countable unions.

5.7.21

Exercise

1. Prove that if X is a set then both $\{\emptyset, X\}$ and $\mathcal{P}(X)$ are event spaces
2. Give examples of 3 event spaces on the set $\{1, 2, 3, 4, 5, 6\}$.

5.7.22

Theorem

Suppose that \mathcal{E} is an event space on X . Prove the following:

1. If $E_i \in \mathcal{E}$ for all $i \in \mathbb{N}$, then $\bigcap_{i \in \mathbb{N}} E_i \in \mathcal{E}$.
2. If E_1 and E_2 are events, then $E_1 \cup E_2$ is an event.

Proof. Assume that \mathcal{E} is an event space on X .

Proof of 1. Assume that $E_i \in \mathcal{E}$ for every $i \in \mathbb{N}$.

(Prove that $\bigcap_{i \in \mathbb{N}} E_i \in \mathcal{E}$. Perhaps DeMorgan's Laws will be helpful!)

Proof of 2. Assume that $E_1, E_2 \in \mathcal{E}$. For $i \in \mathbb{N}$ with $i \geq 3$, let $E_i = \emptyset$. By the

¹The traditional name for an “event space” is the awful term **σ -algebra**.

definition of an “event space”, $\emptyset \in \mathcal{E}$. Notice

$$\bigcup_{i \in \mathbb{N}} E_i = E_1 \cup E_2.$$

By part 1, we have $\bigcup_{i \in \mathbb{N}} E_i$ is an event. Thus, $E_1 \cup E_2$ is an event. \square

The next theorem is the analogue for event spaces of Theorems 5.7.3 and 5.7.8 for convex sets and subgroups, respectively. This result (and proof) can be mind-blowing because the elements of \mathbb{E} are sets, each an event space (not event!). The elements of each of those event spaces are events and events are subsets of X . Rephrasing this, we see that if E is an event, then $E \subset X$. That is $E \in \mathcal{P}(X)$. Every element of an event space \mathcal{E} is an event, so $\mathcal{E} \subset \mathcal{P}(X)$. That is, $\mathcal{E} \in \mathcal{P}(\mathcal{P}(X))$. Finally, if every element of \mathbb{E} is an event space, then $\mathbb{E} \subset \mathcal{P}(\mathcal{P}(X))$. That is, $\mathbb{E} \in \mathcal{P}(\mathcal{P}(\mathcal{P}(X)))$. This is one of the few results I know where triple power sets show up naturally. The amazing thing is that if we let the definitions guide us, we don’t need to think at all about all these power sets. Give it a shot!

5.7.23

Theorem ▶ Intersections of Event Spaces

Let X be a set. Then the following hold:

1. If \mathbb{E} is a non-empty set such that each element $\mathcal{E} \in \mathbb{E}$ is an event space on X , then $\bigcap_{\mathcal{E} \in \mathbb{E}} \mathcal{E}$ is an event space on X .
2. If $\mathcal{U} \subset \mathcal{P}(X)$ then there exists an event space \mathcal{E} on X such that $\mathcal{U} \subset \mathcal{E}$ and if \mathcal{E}' is any event space on X with $\mathcal{U} \subset \mathcal{E}'$, then $\mathcal{E} \subset \mathcal{E}'$.

One particularly common construction occurs when $X \subset \mathbb{R}$. Let \mathcal{U} be the set whose elements are all of the form $U \cap X$ where U is an open interval in \mathbb{R} . The elements of \mathcal{U} are called the **basic open sets** in X . The previous theorem guarantees that there is an event space \mathcal{E} which such that each basic open set in X is an event and so that \mathcal{E} is as small as possible. In other words, if \mathcal{E}' is another event space on X such that each basic open set in X is an event, then $\mathcal{E} \subset \mathcal{E}'$. The event space \mathcal{E} is called the **Borel event space** on X . In a later chapter we will consider ways of assigning probabilities to events.

5.8 Application: Configuration Spaces

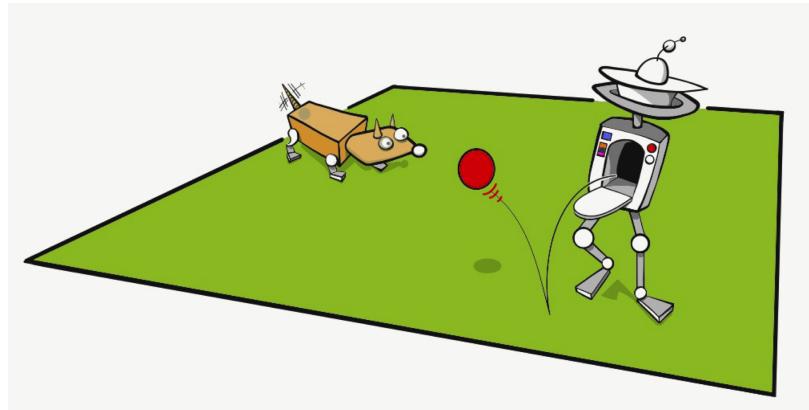
“Perhaps the most fundamental question one can ask about a robot is, where is it? The answer is given by the robot’s *configuration*: a specification of the position of all points of the robot.”

– Kevin M. Lynch and Frank C. Park, *Modern Robotics* [87]

Davros: “Now where are my Daleks?”

– “Destiny of the Daleks,” *Dr Who* (1979)

Suppose that we have two robots MARVIN and K9 moving around on the floor of a large room. If we place a 2-dimensional coordinate system on the floor, MARVIN’s location (at a given point in time) can be given as a point $(x_1, y_1) \in \mathbb{R}^2$. Likewise, K9’s location can be given as a point $(x_2, y_2) \in \mathbb{R}^2$. Since MARVIN and K9 are never in the same location at the same time, $(x_1, y_1) \neq (x_2, y_2)$. We can package all this information together to model the location of the two robots at a particular point in time as a point $r \in (\mathbb{R}^2 \times \mathbb{R}^2) \setminus \Delta$ where $\Delta = \{(a, b) \in \mathbb{R}^2 \times \mathbb{R}^2 : a = b\}$. The set $\mathcal{C}^2(\mathbb{R}^2) = (\mathbb{R}^2 \times \mathbb{R}^2) \setminus \Delta$ is an example of a configuration space.



5.8.1

Definition ▶ Configuration Space

Let X be a set. The **diagonal** of the set $X \times X$ is $\Delta = \{(a, b) \in X \times X : a = b\}$. The **configuration space** of 2 labelled points in X is the set $\mathcal{C}^2(X) = (X \times X) \setminus \Delta$.

5.8.2

Exercise

Generalize the definition of configuration space to the situation when there are more than two labelled points.

In Section 7.9 we will see how to define a configuration space for unlabelled points. Configuration spaces play an important role in robotics, mechanics, and in several other scientific areas.

5.8.3

Exercise

Let $I \subset \mathbb{R}$ be the interval $[0, 1]$. Draw a picture of $\mathcal{C}^2(I)$.

5.8.4

Exercise

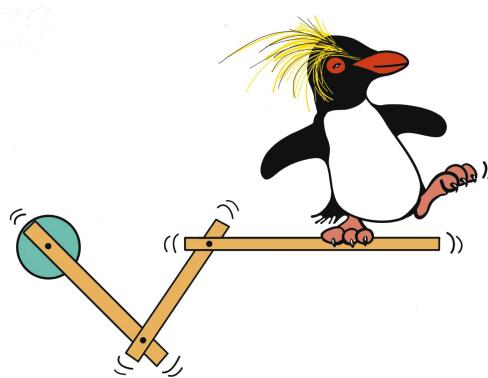
One issue with using $\mathcal{C}^2(\mathbb{R}^2)$ as a model for the position of two robots on a plane is that it allows the robots to get arbitrarily close to each other. To see this, consider points $p_1, p_2 \in \mathbb{R}^2$ with $p_1 = (x_1, y_1)$ and $p_2 = (x_2, y_2)$. The **distance** from p_1 to p_2 is the number

$$d(p_1, p_2) = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}.$$

Observe that (p_1, p_2) is a single point in the configuration space $\mathcal{C}(\mathbb{R}^2)$.

1. Find a point in $\mathcal{C}^2(\mathbb{R}^2)$ which corresponds to the two robots being within a distance .001 of each other.
2. How can the definition of $\mathcal{C}^2(\mathbb{R}^2)$ be adjusted so that a point of the new configuration space corresponds to positions for the two robots in \mathbb{R}^2 which are at least .001 from each other?

Considering our two robots MARVIN and K9 again and recalling that a single point of $\mathcal{C}^2(\mathbb{R}^2)$ corresponds to a position of *both* robots in \mathbb{R}^2 , we might like a way to measure the distance in $\mathcal{C}^2(\mathbb{R}^2)$. If $d_{\mathcal{C}}$ is the notation for whatever metric we decide to use, for points $P, Q \in \mathcal{C}^2(\mathbb{R}^2)$, then $d_{\mathcal{C}}(P, Q)$ will be a measurement of how close the position P of both robots is to the position Q of both robots. If as the robots move from P to Q , we observe that $d_{\mathcal{C}}(P, Q)$ is small, then neither robot has moved very far from its starting point. On the other hand, if $d_{\mathcal{C}}(P, Q)$ is large than at least one of the robots has moved far from its starting point.



Another type of configuration space arises when we consider linkages. One type of linkage arises when we have a device made of three arms hinged together. Suppose the first arm A is 2 feet long, the second B is 1 foot long and the third C is 1/2 foot long. One end of A is fastened to a wall in such a way that it can rotate 2π radians around the point where it is fastened. The other end of A is fastened

to one end of B in such a way that, no matter how A is positioned, the arm B can rotate 2π radians around the point where it is fastened to A . The other end of B is similarly fastened to one end of C so that no matter how A and B are positioned, the arm C can rotate 2π radians around the point where it is fastened to B . How can we describe all possible positions of the linkage? Since the positions of any two of the arms don't affect the ability of the third arm to rotate, each position of the linkage can be described by three angles: θ_A , θ_B , and θ_C , each between 0 and 2π . The angle θ_A tells us how much we've rotated around the point where arm A is attached to the wall. The angle θ_B tells us how much we've rotated arm B around the point where arms A and B are attached. Finally, θ_C tells us how much we've rotated arm C around the point where B and C are attached. Each position of the linkage is then given by an ordered triple: $(\theta_A, \theta_B, \theta_C)$. Since an angle of 0 radians is the same as an angle of 2π radians, each of θ_A , θ_B , and θ_C actually be thought of as points in S^1 . Thus, positions of the linkage correspond to points of $S^1 \times S^1 \times S^1$, the configuration space of the linkage.

5.8.5

Exercise

Suppose that a certain lighting board for theatrical use contains 4 sliders, each of which can move continuously from a position labelled 0 to a position labelled 11. The board also has 3 dials, each of which can be rotated a full 2π radians. Express a configuration space for the lighting board as a Cartesian product.

5.9 Application: The geometric structure of data

“When I began learning about machine learning and data mining, I found that the intuition I had formed while studying geometry was extremely valuable in understanding the basic concepts and algorithms. But in many of the resources I’ve seen, this relatively simple geometry is hidden behind enough equations and algorithms to intimidate all but the most technically inclined readers.”

— Jesse Johnson, *The Shape of Data* [77]

An image on the computer screen can be thought of as an array of pixels with n rows and m columns. If the image is gray-scale, each pixel can be assigned a number $t \in [0, 1]$ corresponding to how gray it is: a value of 0 denotes that it is black, a value of 1 means that it is white, a value in $(0, 1)$ indicates some shade of grey. If we number the pixels $1, 2, \dots, nm$ we can record the image as a point

$$(t_1, t_2, \dots, t_{nm}) \in \mathbb{R}^{nm}$$

For example, the original copy of the photo on the left in Figure 5.18 being 225 pixels wide by 248 pixels represents a single point in \mathbb{R}^{55800} . The original copy of the photo on the right is 173×122 pixels and so represents a single point in \mathbb{R}^{21106} .



Figure 5.18: Two typical black and white photos of delightfully atypical children.

If we consider all the black and white images that are n pixels wide by m pixels tall, produced by some person (perhaps a contributor to Flickr), we have a set of points (called the **data set**) in \mathbb{R}^{nm} . Typically the number $nm \in \mathbb{N}$ is very large and so, if there are also a lot of images, it may be difficult to find patterns in the data set. Similarly, whenever we collect a large number of measurements for a large number of objects in any situation we end up with a large number of points in \mathbb{R}^k for some large k and finding patterns is difficult.

It turns out that we can think of the data set (in our example, the set of images) as a geometric object and then use methods from geometry, topology, probability, and statistics to analyze it. This is an enormous task and is the subject of much active research. In this section we restrict ourselves to describing one method of approaching the problem.

Henceforth, suppose that $k \in \mathbb{N}$ and that $D \subset \mathbb{R}^k$ (the data set) is a finite set of points. For each $r > 0$, we will construct an object (called a simplicial complex) which is a generalization of a graph and which tells us something about how the data points sit in relation to each other. Simplicial complexes, like graphs, are highly structured, easy to store in a computer, and are much easier to study than the original data set.

5.9.1

Definition ▶ Simplicial Complex

A **simplicial complex** (or multi-graph) is a finite set K such that each element of K is a finite set, and for all $A \in K$, $\mathcal{P}(A) \subset K$.

5.9.2

Example

Let a, b, c, d, e , and f be distinct. Define K to be the set whose elements are the following sets:

$$\begin{aligned} &\emptyset, \{a\}, \{b\}, \{c\}, \{d\}, \{e\}, \{f\}, \\ &\{a, b\}, \{b, c\}, \{c, d\}, \{a, c\}, \{a, d\}, \{c, e\}, \{e, f\}, \{e, g\}, \{g, f\}, \{e, f\}, \\ &\{a, b, c\}, \{a, b, d\}, \{b, c, d\}, \{a, c, d\}, \{e, f, g\}, \\ &\{a, b, c, d\}. \end{aligned}$$

We claim that K is a simplicial complex. Checking this is straightforward, but exceedingly tedious, so we just give an idea of how to do it.

5.9.2

Consider the element $\{e, f, g\} \in K$. For K to be a simplicial complex, we must have $\mathcal{P}(\{e, f, g\}) \subset K$. The power set of $\{e, f, g\}$ is the set whose elements are:

$$\begin{aligned} &\emptyset, \\ &\{e\}, \{f\}, \{g\}, \\ &\{e, f\}, \{e, g\}, \{f, g\} \\ &\{e, f, g\}. \end{aligned}$$

We can then check that each element of $\mathcal{P}(\{e, f, g\})$ is also an element of K , so $\mathcal{P}(\{e, f, g\}) \subset K$. Similarly, we can check that the power sets of $\{a, b, c, d\}$ and $\{c, e\}$ are both subsets of K . All other sets in K are subsets of $\{e, f, g\}$, $\{a, b, c, d\}$, and $\{c, e\}$. This implies their power sets are also subsets of K . Thus, K is a simplicial complex.

There is a connection between graphs and simplicial complexes which will help us better visualize simplicial complexes. A graph G consists of a set $V(G)$ of vertices as well as a set $E(G)$ of edges. If G has no loops and if there is at most one edge between any two vertices, then we can identify an edge e with the set $\{v, w\}$ where v and w are the endpoints of e . Notice that the set $K = \{\{v, w\}, \{v\}, \{w\}, \emptyset\}$ consisting of the edge, its endpoints¹, and the empty set satisfy the definition of a simplicial complex. Thus, if we want to draw a picture of K , we can just draw an edge and label its endpoints v and w . More generally, given the graph G , we can let the elements of K be the empty set, the edges $e \in E(G)$, and also all sets of the form $\{v\}$ where $v \in V(G)$. It is easily verified that K satisfies the definition of simplicial complex. We can draw G if we want to visualize G .

Now consider an arbitrary simplicial complex K . For each set $A \in K$ such that A has a unique element v , we draw a dot and label it with v . For each set B such that B has precisely two elements v and w (so that $B = \{v, w\}$ and $v \neq w$) we draw an edge joining the vertex labelled v to the vertex labelled w . But, what about elements in K having more than two elements?

If a, b, c are all distinct and $\{a, b, c\} \in K$, then by the definition of K , the sets $\{a, b\}$, $\{a, c\}$, $\{b, c\}$, as well as $\{a\}$, $\{b\}$, and $\{c\}$ are all elements of K . In our picture, therefore, we have a triangle with edges $\{a, b\}$, $\{b, c\}$, and $\{a, c\}$ and corners $\{a\}$, $\{b\}$, $\{c\}$. To visualize the set $\{a, b, c\}$, we simply shade in the triangle to make it solid. Similarly, if there is a set of the form $\{a, b, c, d\}$ with a, b, c, d all distinct, then we can shade in a tetrahedron. Sets with more than 4 elements correspond to higher-dimensional versions of triangles and tetrahedra. Figure 5.19 shows a picture of the simplicial complex from Example 5.9.2.

Given a data set $D \subset \mathbb{R}^k$ and a real number $r > 0$, for each $a \in D$, let $B_r(a) = \{x \in \mathbb{R}^k : d(a, x) < r\}$ be the open ball of radius r centered at a . (Here d is the standard Euclidean metric on \mathbb{R}^k .)

¹rather the sets whose only elements are the endpoints

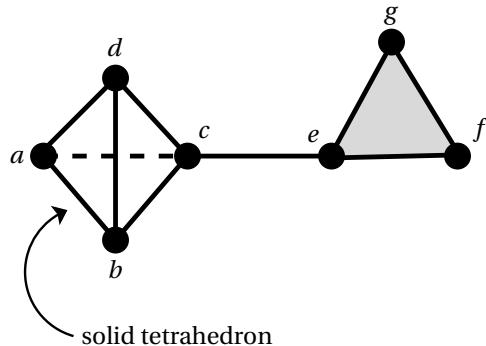


Figure 5.19: The simplicial complex whose elements are $\{a, b, c, d\}$, $\{c, e\}$, and $\{e, f, g\}$ and all subsets of those sets.

5.9.3

Definition ▶ Čech Complex

The **Čech¹ complex** of $D \subset \mathbb{R}^k$ and $r > 0$ is

$$K(D, r) = \left\{ \sigma \subset D : \bigcap_{x \in \sigma} B_r(x) \neq \emptyset \right\}$$

Figure 5.20 shows an example of how to construct the Čech complex.

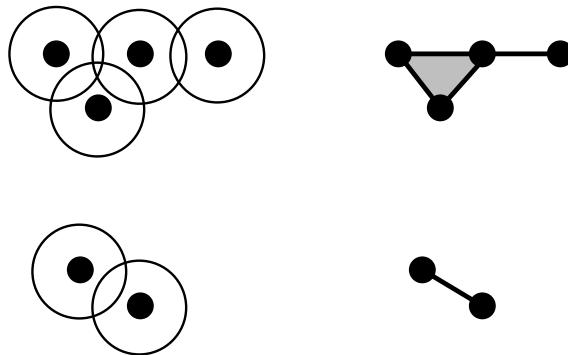


Figure 5.20: On the left are 6 data points D , each surrounded by a circle of radius r . On the right is the associated Čech complex $K(D, r)$.

5.9.4

Exercise

Prove that $K(D, r)$ is a simplicial complex and that if $0 < r_1 < r_2$ then $K(D, r_1) \subset K(D, r_2)$.

The way that the complexes $K(D, r)$ are used to study D is roughly speaking as follows. For a particular value of r , there are algorithms that can compute the number of connected components (i.e. the number of pieces) of $K(D, r)$ as well as the number of “holes” in $K(D, r)$ of each dimension. For example, a hollow triangle is a simplicial complex with a “1-dimensional hole” and a hollow octahedron is a simplicial complex with no 1-dimensional holes but with

¹pronounced “check”

a “2-dimensional hole”. (The area of mathematics that gives a precise definition of “hole” is called homology theory; it is a branch of topology and algebra.) Thus, for each r , and for each dimension $p \in \mathbb{R}$, we have a number $n_p(r)$ which is the number of “ p -dimensional holes” in $K(D, r)$. To study D , we let r vary in the interval $(0, \infty)$. Since D is finite, for very large r , $K(D, r)$ is the set \emptyset . If $r < \min\{d(x, y) : x, y \in D, x \neq y\}$, then the balls $B(x, r)$ for $x \in D$ are all disjoint and so $K(D, r)$ is a set whose elements are precisely \emptyset and all sets of the form $\{x\}$ for $x \in D$. So, speaking informally, as r increases from 0 to some very large number, $K(D, r)$ goes from being an isolated set of points to being a single entity. What happens in between is what tells us something about our data. For example, if r has to be very large before $n_0(r)$ (the number of “pieces” of $K(D, r)$) is smaller than the number of elements of D , then the points in the data set are very spread out. Similarly, if there is a relative long interval (a, b) such that for all $r \in (a, b)$, $n_1(r)$ is large then the data set D is weblik, as it has lots of “1-dimensional holes”. The relatively new mathematical subject which studies how to extract useful information about the data from the Čech (and related) complexes is called “persistent homology”. See [25] for more detail on how persistent homology has proved to be useful in recent years.

5.10 Additional Problems

“Nothing is more comfortable than not having to think.”

– Simone Weil¹, *On the Abolition of All Political Parties* [133]

1. Let $S = \{(x, y) \in \mathbb{R}^2 : (x - 1)^2 + (y + 2)^2 = 1\}$. Let $S' = \{(x, y) \in \mathbb{R}^2 : y = (x - 1)^2 - 1\}$. Show that there is a unique element of $S \cap S'$.
2. Prove (using a proof by contradiction and some algebra) that the curves in \mathbb{R}^2 defined by the equations

$$\begin{aligned} x^2 + 3xy + y^2 &= 1, \text{ and} \\ y &= -2x \end{aligned}$$

do not intersect.

3. Let

$$\mathcal{A} = \left\{ \{1, 2, 3, 4\}, \{2, 3, 5\}, \{2, 9, 17\} \right\}$$

(a) List the elements of $\bigcup_{A \in \mathcal{A}} A$.

(b) List the elements of $\bigcap_{A \in \mathcal{A}} A$.

4. For each $r \in \mathbb{R}$, let L_r be the line in \mathbb{R}^2 that passes through the origin and has slope r . Give a complete description of the sets

$$\bigcup_{r \in \mathbb{R}} L_r \text{ and } \bigcap_{r \in \mathbb{R}} L_r.$$

¹Simone Weil (1909-1943) was a philosopher and Christian mystic. Her brother was the prominent mathematician André Weil

5. Give an example of a set \mathcal{A} all of whose elements are subsets of \mathbb{N} such that all of the following hold:

- (a) There are infinitely many sets in \mathcal{A}
- (b) $\bigcup_{A \in \mathcal{A}} A$ is the set of even natural numbers.
- (c) $\bigcap_{A \in \mathcal{A}} A$ is the set of natural numbers divisible by 4.

6. Let X be a set. An **EQREL** set for X is a subset $E \subset X \times X$ such that the following hold:

- (ER1) For every $x \in X$, $(x, x) \in E$.
- (ER2) If $(x, y) \in E$ then $(y, x) \in E$.
- (ER3) If $(x, y) \in E$ and $(y, z) \in E$, then $(x, z) \in E$.

Assume E_λ is an EQREL set for X for every $\lambda \in \Lambda$ (where Λ is some nonempty index set). Prove that $\bigcap_{\lambda \in \Lambda} E_\lambda$ is also an EQREL set for X .

7. Let X be a set. A **topology** on X is a set $\mathcal{T} \subset \mathcal{P}(X)$ (i.e. a set whose elements are subsets of X) such that axioms (T1), (T2), and (T3) below hold. For convenience, we refer to the elements of \mathcal{T} as **open** sets, although it might be better to refer to them as *orange* sets, so we don't confuse matters with our previous discussion of open subsets of \mathbb{R}^2 .

- (T1) $\emptyset \in \mathcal{T}$ and $X \in \mathcal{T}$ (i.e. the empty set and the entire set are open)
- (T2) If $U_\lambda \in \mathcal{T}$ for every $\lambda \in \Lambda$ (where Λ is some index set) then $\bigcup_{\lambda \in \Lambda} U_\lambda \in \mathcal{T}$.
(i.e. the union of open sets is open.)
- (T3) If $U \in \mathcal{T}$ and $V \in \mathcal{T}$, then $U \cap V \in \mathcal{T}$. (i.e. the intersection of two open sets is open.)

Prove that if \mathbb{T} is a non-empty set such that every element $\mathcal{T} \in \mathbb{T}$ is a topology on X , then so is $\bigcap_{\mathcal{T} \in \mathbb{T}} \mathcal{T}$.

8. Let $X_0 = [0, 1] \subset \mathbb{R}$. Let $X_1 = X_0 \setminus (1/3, 2/3)$. Let $X_2 = X_1 \setminus ((1/9, 2/9) \cup (7/9, 8/9))$. Keep going in this manner, removing the middle third of each closed interval. Figure 5.21 shows X_0 through X_4 . More precisely, assuming we have defined X_i so that

$$X_i = \left[0, \frac{1}{3^i}\right] \cup \left[\frac{2}{3^i}, \frac{3}{3^i}\right] \cup \cdots \cup \left[\frac{3^i - 1}{3^i}, 1\right]$$

Let X_{i+1} be the relative complement in X_i of the open intervals

$$\left(\frac{1}{3^{i+1}}, \frac{2}{3^{i+1}}\right) \cup \left(\frac{3}{3^{i+1}}, \frac{4}{3^{i+1}}\right) \cup \cdots \cup \left(\frac{3^{i+1}-2}{3^{i+1}}, \frac{3^{i+1}-1}{3^{i+1}}\right).$$

- (a) Use the properties of unions and relative complements to express the sets X_i and X_{i+1} in more concise form.

- (b) The intersection $\bigcap_{n \in \mathbb{N}} X_n$ is called the **Cantor set**. Prove it is non-empty.

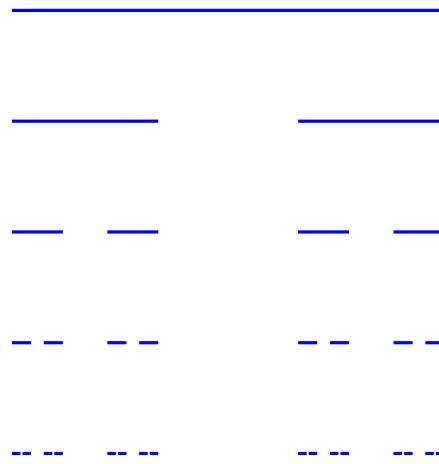


Figure 5.21: Stages 0 through 4 of the construction of the Cantor set. The $i + 1$ st stage is created by removing the middle third from each interval in the i th stage.

6 | Set Theory Axiomatics

Key Concepts

- Understand how the ZFC axioms correspond to the operations on sets in Chapter 5.
- Be able to construct a natural number system using only the ZFC axioms.
- Be able to construct a Cartesian product using only the ZFC axioms.

"I must be very careful here. I am at a dangerous point and am likely to fall into the trap of meddling with the mathematicians."

- Ludwig Wittgenstein² [135]

The previous chapter has given us a host of operations on sets: finding subsets using predicates, taking the intersection of sets, taking the union of sets, finding a power set, and so forth. But we saw in Section 3.7 how the naive definition of a set as a collection of elements gives rise to serious logical issues (even ignoring the fact that we haven't given a definition of "collection"!). For although the object $\{A : A \text{ is a set}\}$ looks like a set because it is dressed in curly braces, it cannot be a set without creating a logical contradiction. What to do?

We need a better definition of a set; hopefully one which avoids creating logical contradictions. Before we do that, we briefly remark on the sociology of set theory.

Ferreirós [47, p. 465] summarizes the important role that set theory has played in the development of mathematics as a discipline:

²Wittgenstein (1889-1951) was an important 20th century philosopher whose work focussed on the nature of language.

“Set theory has served a unique role by systematizing the whole of modern mathematics. In so doing, it has absorbed and represented, more clearly than any other discipline, the peculiar trend of thought that was involved in mathematics’ shift from natural science to autonomous discipline. One of its intriguing features is that, at some point, the belief became deeply established that mathematical knowledge can be reconstructed as being totally independent from features of the physical world.”

Given the ubiquity of sets in modern mathematics, it is easy to forget that even into the 20th century, not all mathematicians (even prominent ones) felt that set theory was a natural basis for mathematics. A former president of the American Mathematical Society, Robert Bryant, reflects on what it is like to read the work of Élie Cartan, one of the leading mathematicians of the late 19th and early 20th centuries,

“What is very different [compared to the work of modern geometers] about Cartan’s work is that it is written in a style of mathematics uninfluenced by set theory. ... He seemed to think of objects as being ‘subject to’ rules rather than being ‘defined by’ them. Instead of saying ‘Consider a map’ or ‘Consider a domain,’ he would say ‘Consider a point depending on some parameters.’ He almost never defined anything as a set, including domains and ranges for functions! ... When we read Cartan, we are looking back into a time before set theory took over and getting a glimpse of how nineteenth-century mathematicians thought.” [76]

Perhaps more telling is that the now ubiquitous notation¹ for functions $f: X \rightarrow Y$ between sets X and Y did not become prevalent until the algebraic topology became an integral part of mathematics post-1940 (see [1, 88]).

Historically, the most important axiomatization of set theory was created by Ernst Zermelo (1871 - 1953) and was further developed by Abraham Fraenkel (1891 - 1965) and Thoralf Skolem (1887-1963). The resulting axiomatic theory is known as Zermelo-Fraenkel set theory and the list of axioms are referred to as ZFC (with the “C” standing for “Choice”). The quest for a time then became showing that:

1. All (or most) of mathematics is a consequence of ZFC.
2. ZFC is complete (meaning that it is possible to prove every true statement using ZFC).
3. ZFC is consistent (meaning that it is impossible to prove both a statement and its negation using ZFC).

The first objective has more-or-less been accomplished and ZFC is the standard set of axioms for most of modern mathematics. Regarding the second and third

¹which we’ll introduce in Chapter 8

goals, in 1931, Kurt Gödel proved his “incompleteness theorems.” The first incompleteness theorem shows that it is impossible to prove that ZFC is complete and the second of which shows that it is impossible to show that ZFC is consistent. Moreover, the same would be true if ZFC is replaced with any system of axioms strong enough to enable elementary arithmetic.

Apart from the issues of consistency and completeness, whose resolution becomes a philosophical rather than a mathematical task, the ZFC axioms have another drawback – some of them are highly non-intuitive and do not correspond to how most mathematicians actually *do* mathematics. There is, however, another way to arrive at the same theory. In the 1960s, F.W. Lawvere developed another set of axioms which also produce set theory of Chapter 5. These axioms are known as the “Elementary Theory of the Category of Sets” (ETCS). See Leinster’s treatment [85] for a brief summary or the book [84] for a complete exposition. Unfortunately, to begin with ETCS and prove elementary results concerning subsets is a rather convoluted process, so we do not follow that approach. What ETCS does do, however, is remind us that just as Peano’s axioms are all that are needed to produce sets functionally equivalent to \mathbb{N} , so the properties of sets are more important than their exact definition. If a logical contradiction were found within ZFC, most mathematicians would not abandon mathematics – they would seek to understand where the contradiction occurs and then adjust the axioms to try to wall off the contradiction from the parts of mathematics most widely used.

Since both the ZFC axioms and the ETCS axioms can be difficult for the beginning student to digest, we present an incomplete list of the ZFC axioms and, even for those, give somewhat incomplete statements. The goal here is to state the essential properties from which almost all of mathematics can be developed and to give some sense for how this is done. We adapt our list from [38, Section II.5] and [39]. The history of the role of logic in mathematics and the development of modern conceptions of proof is extremely interesting, but beyond the scope of this text. The reader is encouraged to consult [31, 46, 47, 55].

6.1 The ZFC axioms

“I went still further, arguing that if we fail to admit the existence of something which has nothing prior to it, it is impossible for us to accept the fact that there exists anything at all. For if we consider in our mind that one thing comes from another thing, we have to predicate the same thing of the second as of the first and say that it could only have come into being from a third thing; the same predicate again must be made of the third thing, namely that it could only have come into being from a fourth thing, and so *ad infinitum*. Since, however, an infinite series cannot be completed, it follows that we are not in existence. But, behold, we are in existence, and unless the things which preceded us were finite (in number), they could not have been completed so as to reach us.”

– Saadia¹ [111]

Since we cannot give a precise definition of every term we use, we will have to have a list of undefined terms and a list of axioms specifying how those terms are to relate to each other. As we have seen, set theory is concerned with elements, sets, what it means for an element to be an element of a particular set and what it means for two elements to be equal or two sets to be equal. Typically, we can make matters simpler by only considering sets, so that the elements of every set are also sets. This has the advantage of streamlining the theory, but has the disadvantage of divorcing our intuition for what sets are from their axiomatization.

6.1.1

Definition ► Undefined terms for ZFC

- The symbol $=$ (pronounced “equals”)
- The symbol \in (pronounced “is an element of”)
- The word “set”.

We also write $x \notin X$ to mean “ x is not an element of X .” If X and Y are sets, then $X \subset Y$ means that for every element $x \in X$, we also have $x \in Y$.

Perhaps it is disturbing that the word “set” is one of our undefined terms, but the meaning of the word “set” will be determined by its usage. Indeed, the very point of the axioms we are about to encounter is that it is the axioms and how they relate to each other which determine what a set is. Thinking of a set as a “collection” is then an act of mathematical modeling. If we want to apply set theory to the physical world, we must make additional assumptions about how the physical world relates to the mathematical world.

Our first axiom fixes the relationship of the symbol “ $=$ ” to the symbol “ \in ”. Recall

¹Sadia ben Joseph (882 - 942) is considered the father of medieval Jewish philosophy. This quotation is part of a longer argument concerning the creation of the world by God from nothing. For us, it is an example of the reluctance of thinkers in the Greek tradition to philosophically accept the existence of an actual infinity, rather than just potential infinity.

that the symbol “ \subset ” was already defined in terms of the symbol “ \in ”.

6.1.2 Axiom of Extensionality

Sets A and B are equal (and we write $A = B$) if and only if $A \subset B$ and $B \subset A$.

Solely on the basis of this first axiom, we can prove our first theorem (silly though it is!)

6.1.3 Theorem

If X is a set, then $X = X$.

Proof. It is obviously true that $x \in X$ if and only if $x \in X$. Thus, $X \subset X$ and $X \in X$, by the definition of \subset . By the definition of equals, $X = X$. \square

Although the first axiom concerned sets, it doesn’t guarantee that there are any sets. If our theory is going to be nontrivial, there had better be a set! Our second axiom says that we assume this to be the case.

6.1.4 Axiom of Existence

There exists a set.

Observe that this axiom doesn’t tell us anything at all about the set that we are assuming to exist. In order to get anything useful, we need to be able to use predicates to create subsets of this (or any other) set.

6.1.5 Axiom of Subset Selection

Let X be a set and let $P(a)$ be a predicate in one free variable. Then there is a set

$$Y = \{a \in X : P(a)\}$$

An immediate consequence of the first two axioms is the existence of the empty set. Often the next theorem is used as an axiom instead of the Axiom of Existence.

6.1.6 Theorem ▶ Existence of \emptyset

There exists a set \emptyset such that \emptyset has no elements.

Proof. Let X be a set. Such an X exists by the Axiom of Existence. Consider the predicate

$$P(a) : "a \neq a".$$

Define $\emptyset = \{x \in X : P(x)\}$. Since every element of X is a set and by Theorem 6.1.3, every set is equal to itself, there does not exist any element $x \in X$ such that $x \neq x$. Thus, \emptyset has no elements. \square

The proof of Theorem 6.1.6 created \emptyset as a subset of some arbitrary set X . If we had chosen a different initial set X , would we have created a different empty set? Prove the next theorem using the Axiom of Extensionality and some statements which are vacuously true.

6.1.7

Theorem

There exists a unique set having the property that it has no elements.

We can also use the Axiom of Subset Selection to show that we can create a set by taking intersections.

6.1.8

Theorem ▶ Intersections

Suppose that \mathcal{H} is a nonempty set. Then there exists a unique set, denoted $\bigcap_{H \in \mathcal{H}} H$ such that $x \in \bigcap_{H \in \mathcal{H}} H$ if and only if $x \in H$ for every $H \in \mathcal{H}$.

Proof. Let $P(a)$ be the predicate: “For every $H \in \mathcal{H}$, $a \in H$ ”. By hypothesis, there exists $H_0 \in \mathcal{H}$. By the Axiom of Subset Selection

$$\bigcap_{H \in \mathcal{H}} H = \{x \in H_0 : P(x)\}$$

is a set. If $x \in H$ for every $H \in \mathcal{H}$, then certainly $x \in H_0$ and $P(x)$ is true. Likewise, if $x \in H_0$ and $P(x)$ is true, then $x \in H$ for every $H \in \mathcal{H}$. Thus, $\bigcap_{H \in \mathcal{H}} H$ is the set we are looking for. Any other set Z with the property that $x \in Z$ if and only if $x \in H$, for every $H \in \mathcal{H}$ must be equal to $\bigcap_{H \in \mathcal{H}} H$ by the Axiom of Extensionality. \square

We certainly need to know that there are nonempty sets. The Power Set Axiom is one way of creating nonempty sets.

6.1.9

Axiom of Power Sets

If X is a set, then there exists a set $\mathcal{P}(X)$ (the **power set of X**) such that $A \in \mathcal{P}(X)$ if and only if $A \subset X$.

The proof of the next theorem uses the Axiom of Power Sets in conjunction with the Axiom of Subset Selection.

6.1.10

Theorem

Suppose that X is a set. Then $\{X\}$ is a set.

In particular, we have our first nonempty set, namely $\{\emptyset\}$!

6.1.11

Axiom of Unions

Suppose that \mathcal{H} is a set. Then there exists a set $\bigcup_{H \in \mathcal{H}} H$ such that $x \in \bigcup_{H \in \mathcal{H}} H$ if and only if there exists $H \in \mathcal{H}$ such that $x \in H$.

The Axiom of Extensionality guarantees that the set $\bigcup_{H \in \mathcal{H}} H$ from the Axiom of Unions will be the unique set X such that $x \in X$ if and only if there exists $H \in \mathcal{H}$ such that $x \in H$.

Notice that the Axiom of Union says that we can only take the union of a collection of sets to obtain a set if that collection is itself a set. In the previous chap-

ter, however, we often wrote things like $\bigcup_{\lambda \in \Lambda} A_\lambda$. When we did this we always assumed that Λ was a set, but we never made any assumption about the collection $\{A_\lambda : \lambda \in \Lambda\}$. For $\bigcup_{\lambda \in \Lambda} A_\lambda$ to be guaranteed to be a set, we do need $\{A_\lambda : \lambda \in \Lambda\}$ to be a set as well. The next axiom guarantees that if we have a set (such as Λ) and a way of matching each element of Λ to a set A_λ , then $\{A_\lambda : \lambda \in \Lambda\}$ will also be a set. The statement of the axiom uses predicates to make precise what we mean by “matching.”

6.1.12

Axiom of Replacement

Suppose that $P(a, b)$ is a predicate in two free variables and that Λ is a set. Suppose that for each $\lambda \in \Lambda$, there is a unique set A_λ , such that $P(\lambda, A_\lambda)$ is true. Then $\{A_\lambda : \lambda \in \Lambda\}$ is a set.

The Axiom of Replacement can be rather difficult to appreciate. Here are two examples to show how it can be used in conjunction with the other axioms to guarantee the existence of certain kinds of sets.

6.1.13

Theorem ▶ Pairing Theorem

Suppose that X and Y are sets. Then $\{X, Y\}$ is a set.

Proof. Recall that $\{\emptyset\}$ is a set. By the Axiom of Power Sets, $\Lambda = \{\emptyset, \{\emptyset\}\}$ is a set. Let $P(a, b)$ be the predicate:

$$(a = \emptyset \text{ and } b = X) \text{ or } (a = \{\emptyset\} \text{ and } b = Y).$$

Notice that for each $\lambda \in \Lambda$ there is a unique set A_λ such that $P(\lambda, A_\lambda)$ is true. That is, if $\lambda = \emptyset$ then X is the unique set such that $P(\lambda, X)$ is true and if $\lambda = \{\emptyset\}$, then Y is the unique set such that $P(\lambda, Y)$ is true. Thus, by the Axiom of Replacement, $\{X, Y\}$ is a set. \square

Use the Axiom of Union and the Axiom of Extensionality to explain why the next corollary is true.

6.1.14

Corollary

Suppose that X and Y are sets. Then there is a unique set, denoted $X \cup Y$, such that $z \in X \cup Y$ if and only if $z \in X$ or $z \in Y$.

The next Corollary lets us begin the process of creating a set that can function as the set of natural numbers.

6.1.15

Corollary

If X is a set, then $X \cup \{X\}$ is also a set.

For a set X , we call the set $S(X) = X \cup \{X\}$ the **successor** of X .

6.1.16 Example

Corollary 6.1.15 implies that the following are all sets:

- $S(\emptyset) = \{\emptyset\}$
- $S(S(\emptyset)) = \{\emptyset, S(\emptyset)\}$
- $S(S(S(\emptyset))) = \{\emptyset, S(\emptyset), S(S(\emptyset))\}.$
- etc.

As in our discussion of natural number systems (Definition 2.4.2), we can now set about basing arithmetic on Set Theory as follows:

6.1.17 Definition ▶ Individual Natural Numbers

Make the following definitions:

- Define $\mathbf{0} = \emptyset$.
- Define $\mathbf{1} = S(\mathbf{0})$.
- Define $\mathbf{2} = S(\mathbf{1})$.
- Define $\mathbf{3} = S(\mathbf{2})$.
- etc.

6.1.18 Exercise ▶ (A chance to ponder)

In our development of set theory so far, we have defined the numbers **2** and **3** (for example) to be sets. In fact, $\mathbf{2} \subset \mathbf{3}$. How do you feel about this? Should numbers be sets? If not, what are they? What's a more basic concept: number or set?

Although we could continue on to define whatever natural number we wish, we do not yet have a set of natural numbers. The Axiom of Infinity will be crucial in creating such a set.

6.1.19 Axiom of Infinity

There exists a set N with the following properties:

- $\mathbf{0} \in N$. (That is, $\emptyset \in N$.)
- For every $A \in N$, $S(A) \in N$.

Observe that the statement of the second property relies on our assumption that elements of a set are themselves sets. (Otherwise, $S(A)$ may not always be de-

fined.) We would like for the set N given by the Axiom of Infinity to satisfy the Peano Axioms. That is, we would like it to satisfy the definition of “Natural Number System” (Definition 2.4.2). As stated, however, it may not. Section 6.3 shows how to create a natural number system from the Axiom of Infinity.

There are two final axioms of set theory which we should mention. Both are rather technical. The first is intended to help make set theory match with our intuition of sets as collections. It will rule out the possibility that a set can be an element of itself. The second is most useful when we phrase it in terms of functions and so we will defer discussion of it until later.

6.1.20 **Axiom of Foundation**

For every nonempty set X , there exists $A \in X$ such that $A \cap X = \emptyset$.

6.1.21 **Theorem ▶ Sets are not elements of themselves**

For every set W , $W \notin W$.

Remember, however, that for every set X , X is a *subset* of itself!

Proof. We prove this by contradiction. Assume that W is a set such that $W \in W$. By Theorem 6.1.10, $X = \{W\}$ is set. Since $W \in W$ and $W \in X$, we have $W \cap X \neq \emptyset$.

Now since $W \in X$, X is nonempty. By the Axiom of Foundation, there exists $A \in X$ such that $A \cap X = \emptyset$. Since W is the unique element of X , $A = W$. Thus, $W \cap X = \emptyset$, contradicting our earlier statement. Thus, no set can be an element of itself. \square

To prove the following theorem, apply the Axiom of Foundation to the set $\{X, Y\}$. In terms of our intuition, this says that there are not two boxes X and Y such that X is an item in Y and Y is an item in X .

6.1.22 **Theorem**

There do not exist sets X and Y such that $X \in Y$ and $Y \in X$.

Here is a new proof of the theorem we call Russell’s Paradox (Theorem 3.7.1). Its proof relies on the Axiom of Foundation.



6.1.23

Theorem ▶ Russell's Paradox Revisited

There does not exist a set U such that $A \in U$ if and only if A is a set.

Proof. If there were a set U such that $A \in U$ if and only if A is a set, then $U \in U$. This contradicts Theorem 6.1.21. Thus, there is no such set U . \square

In our previous proof of Russell's Paradox, we considered a set R such that $A \in R$ if and only if $A \notin A$. We have established, using the Axiom of Foundation, that $A \notin A$ for every set A . Thus, the set R cannot exist, either.

Finally, we present the Axiom of Choice. Figure 6.1 shows how it works. The axiom simply says we can pick one element out of each set from a collection of sets and that these elements together form a set.

6.1.24

Axiom of Choice (AC)

Suppose that \mathcal{H} is a nonempty set such that $\emptyset \notin \mathcal{H}$. Then for each $U \in \mathcal{H}$, there exists $a_U \in U$ such that $A = \{a_U : U \in \mathcal{H}\}$ is a set.

As stated, AC should seem plausible, and we may wonder why it is even needed. So what's the problem? The problem is when we said "choose". Since we had no way of doing that with a predicate, without AC, there is no guarantee that we can collect all of the a_U together into a set (which we wanted to call A). The point of the Axiom of Choice is that we choose to believe this is a valid thing to do. It does, however have some surprising consequences. See, for example, [129]. The axiom is now widely accepted by mathematicians and plays an important

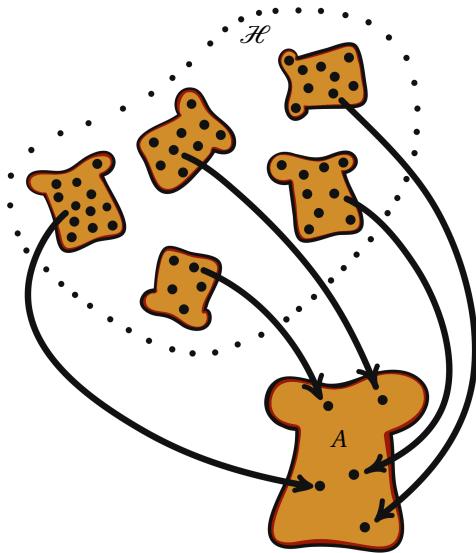


Figure 6.1: An depiction of how the Axiom of Choice works. For each set that is an element of the set \mathcal{H} , we choose an element and put all those elements into a new set, called A . The Axiom of Choice guarantees that there is a way of making the selection of elements so that A is a set.

role in the elementary theory of the category of sets (ETCS). However, those with a computational bent still object to it since the axiom does not specify *how* to choose the elements from each of the sets.

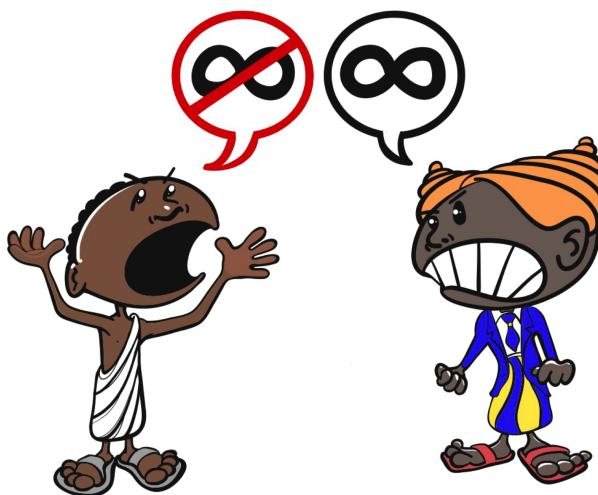
6.1.25 Example

Let $A = \{1, 2, 3\}$ and $B = \{6, 7, 8\}$. Since $\mathcal{H} = \{A, B\}$ is a set, the Axiom of Choice says that we can create a set by choosing one item from each of A and B . So, for instance, the Axiom of Choice might tell us that $\{1, 6\}$ is a set. Alternatively, it might tell us that $\{2, 8\}$ is a set. There are other ways of deducing that $\{1, 6\}$ and $\{2, 8\}$ are sets, however. The true impact of the Axiom of Choice is for infinite collections of sets.

6.2 The controversies

“And this leads to that famous threefold division of intellectual study. One part constitutes the knowledge of the universe, the understanding of nature. The second consists of distinguishing between the things we ought to aim at and the things we ought to avoid – in other words, this is the art of the good life. The third subdivision comprises the assessment of logical consequences and incompatibilities, which is the basic requirement for accurate discussion and analysis.”

– Cicero¹ [28]



Over the years, many of the ZFC axioms have proved to be controversial. The ancient Greeks, for example, would have been very unhappy with the Axiom of Infinity as it postulates the existence of an “actual infinity” rather than just a “potential infinity.” The existence of the set \mathbb{N} allows us think of all the natural numbers as existing as a complete unit. While the Greeks would have agreed that there is always a “next number”, they would not have agreed that we can conceive of all the numbers simultaneously. The Axiom of Infinity continues to be denied by certain mathematicians known as “finitists.” Most modern mathematicians, however, accept it without difficulty. The Axiom of Choice was also controversial as it led to a number of counter-intuitive results. At the present, however, most mathematicians have made their peace with the Axiom of Choice and feel free to use it when it suits them. Currently, the Axiom of Power Sets is the most controversial (see the discussion at [2].) As we will see in Chapter 10, the Axiom of Power Sets implies the existence of very, very large sets. These sets are essentially never used in mainstream mathematics and so the power set axiom seems to create far more mathematics than is actually useful. Again, however,

¹Marcus Tullius Cicero (106-43 BC) was a Roman orator. In this quote, he is articulating the Stoic division of philosophy into physics, ethics, and dialectic.

most mathematicians are happy to use the power set axiom in the limited contexts in which they need it. If a logical contradiction were discovered in the ZFC axioms, however, we would all have to rethink it!

6.3 The existence of a natural number system

“Every conclusion presumes premisses. These premisses are either self-evident and need no demonstration, or can be established only if based on other propositions; and, as we cannot go back in this way to infinity, every deductive science and geometry in particular, must rest upon a certain number of indemonstrable axioms.”

- Henri Poincaré¹, *Science and Hypothesis* [101]

As an application of the ZFC axioms, we will show that the Axiom of Infinity gives rise to a set satisfying the Peano Axioms (Section 2.4). We begin by showing that the set given to us by the Axiom of Infinity satisfies the first two Peano Axioms.

6.3.1

Theorem

Suppose that N is a set such that $\emptyset = \mathbf{0} \in N$ and for every $A \in N$, the set $S(A) = A \cup \{A\} \in N$. Then Axioms (P1) and (P2) hold for $(N, \mathbf{0}, S)$. That is,

- (P1) There does not exist $n \in N$ such that $S(n) = \mathbf{0}$.
- (P2) For every $n, m \in N$, if $S(n) = S(m)$ then $n = m$.

Proof. Consider $n \in N$. By definition $S(n) = n \cup \{n\}$, so $n \in S(n)$. In particular, $S(n) \neq \emptyset$ for every $n \in N$. Thus, for all $n \in N$, $S(n) \neq \mathbf{0}$. Hence, (P1) holds.

We prove (P2) by contradiction. Suppose that there exist $n, m \in N$ such that $n \neq m$ but $S(n) = S(m)$. Since $n \in S(n)$ we have $n \in S(m)$ by the Axiom of Extensionality. By definition of $S(m)$, we have $n \in m \cup \{m\}$. By definition of union, $n \in m$ or $n \in \{m\}$. But if $n \in \{m\}$, then $n = m$ since m is the unique element of $\{m\}$. Thus, $n \in m$. A similar argument shows that $m \in n$. But n and m are sets, so we contradict Theorem 6.1.22. Thus, (P2) holds. \square

It may not be the case, however, that N satisfies (P3). It may be too big! Consider the following example.

6.3.2

Example

Suppose that we already know all about the rational numbers and elementary arithmetic. Consider the following set:

$$N = \left\{ 0, 1, 2, 3, 4, 5, \dots, \frac{1}{2}, \frac{3}{2}, \frac{5}{2}, \frac{7}{2}, \frac{9}{2}, \dots \right\}$$

For $n \in N$, let $S(n) = n + 1$. Notice that $0 \in N$ and that for every $n \in N$,

¹Poincaré (1854–1912) was one of the world’s most influential mathematicians. He made numerous outstanding contributions to many areas of both pure and applied mathematics.

6.3.2

$S(n) \in N$. Thus, $(N, 0, S)$ satisfies Axioms (P1) and (P2).

Now let $A = \{0, 1, 2, 3, 4, \dots\}$. Observe that $(A, 0, S)$ also satisfies Axioms (P1) and (P2). Axiom (P3) would insist that $A = N$. But $A \neq N$, since $3/2 \in N$ and $3/2 \notin A$. Thus, if the Axiom of Infinity handed us this set N , we would not (yet) have a natural number system.

As the previous example indicates, the key to creating a natural number system will be to construct a set satisfying axioms (P1) and (P2) which is “as small as possible.” That is, we will want a subset $\mathbf{N} \subset N$ such that \mathbf{N} satisfies (P1) and (P2) and if $Z \subset N$ is any other subset containing $\mathbf{0}$ and the successors of all its elements, then $\mathbf{N} \subset Z$. We have seen several constructions of this sort in Section 5.7.

6.3.3

Theorem

Let N be a set such that $\emptyset = \mathbf{0} \in N$ and for all $A \in N$, $A \cup \{A\} = S(A) \in N$. Then, there is a subset $\mathbf{N}^* \subset N$, such that $\mathbf{0} \in \mathbf{N}^*$ and $(\mathbf{N}^*, \mathbf{0}, S)$ is a natural number system.

Proof. We are given a set N such that $\mathbf{0} \in N$ and for all $A \in N$, the set $S(A) \in N$. Let $\mathbf{S} \subset \mathcal{P}(N)$ be the set of all subsets Z of N such that $\mathbf{0} \in Z$, and for all $A \in Z$, $S(A) \in Z$. The set \mathbf{S} is the set of all possible candidates for natural number systems.

(Use Axioms of Set Theory to explain why \mathbf{S} is a set.).

By assumption, $N \in \mathbf{S}$ so \mathbf{S} is nonempty. By Theorem 6.3.1 (applied to Z in place of N), every $Z \in \mathbf{S}$ satisfies (P1) and (P2). Define

$$\mathbf{N}^* = \bigcap_{Z \in \mathbf{S}} Z.$$

Recall from Theorem 6.1.8 that \mathbf{N}^* is a set.

(Show that $\mathbf{N}^ \in \mathbf{S}$.)*

Thus, by our previous remarks \mathbf{N}^* satisfies (P1) and (P2).

(Show that for every $Z \in \mathbf{S}$, we have $\mathbf{N}^ \subset Z$).*

Therefore, \mathbf{N}^* is the smallest subset of N containing $\mathbf{0}$ and the successors of all its elements. It remains to show that \mathbf{N}^* satisfies (P3).

Suppose that $A \subset \mathbf{N}^*$ has the following properties:

- $\mathbf{0} \in A$
- If $n \in A$, then $S(n) \in A$.

By assumption, $A \in \mathbf{S}$. By our previous remarks, $\mathbf{N}^* \subset A$. Since we assumed $A \subset \mathbf{N}^*$, we have (by the Axiom of Extensionality) $A = \mathbf{N}^*$. Hence, \mathbf{N}^* satisfies (P3).

Since (P1), (P2), and (P3) hold, $(\mathbf{N}^*, \mathbf{0}, S)$ is a natural number system. \square

Back in Section 2.4, we explained how the existence of a natural number system is enough to develop the basic arithmetic of natural numbers.

6.4 The existence of the Cartesian product

“Get to know other worlds, if only for comparison.”

– Wislawa Szymborska¹, *We’re Extremely Fortunate* [121]

In Definition 5.6.1 it is assumed that $X \times Y$ is a set, however nothing we have said so far indicates that there is such a set. Under the ETCS axiomatization of set theory, this is taken as an axiom. However, under ZFC, we can prove that, given sets X and Y , there is a set with the right kind of properties to be considered the Cartesian product $X \times Y$ of X and Y . That is, the Cartesian product exists² as a set. Here we briefly sketch how to do this. This idea is due to Kuratowski.

6.4.1

Theorem

Suppose that X and Y are sets. Then for each $x \in X$ and $y \in Y$, there is a set (x, y) with the property that $(a, b) = (x, y)$ if and only if $a = x$ and $b = y$. Furthermore, $\{(x, y) : x \in X, y \in Y\}$ is a set.

Proof. We have already seen (Theorem 6.1.13) that $\{X, Y\}$ is a set. The Axiom of Union guarantees that $X \cup Y$ is a set. The Power Set Axiom guarantees that $\mathcal{P}(X \cup Y)$ is a set and that for a given $x \in X$ and $y \in Y$, $\{x\}$ and $\{x, y\}$ are sets. The Axiom of Subset Selection guarantees that

$$(x, y) = \{z \in \mathcal{P}(X \cup Y) : z = \{x\} \text{ or } z = \{x, y\}\}$$

is a set for each $x \in X$ and $y \in Y$. That is, $(x, y) = \{\{x\}, \{x, y\}\}$ is a set.

We claim that if $(x, y) = (a, b)$, then $x = a$ and $y = b$. Suppose that $(x, y) = (a, b)$. Then, by definition, $\{\{x\}, \{x, y\}\} = \{\{a\}, \{a, b\}\}$. By the Axiom of Extensionality, either $x = a$ and $\{x, y\} = \{a, b\}$ or $\{x\} = \{a, b\}$ and $\{x, y\} = \{a\}$. Suppose, first, that the former happens. Then $x = a$ and so $\{x, y\} = \{a, y\} = \{a, b\}$ which implies (by the Axiom of Extensionality) that $y = b$. On the other hand, if the latter occurs, then $x, y \in \{a\}$ which implies that $x = a = y$. Also, $a, b \in \{x\}$ and so $a = b = x$. Consequently, $x = a$ and $y = b$, as desired.

We now wish to show that $X \times Y$ is a set. Observe that for each $x \in X$ and $y \in Y$, $(x, y) \in \mathcal{P}(X \cup Y)$. Thus, by the Axiom of Subset Selection

$$X \times Y = \{z \in \mathcal{P}(X \cup Y) : \exists x \in X, y \in Y \text{ s.t. } z = (x, y)\}$$

is a set. \square

¹Wislawa Szymborska (1923 - 2012) won the Nobel Prize for Literature in 1996.

²I think, therefore I’m a set?

6.5 Functions, Formally

“We must be still and still moving
 Into another intensity”
 – T.S. Eliot¹, *Four Quartets* [42]

In Section 5.6, we alluded to the connection between Cartesian Products and functions. Although we do not thoroughly explore functions until Chapter 8, we can briefly describe how the ZFC axioms, which are just about sets, also let us work with functions. Here is an abbreviated definition of function.

Informally, we define

6.5.1

Definition ► Informal Definition of Function

Let X and Y be sets. A relationship f between a set X to a set Y is a **function** $f: X \rightarrow Y$ if the following conditions hold:

- (The domain condition) For each $x \in X$, there exists a $y \in Y$ such that $y = f(x)$.
- (The well-defined condition) If $a, b \in X$ and $a = b$, then $f(a) = f(b)$.

The philosophy undergirding ZFC is that *every* mathematical object should be able to be modelled by a set. The remainder of this section shows how to do this for functions. Under the ETCS axiom system, however, the notion of “function” is taken as an undefined term and the foundational axioms of the theory guarantee that these sets exist. So this section is not intended to help us understand *what* functions are, but rather to help us understand how they relate to commonly accepted foundations of mathematics.

6.5.2

Definition ► Formal Definition of Function

Let X and Y be sets. A subset $f \subset X \times Y$ is a **function** from X to Y if the following condition holds:

- (The domain condition) For each $x \in X$, there exists a $y \in Y$ such that $(x, y) \in f$.
- (The well-defined condition) If $(a, y_1) \in f$ and $(b, y_2) \in f$ have the property that $a = b$, then $y_1 = y_2$.

If $f \subset X \times Y$ is a function from X to Y we write $f: X \rightarrow Y$. If $(x, y) \in f$, then we write $y = f(x)$.

¹Thomas Stearns Eliot (1888-1965) won the 1948 Nobel Prize in Literature.

6.5.3

Exercise

Suppose that $f: X \rightarrow Y$ and $g: X \rightarrow Y$ are two functions (according to the set theoretic definition above). Prove that they are equal if and only if for every $x \in X$, we have $f(x) = g(x)$. Remember to prove that this will mean that you need to show $f \subset g$ and $g \subset f$.

The formal definition makes it clear that the domain condition is about existence and the well-defined condition is about uniqueness. Notice also that our formal definition means that a function is *by definition* equal to its graph (which was defined in Section 5.6). The formal definition of a function is unfortunately counter-intuitive since we rarely think of a function as being a set. We more often think of it as being a process or algorithm for converting elements of X into elements of Y . So our formal definition converts the movement that we associate with functions into the staticity that we associate with sets. Additionally, from a modern perspective we often consider function-like objects (called **morphisms**) between objects that are not sets and so the desire that a function be a set is not as strong. Nevertheless, viewing functions as sets does have the major advantage that we can discuss sets of functions. Prove the next theorem using the results of this section.

6.5.4

Theorem

Suppose that X and Y are sets. Then

$$\{f : f: X \rightarrow Y \text{ is a function}\}$$

is a set.

Finally, we give an application of the formal definition of a function to the creation of Cartesian Products. Recall that an ordered pair (x, y) was defined to be the set $\{\{x\}, \{x, y\}\}$ and that $X \times Y$ was the set of all ordered pairs (x, y) with $x \in X$ and $y \in Y$. We could have defined Cartesian products of more than two sets in a similar way, but the definitions get overwhelmingly complicated. We can use functions to make life easier. For instance, for sets X , Y , and Z we can define an ordered triple (x, y, z) to be a function $f: \{1, 2, 3\} \rightarrow X \cup Y \cup Z$ such that $f(1) = x \in X$, $f(2) = y \in Y$, and $f(3) = z \in Z$. Observe that if f and g are two such ordered triples, then $f = g$ if and only if $f(1) = g(1)$, $f(2) = g(2)$, and $f(3) = g(3)$. That is, if $(x, y, z) = f$ and $(x', y', z') = g$, then by the definition of function equality, $(x, y, z) = (x', y', z')$ if and only if

$$\begin{aligned} x &= f(1) = g(1) = x', \\ y &= f(2) = g(2) = y', \text{ and} \\ z &= f(3) = g(3) = z' \end{aligned}$$

Inspired by this, we could define an ordered n -tuple (x_1, x_2, \dots, x_n) for x_i an element of a set X_i to be a function $f: \{1, \dots, n\} \rightarrow X_1 \cup \dots \cup X_n$ such that $f(i) = x_i \in X_i$ for each $i \in \{1, \dots, n\}$. More generally still, if X_λ is a set for each λ in some

index set Λ , we can define the Cartesian product

$$\prod_{\lambda \in \Lambda} X_\lambda = \{f: \Lambda \rightarrow \bigcup_{\lambda \in \Lambda} X_\lambda\}.$$

This gives us a way of discussing “infinite ordered pairs” and “infinite Cartesian products” while being sure that we are still in the realms of set theory. (The capital pi for “product” is standard usage, but a large \times can also be used.)

6.5.5

Exercise

Let $Y = \{1, 2, 3\}$ and $X = \mathbb{R}$. For each $y \in Y$, let $X_y = X$ and for each $x \in X$, let $Y_x = Y$. Explain the difference between $\prod_{y \in Y} X_y$ and $\prod_{x \in X} Y_x$. Can you sketch a picture of each?

7 | Equivalence Relations

Key Terms

- relation
- reflexive relation
- symmetric relation
- transitive relation
- equivalence relation
- equivalence class
- quotient set

“... gracious as a newly laid table where related objects might gather ...”

– Barbara Guest, *Words* [58]

So far in this text, we've carefully considered what it means for two sets to be equal. We have a very precise definition: two sets are equal if and only if they have the same elements. But there are many places where the correct notion of “equals” is less evident.

7.0.1 Example

Is $0 = 2\pi$? When we consider 0 and 2π as numbers, the answer is clearly: “No!” After all, $2\pi \approx 6.28 > 0$. On the other hand, when we consider them as angles measured in radians, the answer is a definite: “Yes!” How can it be that sometimes 0 does equal 2π and sometimes it does not?

7.0.2

Example

Is $\frac{1}{3} = \frac{5}{15}$? The answer from elementary school is a clear: “Yes!” because $15 = 3 \cdot 5$ (cross-multiplying). However, if two things are actually equal, shouldn’t they have exactly the same properties? And yet, we say that $\frac{1}{3}$ has the property that it is in lowest terms, while $\frac{5}{15}$ does not. How can two things that are equal have different properties?

In this chapter we take up the question of what it means for two objects to be “the same” and how “sameness” depends on the context in which we are working. We then use our answer to the question to create an immense variety of new mathematics.

We begin with the more mundane, but still useful, discussion of how we might organize elements of a set. We will discuss a certain type of organizational scheme, called a “partition” and then relate partitions to the question of what it means for two objects to be equivalent.

7.1 Partitions

“It is the wittiest partition that ever I heard discourse, my lord.”

- William Shakespeare, *A Midsummer Night's Dream* V.1

Consider how a residential college might assign its college students to dorm rooms. Each student is assigned to some room (assuming no one lives off-campus), each room (ideally) has at least one occupant, and no student is assigned to more than one room. On some dean’s computer is a spreadsheet with a list of student names organized by room assignment. This list is a partition of the students into dorm rooms. More formally:

7.1.1

Definition ▶ Partition

Let X be a set. A set $P \subset \mathcal{P}(X)$ is a **partition** of X if the following hold:

1. (Nonempty) $\emptyset \notin P$.
2. (Covering) $X = \bigcup_{A \in P} A$
3. (Pairwise disjoint) If $A, B \in P$ then either $A = B$ or $A \cap B = \emptyset$.

An element $A \in P$ is called a **room**. If x is an element of a room A , then we say x **inhabits**¹ A .

Connecting the definition to our dorm-room analogy, the set X is the set of students at the college; the set P corresponds to the set of room assignments; the nonempty condition guarantees each dorm room has an inhabitant; the covering condition guarantees every student is an inhabitant of some room; and the

¹The terminology of “room” and “inhabits” is nonstandard.

pairwise disjoint condition guarantees that no student is an inhabitant of more than one room. It is best to think about each element of the partition as a subset of the student body, rather than (say) the dorm room itself as a physical space.

As another imperfect analogy, we might think of a partition as being the floor plan of a house. The house is divided into rooms and the partition is the list of rooms (in no particular order). The nonempty criterion ensures that a room occupies some amount of space in the house. The pairwise disjoint property says that no two rooms overlap and the covering property says that every point in the house lies in some room (Figure 7.1).

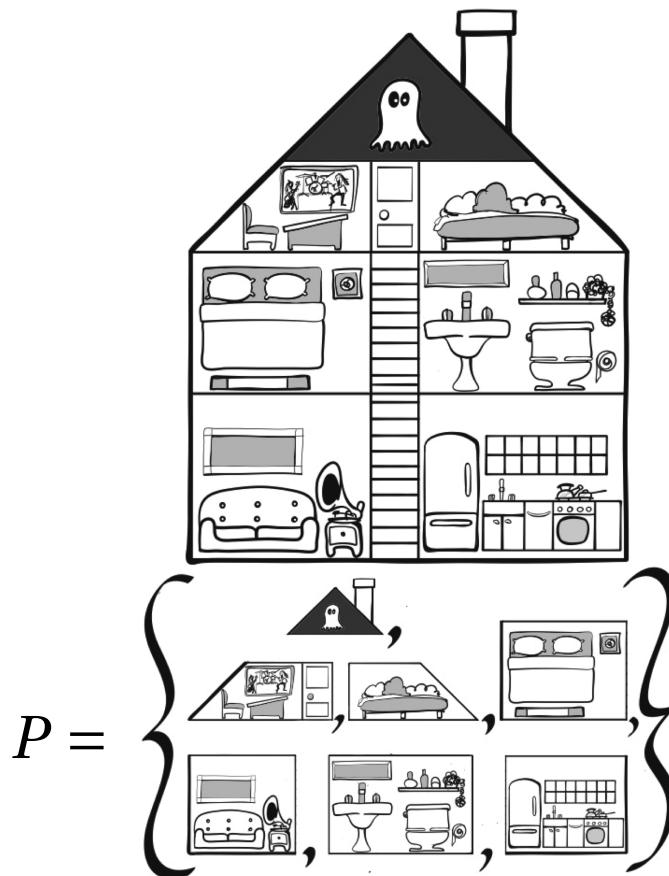


Figure 7.1: The house has been partitioned into rooms. The partition is the set of rooms. Their union is the house, no room is empty, and they are pairwise disjoint. Apparently, the stairway is not part of the house. Perhaps the ghost owns it by an exception in deed.

Observe that a partition is a set whose elements are sets. For some reason, many of us have a difficult time coming to grips with such sets¹. The following examples and exercises are intended to help you overcome any discomfort.

¹for more on this see [20]

7.1.2

Example

Consider the set $X = \mathbb{R}^2$. Let

$$A = \{(x, y) \in \mathbb{R}^2 : (y < x) \text{ or } (x = y \text{ and } 0 < x)\};$$

let $B = \{(x, y) \in \mathbb{R}^2 : |x| < y\}$; and let $C = \{(x, y) \in \mathbb{R}^2 : x \leq y \leq -x\}$. Then the set $P = \{A, B, C\}$ is a partition of X . We depict it in Figure 7.2 by assigning colors to points in \mathbb{R}^2 based on which set in the partition they belong to. More generally, any way of coloring points in \mathbb{R}^2 corresponds to a partition of \mathbb{R}^2 by considering each subset of points with the same color to be one room of the partition. Any particular room need not be connected - it could just be a collection of disconnected points.



Figure 7.2: We indicate the partition $\{A, B, C\}$ of \mathbb{R}^2 by coloring the points in A orange, the points in B red, and the points in C black.

7.1.3

Example

Here are some partitions of the real numbers:

1. $P_1 = \{\mathbb{R}\}$
2. $P_2 = \{\{x\} : x \in \mathbb{R}\}$
3. $P_3 = \{(-\infty, 0], (0, \infty)\}$
4. $P_4 = \{(-\infty, 0) \cup (5, 7) \cup (8, \infty), [0, 5] \cup [7, 8]\}$
5. $P_5 = \{(n, n+1] : n \in \mathbb{Z}\}.$

The set P_1 is a partition of \mathbb{R} with a single room and every real number is an inhabitant of this room. The set P_2 is a partition of \mathbb{R} with infinitely many rooms, one for each real number. Each real number x is the sole inhabitant of the room $\{x\}$ containing it. The set P_3 is a partition of \mathbb{R} with two rooms. The positive real numbers inhabit one room and the non-positive real numbers inhabit the other. The partition P_5 has also has two rooms. The first room is the union of three intervals and the second is the

union of two intervals. Finally, the set P_5 is a partition of \mathbb{R} with infinitely many rooms, one for each integer n . A real number x inhabits the room $(n, n + 1]$ if and only if $n < x \leq n + 1$.

The next exercise shows that every nonempty set has at least two partitions.

7.1.4

Exercise

Let X be a nonempty set. Prove the following:

1. $\{X\}$ is a partition of X .
2. $\{\{x\} : x \in X\}$ is a partition of X . (Recall that $\{x\}$ is not the same as x !)

7.1.5

Exercise

For each of the following statements, find a partition of \mathbb{N} satisfying the stated requirement. You will create different partitions for each of the requirements.

1. Every room of the partition has exactly two inhabitants;
2. There are exactly three rooms in the partition;
3. There are infinitely many rooms in the partition and each room has infinitely many inhabitants.

7.2 Equivalence Relations

“Spaceship-flying computers might be the future, but it didn’t mean John Glenn had to trust them. He did, however, trust the brainy fellas who controlled the computers. And the brainy fellas who controlled the computers trusted *their* computer, Katherine Johnson. It was as simple as eighth-grade math: by the transitive property ... John Glenn trusted Katherine Johnson.”

— Margot Lee Shetterly, *Hidden Figures* [114]

At first glance, equivalence relations seem to have nothing to do with partitions. In the remainder of the chapter, however, we will see that they are essentially the same concept.

7.2.1 Definition

A **relation** R is a predicate $R(a, b)$ in two free variables, a and b . If $R(a, b)$ is true for a particular choice of a and b , we write $a R b$, which we read as “ a is related to b .”

If X is a set, a relation $R(a, b)$ is a **relation on X** if a and b are both required to be elements of X . We often use other symbols instead of R and, rather than writing R as a predicate, we simply give the condition which a and b are required to meet in order to satisfy the predicate.

7.2.2 Example

Define a relation R on \mathbb{N} by declaring $a R b$ if and only if $|b - a|$ is an odd prime. For example, $3 R 8$ but it is not the case that $7 R 9$.

7.2.3 Example

Let X be a set and define a relation R on $\mathcal{P}(X)$ by declaring ARB if and only if $A \subset B$.

As in the next two examples, we are free to use symbols other than R to denote a relation.

7.2.4 Example

Define a relation \leq on \mathbb{N}^* by declaring that $a \leq b$ if and only if there exists $m \in \mathbb{N}^*$ such that $a + m = b$. We see that the relation we have just defined coincides with the usual notion of “less than or equal to” for the extended natural numbers.

7.2.5

Example

Define a relation \sim on \mathbb{R}^2 by declaring $(x, y) \sim (a, b)$ if and only if there exists $k \neq 0$ such that $(x, y) = (ka, kb)$.

The next definition gives various properties that a relation may or may not have. We will focus on relations that are equivalence relations, although partial orders are also important in mathematics.

7.2.6

Definition

Suppose that \sim is a relation. It is:

- **reflexive** if, for all x , $x \sim x$.
- **symmetric** if, for all x, y , if $x \sim y$, then $y \sim x$.
- **antisymmetric** if whenever $x \sim y$ and $y \sim x$, then $x = y$.
- **transitive** if, for all x, y, z , if $x \sim y$ and $y \sim z$, then $x \sim z$.

If \sim is reflexive, symmetric, and transitive, it is an **equivalence relation**. If \sim is reflexive, antisymmetric, and transitive it is a **partial order**.

If we take the terminology “related” as an indication of the meaning, we can understand the definition by noting that the reflexive property means that each person is related to himself or herself; the symmetric property means that if I’m related to you then you’re related to me; transitivity means that if I’m related to you and you’re related to Mary Ellen Rudin, then I’m also related to Mary Ellen Rudin.

7.2.7

Exercise

Here is a list of sets with relations. Determine if the relation is reflexive, symmetric, antisymmetric, or transitive.

1. The real numbers \mathbb{R} with the relation \leq (the usual “less than or equal to”)

2. The set $\mathcal{P}(\mathbb{R}^2)$ with the relation \subset .

3. The set

$$N = \left\{ 0, \{0\}, \{0, \{0\}\}, \{0, \{0\}, \{0, \{0\}\}\}, \dots \right\}$$

with the relation \in (meaning “is an element of”).

4. The set $\{0, \{0\}, \{\{0\}\}\}$ with the relation \in (meaning “is an element of”).

5. The positive real numbers \mathbb{Q}^+ with the relation \sim defined by $a \sim b$ if and only if $\frac{a}{b} \leq 1$.

6. The integers \mathbb{Z} with the relation \equiv_5 , defined by declaring $x \equiv_5 y$ if and only if $x - y = 5k$ for some $k \in \mathbb{Z}$.
7. The set $\mathbb{R}^2 \setminus \{(0, 0)\}$ with the relation \sim defined by declaring $(x, y) \sim (a, b)$ if and only if there exists $k \in \mathbb{R} \setminus \{0\}$ such that $(x, y) = (ka, kb)$.
8. The set $\mathbb{Z} \times \mathbb{N}$ with the relation \sim defined by declaring $(a, b) \sim (c, d)$ if and only if $ad = bc$.
9. Let a and b be real numbers. Define $a \sim b$ if and only if $|a - b| \leq 1$.
10. Let a and b be points in \mathbb{R}^2 . Define $a \sim b$ if and only if $d(a, b) \leq 1$. (Here $d(a, b)$ is the distance from a to b .)
11. A group G having operation \circ and identity \mathbb{I} . The relation \sim is defined by declaring $g_1 \sim g_2$ if and only if there exists $h \in G$ such that $g_1 = h^{-1} \circ g_2 \circ h$.

If \sim is an equivalence relation, and if $a \sim b$ then we say that a and b are **related** or are **equivalent** (under the equivalence relation \sim). We read $a \sim b$ as “ a is related to b ” or “ a is equivalent to b .” Equivalence relations turn out to be the key to answering the questions raised at the beginning of this chapter. We often use equivalence relations when we want to think of two things which are different as being “the same.” For example, the numbers 0 and 2π are different real numbers, but when we treat them as angles they are “the same.” Since it is easy to confuse “the same” with “equal,” we prefer to say that, when thought of as angles, 0 and 2π are equivalent real numbers. The next theorem, which you’ll be asked to generalize, makes this more precise.

7.2.8

Theorem

Define the relation \sim on \mathbb{R} by declaring $x \sim y$ if and only if $x - y = 2\pi k$ for some $k \in \mathbb{Z}$. Then \sim is an equivalence relation.

Proof. We must show that \sim is reflexive, symmetric, and transitive.

Reflexive: Suppose that $x \in \mathbb{R}$. Then,

$$x - x = 0 = 2\pi(0).$$

Since $0 \in \mathbb{Z}$, $x \sim x$. Since this holds for all $x \in \mathbb{R}$, \sim is reflexive.

Symmetric: Suppose that $x, y \in \mathbb{R}$ and that $x \sim y$. We will show that $y \sim x$.

By the definition of \sim , since $x \sim y$, there exists $k \in \mathbb{Z}$ such that $x - y = 2\pi k$. Multiplying both sides of the equation by (-1) shows that

$$y - x = 2\pi(-k).$$

Since $-k$ is also an integer, $y \sim x$. Hence, \sim is symmetric.

¹Notice how we chose to use the symbol ℓ rather than to overuse k !

Transitive: Suppose that $x, y, z \in \mathbb{R}$ and that $x \sim y$ and $y \sim z$. We will show that $x \sim z$. By the definition of \sim , there exist $k, \ell \in \mathbb{Z}$ such that¹

$$\begin{aligned}x - y &= 2\pi k, \text{ and} \\y - z &= 2\pi\ell.\end{aligned}$$

Adding the two equations shows that $x - z = 2\pi(k + \ell)$. Since $k + \ell \in \mathbb{Z}$, $x \sim z$, as desired. Thus, \sim is reflexive, symmetric and transitive. Consequently, it is an equivalence relation. \square

7.2.9

Exercise

Define \sim on $\mathbb{Z} \times \mathbb{N}$ by declaring $(a, b) \sim (c, d)$ if and only if $ad = bc$. Prove that \sim is an equivalence relation. For reasons that we'll see later, you should use only facts about integers, and not any facts about rational numbers that aren't integers.

Here are some more examples. For each you should verify that it is reflexive, symmetric, and transitive.

7.2.10

Example ▶ (Equivalence Relations)

1. Let k be an integer. For $a, b \in \mathbb{R}$, define $a \sim b$ if and only if $a - b$ is a multiple of k . Then \sim is an equivalence relation on \mathbb{R} .
2. For real numbers x and y , define $x \sim y$ if and only if $x - y$ is a rational number. Then \sim is an equivalence relation on \mathbb{R} .
3. Let U be a set and let $A \subset U$ be a subset. Define $x \sim y$ if and only if either both x and y are elements of A or $x = y$. Then \sim is an equivalence relation on U .
4. Let $C([0, 1])$ be the set of all continuous real-valued functions on the interval $[0, 1] \subset \mathbb{R}$. For $f, g \in C([0, 1])$, define $f \sim g$ if and only if

$$\int_0^1 f dx = \int_0^1 g dx$$

Then \sim is an equivalence relation.

5. Let $C^1(\mathbb{R})$ be the set of all real-valued functions on \mathbb{R} which are differentiable and have continuous derivative (for example, $f(t) = e^{3t}$). For $f, g \in C^1([0, 1])$, define $f \sim g$ if and only if

$$\forall t \in \mathbb{R}, f'(t) = g'(t)$$

7.2.11

Exercise

Let U be a set and let $A \subset U$ be a subset. Define $x \sim y$ if and only if either both x and y are elements of A or both x and y are not elements of A . Show that \sim is an equivalence relation on U . As a challenge, use a partition of a nonempty set X to create an equivalence relation on X . Be sure to prove it is actually an equivalence relation.

7.2.12

Exercise

Suppose that d is a metric on a set X . For each $x \in X$ and $r > 0$, let $B_d(x, r)$ be the open ball of radius r centered at $x \in X$. That is,

$$B_d(x, r) = \{y \in X : d(x, y) < r\}.$$

For metrics d and d' , define $d \sim d'$ if and only if the following two conditions hold:

- For every $x \in X$ and $r > 0$, there exists $r' > 0$ such that

$$B_{d'}(x, r') \subset B_d(x, r).$$

- For every $x \in X$ and $r' > 0$, there exists $r > 0$ such that

$$B_d(x, r) \subset B_{d'}(x, r').$$

Prove that \sim is an equivalence relation on the set of metrics on X .

7.2.13

Exercise

Let X be a metric space and let \mathcal{D} be the set of all metrics on X . For metrics $d, d' \in \mathcal{D}$, define the following relations \sim on \mathcal{D} . For each, prove that \sim is an equivalence relation.

1. $d \sim d'$ if and only if there exists $k > 0$ such that $d'(x, y) = kd(x, y)$, for all $x, y \in X$.
2. $d \sim d'$ if and only if there exists $C \geq 0$ such that, for all $x, y \in X$,

$$d(x, y) - C \leq d'(x, y) \leq d(x, y) + C$$

3. $d \sim d'$ if and only if there exists $K \geq 1$ and $C \geq 0$ such that for all $x, y \in X$, we have

$$\frac{1}{K}d(x, y) - C \leq d'(x, y) \leq Kd(x, y) + C$$

The next theorem begins to suggest that there is a connection between partitions and equivalence relations. The idea is to show that partitions give rise to equivalence relations by defining elements of X to be related if and only if they inhabit

the same room of the partition.

7.2.14

Theorem ▶ Partitions give rise to equivalence relations

Suppose that X is a nonempty set and that P is a partition of X . Define \sim on X by declaring $a \sim b$ if and only if there exists $A \in P$ such that $a \in A$ and $b \in A$. Then \sim is an equivalence relation on X .

In the next section, we show that equivalence relations also give rise to partitions.

7.3 Equivalence Classes

"Pitch class. A pitch without reference to the octave or register in which it occurs. There are twelve pitch classes employed in Western tonal music, each of which is represented in each octave of the entire range of pitches."

– Don Michael Randel, *Harvard Concise Dictionary of Music* [106]

Given an equivalence relation on X and an element $x \in X$, it is natural to consider all the other elements of X which are related to x . This set is called the equivalence class of x . For instance, in music we often consider two pitches that are some number of octaves apart as the same note. As in the quote above, when we refer to an "A," we are referring to any number of pitches, any two of which are separated by some number of octaves. The "A" is the equivalence class of pitches, and a particular element of the class is the "A" in some particular octave, for instance, the pitch at 440 Hertz which orchestras use for tuning. More generally,

7.3.1

Definition

Let X be a set and let \sim be an equivalence relation on X . For each $x \in X$ define the **equivalence class of x** to be:

$$[x] = \{y \in X : x \sim y\}.$$

We also say that x is a **representative** of the equivalence class $[x]$.

The equivalence class of an element x depends on both the element x and on the equivalence relation \sim . Recall that $x \sim y$ means that x and y are related (using the equivalence relation \sim). Developing the metaphor, the equivalence class $[x]$ is just the family of x (that is, everyone related to x). Figure 7.3 shows an example involving families (i.e. equivalence classes) of 2-dimensional shapes.

7.3.2

Example

Let \sim be the equivalence relation on \mathbb{R} defined by declaring $x \sim y$ if and only if $x - y$ is an integer multiple of 2π . Then:

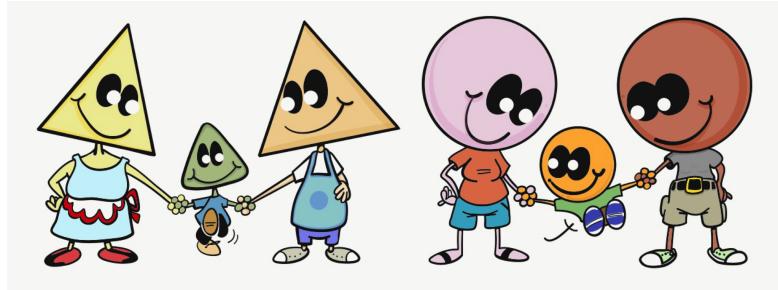


Figure 7.3: We can put an equivalence relation on shapes by declaring two shapes to be equivalent if and only if they are related by scaling and translation. The equivalence class of an equilateral triangle is its “family”: the set of all equilateral triangles. Similarly, the equivalence class of a circle is its “family”: the set of all circles.

- 7.3.2
- $[0] = \{\dots, -6\pi, -4\pi, -2\pi, 0, 2\pi, 4\pi, 6\pi, \dots\}$
 - $[\pi] = \{\dots, -3\pi, -\pi, \pi, 3\pi, 5\pi, \dots\}$.
 - $[2\pi] = \{\dots, -8\pi, -6\pi, -4\pi, -2\pi, 0, 2\pi, 4\pi, 6\pi, 8\pi, \dots\}$.

Notice that $[0] = [2\pi]$. This is not an accident, as shown by Theorem 7.3.10 below.

7.3.3 **Example ▶ (Evens and Odds)**

Let \sim be the equivalence relation on the integers defined by $x \sim y$ if and only if $x - y$ is even. Then there are precisely two equivalence classes: the even integers and the odd integers.

7.3.4 **Example ▶ (In and Out)**

Let U be a set and let $A \subset U$. Let \sim be the equivalence relation on U defined by $x \sim y$ if and only if either both x and y are elements of A or both x and y are not elements of A . There are precisely two equivalence classes: A and $U \setminus A$.

7.3.5 **Exercise**

For the following sets X , equivalence relations \sim , and elements $x \in X$, determine the equivalence class for the given element.

1. Let $X = \mathbb{Z}$. For $a, b \in X$, define $a \sim b$ if and only if $a - b \in 3\mathbb{Z}$.
 - (a) Let $x = 0$. Find $[x]$.
 - (b) Let $x = 1$. Find $[x]$.
 - (c) Let $x = 2$. Find $[x]$.
 - (d) Let $x = 3$. Find $[x]$.

- (e) Let $x = 4$. Find $[x]$.
2. Let $X = \mathcal{P}(\{1, 2, 3, 4, 5\})$. For $A, B \in X$, define $A \sim B$ if and only if A and B have the same number of elements.
- Let $A = \{1, 2\}$. Find $[A]$.
 - Let $A = \{2, 3\}$. Find $[A]$.
 - Let $A = \{1\}$. Find $[A]$.
 - Let $A = \{2\}$. Find $[A]$.
 - Let $A = \{1, 2, 3, 4, 5\}$. Find $[A]$.
3. Let $X = \mathbb{Z} \times \mathbb{N}$. Define $(a, b) \sim (c, d)$ if and only if $ad = bc$.
- Let $(a, b) = (1, 2)$. Find $[(a, b)]$.
 - Let $(a, b) = (2, 4)$. Find $[(a, b)]$.
 - Let $(a, b) = (1, 3)$. Find $[(a, b)]$.
 - Let $(a, b) = (3, 9)$. Find $[(a, b)]$.
 - Let $(a, b) = (5, 2)$. Find $[(a, b)]$.
 - Let $(a, b) = (10, 4)$. Find $[(a, b)]$.
4. Let $X = C^1(\mathbb{R})$ be the set of all real-valued functions f on \mathbb{R} such that f is differentiable and f' is continuous. Define $f \sim g$ if and only if $f'(t) = g'(t)$ for every $t \in \mathbb{R}$.

7.3.5

- Let $f(t) = t^2$ for all $t \in \mathbb{R}$. Find $[f]$.
- Let $f(t) = e^{2t}$ for all $t \in \mathbb{R}$. Find $[f]$.
- Let $f \in X$ be arbitrary. Find $[f]$.

5. Let $X = \mathbb{R}^4$. Let $W = \{(x, y, z, w) \in X : x + y + z + w = 0\}$. For $\mathbf{v}, \mathbf{w} \in X$, define $\mathbf{v} \sim \mathbf{w}$ if and only if $\mathbf{v} - \mathbf{w} \in W$.

- Let $\mathbf{v} = (0, 0, 0, 0)$. Find $[\mathbf{v}]$
- Let $\mathbf{v} = (1, 0, -1, 0)$. Find $[\mathbf{v}]$.
- Let $\mathbf{v} = (3, 3, 3, 3)$. Find $[\mathbf{v}]$.
- Let $\mathbf{v} = (4, 3, 2, 3)$. Find $[\mathbf{v}]$.

Developing the ideas from the previous example, we can begin to answer the questions posed in the introduction to the chapter.

7.3.6

Example ▶ (Angles)

Define \sim on \mathbb{R} by declaring $x \sim y$ if and only if $x - y = 2\pi k$ for some $k \in \mathbb{Z}$. Then for a given $\theta \in \mathbb{R}$, define the **angle θ radians** to be the equivalence class $[\theta]$. We claim that $[\theta] = [\theta + 2\pi k]$ for any $k \in \mathbb{Z}$. Assuming the claim, we see that angle θ radians is equal to the angle $\theta + 2\pi k$ radians for any $k \in \mathbb{Z}$.

7.3.7

Exercise

Prove the claim in Example 7.3.6. Have we shown that $(a, b) \sim (c, d)$ if and only if there exists $k \in \mathbb{N}$ such that $(c, d) = (ka, kb)$ or $(a, b) = (kc, kd)$? If not, is this something you could prove?

7.3.8

Example ▶ (Rational Numbers)

Define \sim on $\mathbb{Z} \times \mathbb{N}$ by declaring $(a, b) \sim (c, d)$ if and only if $ad = bc$. For a given pair $(a, b) \in \mathbb{Z} \times \mathbb{N}$, we let the notation $\frac{a}{b}$ mean the equivalence class $[(a, b)]$. We claim that

$$[(a, b)] = [(ka, kb)]$$

for any $k \in \mathbb{N}$. Thus, we have the well known fact that:

$$\frac{a}{b} = \frac{ka}{kb}$$

for every $k \in \mathbb{N}$.

7.3.9

Exercise

Prove the claim in Example 7.3.8.

In Exercise 7.3.5, and based on Examples 7.3.6 and 7.3.8, you may have begun to guess that equivalence classes are equal whenever their representatives are related. We can think of this using a familial metaphor. Informally:

- each person is a member of their own family;
- if two people are related then they have the same families; and
- two people's families are either exactly the same or have no person in common.

Two elements are related exactly when they have the same family. Although the metaphor helps us believe that $x \sim y$ exactly when $[x] = [y]$, we actually need to prove this. The proof is a lengthy series of element arguments using the reflexive, symmetric, and transitive properties.

7.3.10

Theorem ▶ Fundamental Properties of Equivalence Relations

Let X be a set and assume that \sim is an equivalence relation on X . Then the following are true:

1. For every $x \in X$, $x \in [x]$.
2. For all $x, y \in X$, we have $x \sim y$ if and only if $[x] = [y]$.
3. For all $x, y \in X$, if $[x] \cap [y] \neq \emptyset$, then $[x] = [y]$.

Proof. We prove each of the three required properties.

Proof of (1): Let $x \in X$.

(Use the reflexive property and the definition of equivalence class to show that $x \in [x]$.)

Proof of (2): We must prove both directions. Let $x, y \in X$ be arbitrary.

Proof of \Rightarrow : Assume that $x \sim y$. We must show that $[x] = [y]$.

(Choose an arbitrary element of $[x]$ – but don't call it x , since that's already taken! – and show that it is also an element of $[y]$.)

(Choose an arbitrary element of $[y]$ – but don't call it y , since that's already taken! – and show that it is also an element of $[x]$.)

Hence $[x] \subset [y]$ and $[y] \subset [x]$, so $[x] = [y]$.

Proof of \Leftarrow : Assume that $[x] = [y]$. We will show that $x \sim y$.

(Do it!)

Proof of (3): Suppose that $[x] \cap [y] \neq \emptyset$. We will show that $[x] = [y]$.

Let $z \in [x] \cap [y]$.

(Use previous results to show that $[z] = [x]$ and $[z] = [y]$ and, therefore, that $[x] = [y]$.)

□

7.4 Quotient Sets

“Both visual and musical compositions are appreciated for the beauty of a set of complex relations embodied in them. And as in pure mathematics, so also in the abstract arts, these interesting relationships are discovered, or created, within structures composed of utterances denoting no tangible object.” – Michael Polanyi¹

At the very beginning of the book, we said that sets are a way of thinking of a “many” as a “one.” Given an equivalence relation on X and the equivalence classes $[x] \in X$ for all $x \in X$, we can package the equivalence classes together into a set, called the quotient set. Since each $[x] \subset X$, the quotient set will be a set whose elements are sets. Indeed, the quotient set is a subset of $\mathcal{P}(X)$.

7.4.1

Definition ► Quotient Set

Let \sim be an equivalence relation on a set X . Define the **quotient set** X/\sim to be the set such that $z \in X/\sim$ if and only if there exists $x \in X$ such that $z = [x]$. That is,

$$X/\sim = \{[x] : x \in X\}$$

If the equivalence class $[x]$ of x is x ’s family, we might think of the quotient set A/\sim as a church picnic – a gathering of all the families, as in Figure 7.4. We need to remember that, as with actual church picnics, families can be of different sizes. Some equivalence classes may have just 1 element; some may have 2 elements; some may even have infinitely many elements!

7.4.2

Example ► (Evens and Odds, again)

Let \sim be the equivalence relation on the integers defined by $x \sim y$ if and only if $x - y$ is even. Then there are precisely two equivalence classes: the even integers and the odd integers. Thus, $\mathbb{Z}/\sim = \{[0], [1]\}$.

7.4.3

Example ► (In and Out, again)

Let U be a set and let $A \subset U$. Let \sim be the equivalence relation on U defined by $x \sim y$ if and only if either both x and y are elements of A or both x and y are not elements of A . There are precisely two equivalence classes: A and $U \setminus A$. Thus, $U/\sim = \{A, U \setminus A\}$.

7.4.4

Example ► (Angles, again)

Let \sim be the equivalence relation defined on \mathbb{R} by declaring $x \sim y$ if and only if $x - y = 2\pi k$ for some $k \in \mathbb{Z}$. An **angle measured in radians** is an equivalence class $[\theta] \in \mathbb{R}/\sim$ and the quotient set \mathbb{R}/\sim is the **set of angles measured in radians**.

¹The quotation can be found on page 193 of [102].

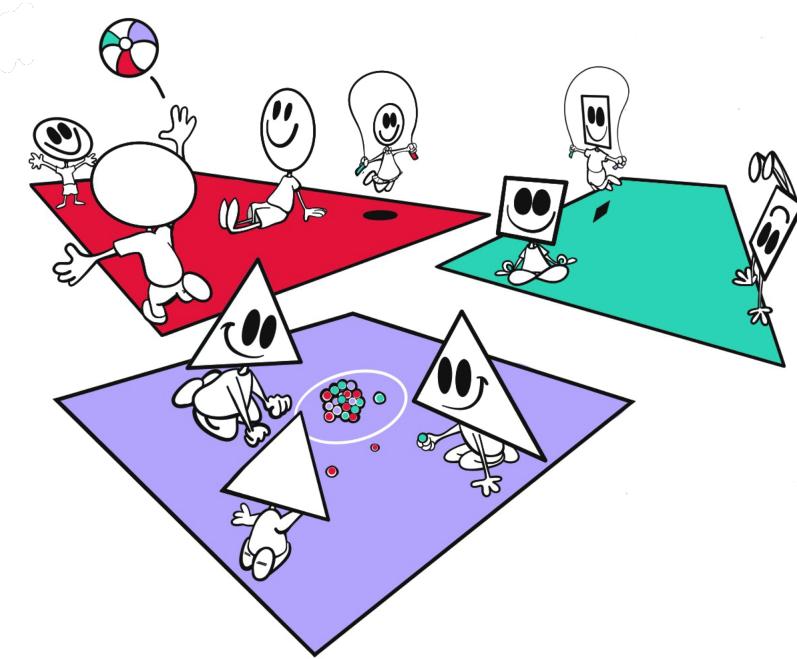


Figure 7.4: The quotient set is the set of all equivalence classes. Each element of the quotient set is an equivalence relation, that is a set of related elements.

7.4.5 Example ► (Rationals, again)

Let \sim be the equivalence relation defined on $\mathbb{Z} \times \mathbb{N}$ by declaring $(a, b) \sim (c, d)$ if and only if $ad = bc$. The set of **rationals** is the quotient set $\mathbb{Q} = (\mathbb{Z} \times \mathbb{N})/\sim$. An element of \mathbb{Q} of the form $[(a, b)]$ is denoted by $\frac{a}{b}$.

7.4.6 Exercise

Determine the quotient set X/\sim for each of the following equivalence relations.

1. Let $X = \mathbb{Z}$ and define $a \sim b$ if and only if $b - a \in 3\mathbb{Z}$.
2. Let $X = \mathbb{Z}$ and define $a \sim b$ if and only if $b - a \in 4\mathbb{Z}$.
3. Let $X = \mathbb{R}^2$ and define $(x, y) \sim (a, b)$ if and only if one of the following holds:
 - $x \geq y$ and $a \geq b$
 - $x < y$ and $a < b$.
4. Let $X = \mathbb{R}^2$ and define $(x, y) \sim (a, b)$ if and only one of the following holds:
 - $x \geq 0, y \geq 0, a \geq 0, b \geq 0$
 - $x < 0, y < 0, a < 0, b < 0$

- $xy < 0$ and $ab < 0$.
- $x = 0$ and $y < 0$ and $a = 0$ and $b < 0$.
- $y = 0$ and $x < 0$ and $b = 0$ and $a < 0$.

7.4.7

Example

Let $X = [0, 1] \subset \mathbb{R}$ and let $A = \{0, 1\} \subset X$. Define $x \sim y$ if and only if either both x and y are elements of A or both x and y are elements of A^C . Then X/\sim “is” a circle, as in Figure 7.5.

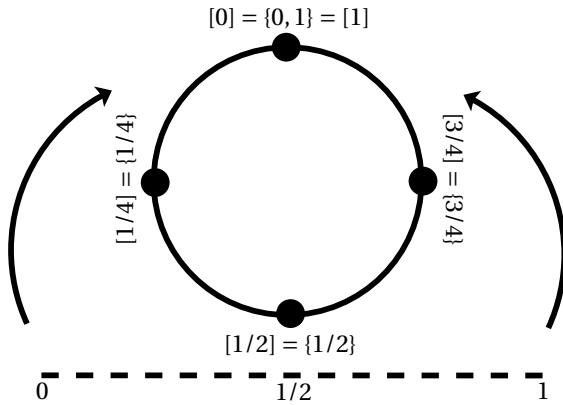


Figure 7.5: The circle “is” the quotient space of the interval under the relation \sim defined by $x \sim y$ if and only if $x = y$ or $\{x, y\} = \{0, 1\}$.

7.4.8

Example

Let $S = [-1, 1] \times [-1, 1] \subset \mathbb{R}^2$. Define an equivalence relation on S as follows:

- For every $(x, y) \in S$, $(x, y) \sim (x, y)$.
- For every $y \in [-1, 1]$, let $(-1, y) \sim (+1, y)$ and $(+1, y) \sim (-1, y)$.

(Check that this actually is an equivalence relation.) In essence, we have taken a solid square and declared each point on a vertical edge to be “the same as” the corresponding point on the opposite vertical edge. In essence, we have glued the vertical edges together. We can draw a picture of this, if we allow ourselves to bend and distort. See Figure 7.6.

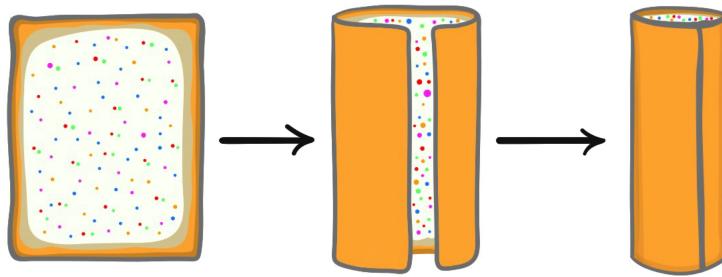


Figure 7.6: Rolling up a toaster pastry and sealing the edges with frosting, makes a cylinder!

7.4.9 Example

Let $S = [-1, 1] \times [-1, 1] \subset \mathbb{R}^2$. Define an equivalence relation on S as follows:

- For every $(x, y) \in S$, $(x, y) \sim (x, y)$.
- For every $y \in [-1, 1]$, let $(-1, y) \sim (+1, y)$ and $(+1, y) \sim (-1, y)$.
- For every $x \in [-1, 1]$, let $(x, -1) \sim (x, +1)$ and $(x, +1) \sim (x, -1)$.

(Check that this actually is an equivalence relation.) We have taken a solid square and declared each point on the edge to be “the same as” the point on the edge opposite it. The four corners of the square are all equivalent to each other. In essence, we have glued opposite points on the boundary of the square together. We can draw a picture of this, if we allow ourselves to bend and distort. See Figure 7.7.

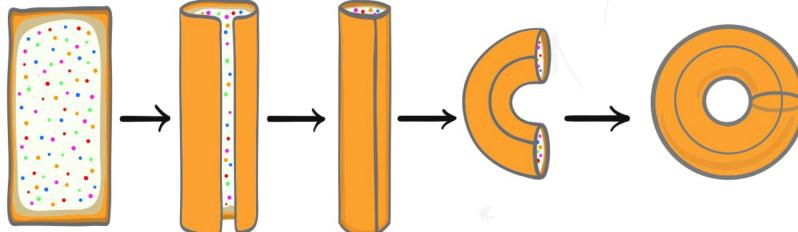


Figure 7.7: How to make a hollow bagel from a toaster pastry.

In Figure 7.5, the word “is” was in scare quotes, since we have discussed only the definition of a particular set (the quotient set). For instance, in Example 7.4.7, the circle S^1 is literally the set $\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$, but that is not, as a set, equal to X/\sim . To claim that the quotient set X/\sim *is* the circle, we should have a way of taking any concept which is defined for S^1 or any theorem which is true for S^1 and converting into a similar concept or true theorem for X/\sim .

Similarly, in Examples 7.4.4 and 7.4.5, we need to be careful when we claim that we have created the set of angles or the set of rationals. To most of us, the set of angles or the set of rationals is more than just a set - it comes with extra structure. For instance, we may want to add angles or rationals or we may want to be able to discuss what it means for two angles or two rationals to be close to each other. Simply writing a set as quotient sets does not by itself mean that the set comes equipped with the ability to add or with a metric. We'll take this issue up again in Section 7.6.

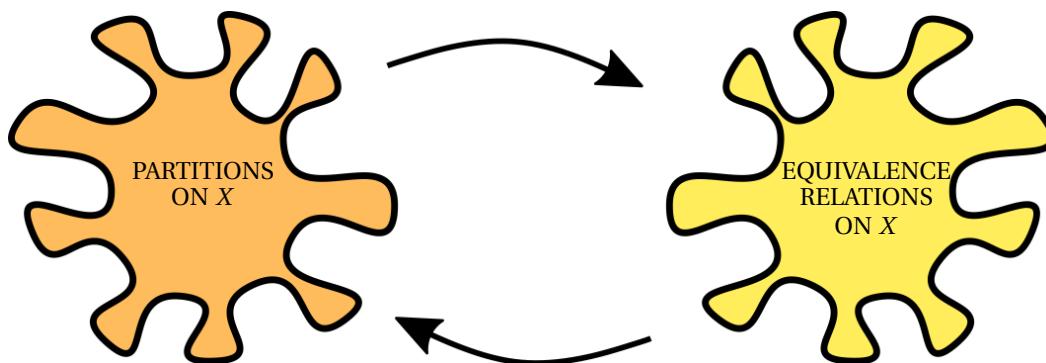
Look back over each example in the previous exercise. Notice that in each case X/\sim is a partition of X . The next section shows this is not an accident.

7.5 Equivalence Relations vs. Partitions

"[A]t each step, it was a struggle that I loved working through. I didn't mind being stuck and feeling dumb. I knew I could get through it if I kept plugging away. In today's language, I would say that I was lucky to have formed a 'growth mindset' about learning math – I was willing to work on hard problems to find success – rather than a 'fixed mindset,' where I judged myself harshly when I didn't know something. To this day, I still benefit from this mindset, and I've basically made a career out of trying new things that I don't know anything about. It's in the process of making mistakes and figuring out how to make progress where the real fun begins.

– Laura Taalman¹

In this section, we see that every equivalence relation gives rise to a partition and we will also see how every partition gives rise to an equivalence relation; equivalence relations and partitions are two sides of the same coin.



We saw in Theorem 7.2.14 that, given a partition P on a set X , we can define an induced equivalence relation \sim_P on X by declaring two elements of X to be related if and only if they inhabit the same room. If, on the other hand, we begin

¹Laura Taalman is a mathematician, 3D-print designer, and Calculus textbook author. This quote is from the book [68], a collection of autobiographical stories of mathematicians persisting through struggle.

with an equivalence relation \sim on X , the quotient set X/\sim is a partition of X . The rooms are the equivalence classes. Since two elements of X inhabit the same equivalence class if and only if they are related, the induced equivalence relation from this partition is equal to the original equivalence relation \sim . The next two results make this relationship precise. The first result has a straightforward proof using Theorem 7.3.10.

7.5.1

Theorem ▶ Quotient sets are partitions

Suppose that X is a set and that \sim is an equivalence relation on X . Then the quotient set X/\sim is a partition P of X . Furthermore, two elements of X are related by the equivalence relation \sim if and only if they are related by the induced equivalence relation \sim_P .

7.5.2

Theorem ▶ Partitions induce equivalence relations

Given a partition P of a set X and the equivalence relation \sim_P defined above, we have $X/\sim_P = P$.

7.6 Angle addition

“If a crocodile is aimed from upriver to eat the monkey
and an anaconda from downriver burns
with the same ambition, I do
the math, algebra, angles, rate-of-monkey,
croc- and snake-speed, ...”

– Thomas Lux, *To Help the Monkey Cross the River* [86]

Recall from Example 7.4.4, our definition of “angle”:

7.6.1

Definition ▶ Angles

An **angle** is an element of \mathbb{R}/\sim where $x \sim y$ if and only if $x = y + 2\pi k$ for some $k \in \mathbb{Z}$. We say that the equivalence class $[x] \in \mathbb{R}/\sim$ is an angle of x **radians**.

We know from experience that the idea of adding two angles makes sense. For example, if we add π radians to π radians we get 2π radians and if we add 3π radians to π radians we still get 2π radians (which is the same angle as 4π radians). To make this notion of angle addition mathematically precise, we do the following:

7.6.2

Definition

Suppose that $[x], [y] \in \mathbb{R}/\sim$ are angles. We define their sum by

$$[x] + [y] = [x + y].$$

Just because we declare a definition, doesn't mean that it makes sense. In particular, we know that $[0] = [2\pi]$ and that $[\pi/3] = [-(11/3)\pi]$. Clearly we want

$$[0] + [\pi/3] = [2\pi] + [-(11/3)\pi].$$

But does equality actually hold, when we insist on using Definition 7.6.2? The next lemma guarantees that angle addition makes sense, not just in that specific case, but in all cases.

7.6.3

Lemma

Suppose that $[x] = [a]$ and $[y] = [b]$. Then $[x] + [y] = [a] + [b]$.

Proof. By definition $[x] + [y] = [x + y]$ and $[a] + [b] = [a + b]$. We must show that $[x + y] = [a + b]$.

Since $[x] = [a]$ and $[y] = [b]$, by Theorem 7.3.10 we must have $x \sim a$ and $y \sim b$. By the definition of \sim , ____.

⟨ Finish the thought ⟩

⟨ Show that $x + y \sim a + b$. ⟩

Thus, by Theorem 7.3.10, we have $[x + y] = [a + b]$, as desired. \square

As a result of Lemma 7.6.3, we say that angle addition is **well-defined**. We also need to show that addition has all the usual properties: that is, angles with $+$ form a group.

7.6.4

Lemma

Let A be the set of angles and let $+$ be defined as above. Using $+$ as the operation and $[0]$ as the identity, A is a group. Furthermore, for all $[x], [y] \in A$, $[x] + [y] = [y] + [x]$.

Proof. We must show that $(A, [0], +)$ satisfies the axioms of a group and, additionally, that $+$ is commutative. We supply the proof that $+$ is associative and leave the other proofs for the reader.

Claim: Angle addition is associative.

The proof is based on the fact that addition of real numbers is associative. Let $[x]$, $[y]$, and $[z]$ be angles. We must show that

$$([x] + [y]) + [z] = [x] + ([y] + [z]).$$

By the definition of $+$, $([x] + [y]) = [x + y]$. Hence,

$$([x] + [y]) + [z] = [(x + y)] + [z] = [(x + y) + z].$$

Similarly,

$$[x] + ([y] + [z]) = [x] + ([y + z]) = [x + (y + z)].$$

Since addition of real numbers is associative, $x + (y + z) = (x + y) + z$. Consequently,

$$[(x + y) + z] = [x + (y + z)].$$

And so,

$$([x] + [y]) + [z] = [x] + ([y] + [z]) \quad \square(\text{Claim})$$

(Finish the proof of the theorem!)

□

7.7 Constructing the integers and rationals

“And further I discovered to them numbering, pre-eminent among subtle devices ...”

– Aeschylus¹, *Prometheus Bound* [5]

In this section we show how, knowing only about the natural numbers, the concept of an equivalence relation allows us to create the integers and the rational numbers. The ideas themselves are lovely, but they are also practical: computers begin life simply as electrical circuits; they know nothing about mathematics and they have to be “taught” how to work with integers and rational numbers. The constructions in this section give one way this might be done (assuming the computer already knows about the natural numbers.)

Constructing the integers

Assume that, as in Section 2.4, we have from first principles constructed the sets \mathbb{N} and $\mathbb{N}^* = \mathbb{N} \cup \{0\}$. Assume also that we have defined all the basic concepts from arithmetic for the numbers in \mathbb{N}^* . For example, given $a, b \in \mathbb{N}^*$ we know what the numbers $a + b$ and $a \cdot b = ab$ are. We also know what the symbols $a \leq b$ mean. Not only that, we understand the basic rules governing the interaction between the symbols. For example, we know that if $a, b, c \in \mathbb{N}^*$ then $a(b + c) = ab + ac$ and $b \leq c \Rightarrow ab \leq ac$. Here are some of the basic facts we assume we know for all $a, b, c \in \mathbb{N}^*$:

- If $a + b = c$ and $a + b' = c$, then $b = b'$ (the cancellation property for addition)
- $a + 0 = 0 + a = a$ (0 is the additive identity)
- If $ab = c$ and $ab' = c$ then $b = b'$ (the cancellation property for multiplication).

¹In Greek mythology, Prometheus is the giver of gifts to humankind, including the gift of arithmetic.

We now need to define the set \mathbb{Z} and show how the definitions of addition, multiplication, and \leq can be extended to \mathbb{Z} so that all the familiar properties from arithmetic hold. This actually takes rather a lot of fairly tedious effort, so we will only give the flavor of how this is done.

7.7.1

Definition ▶ Negative naturals

For $a \in \mathbb{N}$, let $-a$ denote the ordered pair $(1, a)$ and define $-(-a) = a$. Let $-\mathbb{N} = \{-a : a \in \mathbb{N}\}$ and let $\mathbb{Z} = -\mathbb{N} \cup \mathbb{N}^*$.

7.7.2

Definition ▶ Addition for \mathbb{Z}

Define the following for $a, b \in \mathbb{Z}$:

$$a+b = \begin{cases} a+b & \text{if } a, b \in \mathbb{N}^* \\ c & \text{if } a \in \mathbb{N}^*, b \in -\mathbb{N} \text{ and } (-b) + c = a \text{ for some } c \in \mathbb{N}^* \\ c & \text{if } b \in \mathbb{N}^*, a \in -\mathbb{N} \text{ and } (-a) + c = b \text{ for some } c \in \mathbb{N}^* \\ -((-a) + (-b)) & \text{if } a, b \in -\mathbb{N} \end{cases}$$

7.7.3

Exercise

Using basic facts about the definition of $+$ for elements of \mathbb{N}^* and using Definition 7.7.2 prove the following facts:

1. For all $a \in \mathbb{Z}$, $a + 0 = 0 + a = a$.
2. For all $a, b \in \mathbb{Z}$, $a + b = b + a$.

7.7.4

Exercise

Use multiplication on \mathbb{N}^* to define multiplication on \mathbb{Z} . Show the commutative, associative, and distributive properties.

Constructing the rationals

We now assume that we have constructed \mathbb{Z} and that it is possible to add, subtract, multiply, and compare these numbers and that these operations work they way we learned they do in elementary school. We must define \mathbb{Q} , extend the definitions of $+$, \cdot , and \leq to elements of \mathbb{Q} and prove that these operations continue to work the way we expect them to. Once again to completely carry out this program requires too much tedium, but we do enough to give the flavor of how it can be done.

The next definition appeared as Definition 7.4.5.

7.7.5

Definition

The rational numbers \mathbb{Q} are defined to be the quotient set $(\mathbb{Z} \times \mathbb{N})/\sim$ where

$$(a, b) \sim (c, d)$$

if and only if $ad = bc$. We will write $\frac{a}{b}$ instead of $[(a, b)]$.

Recall from Exercise 7.2.9 that the relation \sim in Definition 7.7.5 is an equivalence relation.

7.7.6

Definition

We define the following operations on \mathbb{Q} :

- Addition is defined by

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

- Negation is defined by

$$-\frac{a}{b} = \frac{-a}{b}$$

- Multiplication is defined by

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Also we say that

$$\frac{0}{1} \leq \frac{a}{b}$$

if and only $ab \in \mathbb{N}^*$.

If r and q are rational numbers, we define $r - q$ to be equal to $r + (-q)$. We say that $q \leq r$ if and only if $\frac{0}{1} \leq r - q$.

7.7.7

Lemma

The previous definitions of $-$, $+$, \cdot , and \leq are well-defined. That is, they do not depend on the particular members of the equivalence classes used in the definitions.

Question: Where do these definitions come from?

Answer: They come from the fact that we already *know* how rational numbers should behave.

Question: If we already know how rational numbers should behave, why should we do all this hard work?

Answer: It's the work that shows us these basic arithmetic facts can be created solely from the axioms of set theory. Furthermore, maybe we can adapt the con-

struction to create brand new number systems! In Chapter 12, we will show how to construct the reals from the rationals and we will adapt a construction of the *real numbers* to create a new number system called the 10-adics.

Notice that our construction of the integers \mathbb{Z} does make \mathbb{N} a subset of \mathbb{Z} ; but our creation of \mathbb{Q} does *not* make \mathbb{Z} a subset of \mathbb{Q} . This can be rectified by redefining the integer n to be the rational number $\frac{n}{1}$ for all $n \in \mathbb{Z}$. We should then show that this redefinition preserves all of the structures on \mathbb{Z} (such as addition, multiplication, and the notion of \leq). We'll move onto different things instead, but at this point you know enough that you could complete the task if you were sufficiently motivated.

7.8 Modular Arithmetic

“No bodily sense makes contact with all numbers, for they are innumerable. How do we know that this rule holds throughout? How can any phantasy or phantasm yield such certain truth about numbers which are innumerable? We must know this by the inner light, of which bodily sense knows nothing.”

– Augustine¹, *On Free Will* [8]

7.8.1 Exercise

What day of the week will it be in 180 days?

If you answered this question quickly and correctly, it's likely that you divided 180 by 7, found the remainder to be 5, and either counted forward from 5 days from today or two days backward from today. If you did this, you used modular arithmetic. Modular arithmetic is a valuable concept in its own right and it provides a wonderful forum for using equivalence classes.

The basic idea is, once a natural number p is chosen, to define integers a and b to be **equivalent modulo p** if and only if their difference is an integer multiple of p . More formally, let $p \in \mathbb{N}$ and define the relation \equiv_p on \mathbb{Z} as follows:

$$(a \equiv_p b) \Leftrightarrow \exists k \in \mathbb{Z} \text{ s.t. } b = a + kp.$$

We say that a is **equivalent** (or **congruent**) to b modulo (or mod) p . Some authors write $a \equiv b \pmod{p}$ instead of $a \equiv_p b$.

7.8.2

Theorem ▶ Equivalence mod p is an equivalence relation

If $p \in \mathbb{N}$, then \equiv_p is an equivalence relation on \mathbb{Z} .

¹ Augustine (343 - 430) was from the North African city of Hippo and is the most influential of all post-Biblical Christian theologians. Much of his work concerns the application of Platonic philosophy to Christian belief and practice. This quote is from a section of his writing where he compares the pursuit of wisdom to the understanding of numbers.

The quotient set \mathbb{Z}/\equiv_p is usually denoted $\mathbb{Z}/p\mathbb{Z}$ (or by some authors \mathbb{Z}_p). We refer to the set as the “integers mod p .” The key to connecting the integers mod p to Exercise 7.8.1 lies in understanding the relationship between the equivalence classes which are elements of $\mathbb{Z}/p\mathbb{Z}$ and division of integers. We’ll use the division algorithm which says that when dividing an integer n by a natural number p , the remainder r will always be strictly less than p . We’ll prove the division algorithm in Chapter 9. More precisely, for $p \geq 1$, the division algorithm implies that for every $n \in \mathbb{Z}$, there exist unique $q \in \mathbb{Z}$, $r \in \mathbb{N}^*$ such that

$$n = pq + r$$

and

$$0 \leq r < p.$$

It follows that the possible remainders when dividing by p are:

$$0, 1, 2, \dots, p - 1.$$

When $n = pq + r$, we have $n - r \in p\mathbb{Z}$. Thus, $n \equiv_p r$. We conclude that

$$\mathbb{Z}/p\mathbb{Z} = \{[0], [1], \dots, [p - 1]\}.$$

Figure 7.8 uses this insight to depict the integers modulo 8.

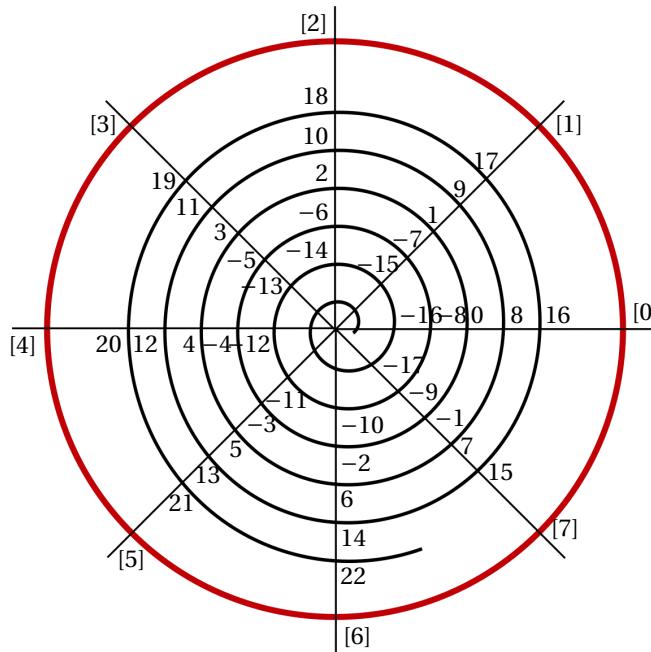


Figure 7.8: We can picture the integers modulo 8 by placing the number line in an infinite spiral so that it makes a complete turn every 8 integers. Integers on the same ray extending from the center of the spiral lie in the same equivalence class. The red outer circle shows the equivalence classes.

Just as we extended the definition of addition and multiplication from \mathbb{Z} to \mathbb{Q} , we can also extend it from \mathbb{Z} to $\mathbb{Z}/p\mathbb{Z}$.

7.8.3

Definition

Suppose that $p \in \mathbb{N}$, then we define $+$ and \cdot on $\mathbb{Z}/p\mathbb{Z}$ as follows:

- $[a] + [b] = [a + b]$
- $[a] \cdot [b] = [a \cdot b]$.

In other words, the sum of the classes is the class of the sums and the product of the classes is the class of the products.

7.8.4

Example

Let $p = 5$. We work in $\mathbb{Z}/5\mathbb{Z}$. From the definition of addition, we have:

$$[0] + [2] = [2]$$

and

$$[5] + [7] = [12].$$

But recall that $0 \equiv_5 5$ and $2 \equiv_5 7$. Thus, $[0] = [5]$ and $[2] = [7]$ (by Theorem 7.3.10). Fortunately, $2 \equiv_5 12$, so $[2] = [12]$.

Similarly, from the definitions, we have

$$[0] \cdot [2] = [0]$$

and

$$[5] \cdot [7] = [35].$$

Observe that $[0] = [35]$.

In the previous example, we've seen how different ways of writing the equivalence classes produced answers after addition or multiplication which looked different but which were actually equal. Was this just a fluke of our choice to consider $p = 5$, or perhaps our choice to consider the classes $[0]$ and $[2]$? As we've seen, just because we make a definition, doesn't mean that it doesn't lead to contradictions.

More generally, in the definition of $+$ on $\mathbb{Z}/p\mathbb{Z}$, for instance, we use particular representatives of the classes $[a]$ and $[b]$ to define $[a] + [b]$. However, we know that if $a' \in [a]$ and $b' \in [b]$ then $[a'] = [a]$ and $[b'] = [b]$. With our definition, are we guaranteed that $[a'] + [b'] = [a] + [b]$? The next lemma says "yes".

7.8.5

Lemma ▶ Modular arithmetic is well-defined.

Suppose that $[a'] = [a]$ and $[b'] = [b]$. Then $[a'] + [b'] = [a] + [b]$ and $[a'] \cdot [b'] = [a] \cdot [b]$.

7.8.6

Theorem

Let $p \in \mathbb{N}$. Then $(\mathbb{Z}/p\mathbb{Z}, [0], +)$ is a group such that the operation $+$ is commutative.

7.9 Application: Configuration spaces of unlabelled points

“When discussing a particular piece of mathematics, the mathematician may ask, ‘Now, what is really going on here?’ That is, what is the core mathematical idea? A piece of mathematics, a proof for example, may go on for pages and pages and may include detailed calculations and subtle logical arguments. However, there is often a surprisingly concise mathematical idea that forms the basis for all the detailed work.”

—William Byers, *How Mathematicians Think* [22]

In Section 5.8, we considered the problem of describing all possible positions of two robots MARVIN and K-9 who can move around the factory floor $F = [0, 1] \times [0, 1]$. We saw that their possible positions are described by the **configuration space** $\mathcal{C}^2(F) = (F \times F) \setminus \Delta$ where $\Delta = \{(a, b) \in F \times F : a = b\}$ is the diagonal¹. Since elements of $\mathcal{C}^2(F)$ are of the form (a, b) with $a, b \in F$ and $a \neq b$, we see that the single point $(a, b) \in \mathcal{C}^2(F)$ tells us the position $a \in F$ of MARVIN and the position $b \in F$ of K9. We subtract the diagonal Δ from $F \times F$ to ensure that the two robots never occupy the same location.

A similar problem is to find a way of describing all possible positions of two indistinguishable points in a set (likely a metric space) F . For instance, if we have two specks of dust moving around in a soap film, we could begin by considering the configuration space of two labelled points as we did previously. Supposing that the soap film can be described as a square $F = [0, 1] \times [0, 1]$, then each element of the set $\mathcal{C}^2(F) = (F \times F) \setminus \Delta$ is a potential position of the two dust specks. However, this description is unsatisfactory as our dust specks (unlike MARVIN and K9) are indistinguishable from each other. To see this, observe that $(a, b) \in \mathcal{C}^2(F)$ is never equal to (b, a) , but since the specks are indistinguishable the points (a, b) and (b, a) represent the same configuration of dust specks. Indeed, for each possible position of the two dust specks we have *two* elements of $\mathcal{C}^2(F)$. Although we could just work with this ambiguity, it would be better to find a set such that there is a (natural) correspondence between elements of the set and positions of the dust specks. We can create such a set using an equivalence relation. For notational convenience, we denote $\mathcal{C}^2(F)$ simply by \mathcal{C} .

¹Remember that since $a, b \in F = [0, 1] \times [0, 1]$, we have $(a, b) = ((x, y), (z, w))$ for some $x, y, z, w \in [0, 1]$.

7.9.1

Definition ▶ Unordered Configuration Space

Suppose that F is a set. The **ordered configuration space** of two distinguishable points in X is the set

$$\mathcal{C} = (F \times F) \setminus \Delta$$

where $\Delta = \{(a, b) \in F \times F : a \neq b\}$. The **unordered configuration space** of two *indistinguishable* points in X is the quotient set

$$\overline{\mathcal{C}} = \mathcal{C} / \sim$$

where \sim is the equivalence relation defined as follows. For $(a, b), (c, d) \in \mathcal{C}$, declare $(a, b) \sim (c, d)$ if and only if $(a, b) = (c, d)$ or $(a, b) = (d, c)$.

7.9.2

Exercise

Verify that \sim is an equivalence relation.

Observe that each element $[(a, b)] \in \overline{\mathcal{C}}$ is the set whose elements are (a, b) and (b, a) . Thus, the elements of $\overline{\mathcal{C}}$ are in bijection with positions of two indistinguishable points in F .

It may seem that we haven't gained much by this construction. However, in many instances, we can analyze the set $\overline{\mathcal{C}}$ (along with whatever other structures it might admit) to gain a useful perspective on possible point positions in F . For instance, if we let $F = [0, 1]$ (so we are considering the positions of two indistinguishable points on a line segment), then $\overline{\mathcal{C}}$ is the triangle pictured on the right of Figure 7.9. Formally, we have chosen from each class $[(x, y)] \in \overline{\mathcal{C}}$ the element which is in the upper left half of the square $[0, 1] \times [0, 1]$.

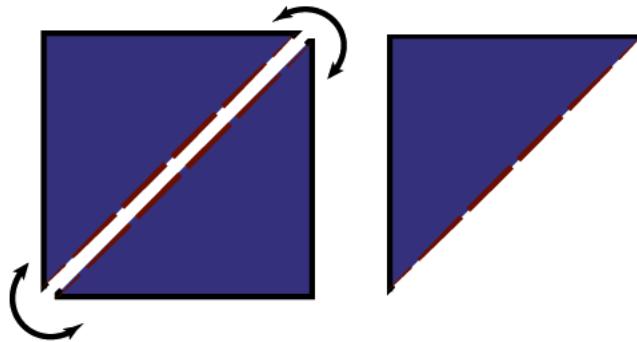


Figure 7.9: On the left we notice that $[0, 1] \times [0, 1] \setminus \Delta$ is union of two triangles. On the right, we apply the equivalence relation to glue the two triangles together. The resulting unordered configuration space is equivalent to a right triangle with missing hypotenuse, depicted on the right.

If instead we consider $F = S^1 = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$, then $F \times F$ is the torus $S^1 \times S^1$, which we represent as a square with opposite sides identified. Then, \mathcal{C} is the result of removing a certain curve $\Delta = \{(a, b) \in S^1 \times S^1 : a = b\}$ from the torus,

as on the top left of Figure 7.10. Recall that the four corners of the square all represented the same point of $F \times F$ and that deleting Δ removes that point, so \mathcal{C} consists of two triangles each with a single edge and all vertices removed. Taking the quotient, to arrive at $\overline{\mathcal{C}}$, we identify the lower triangle with the upper triangle via the reflection across the line $y = x$. As before, we can depict the result of the gluing as a triangle. For convenience, we stretch the triangle out to a rectangle with two opposite sides deleted and the other two opposite sides identified via a map that flips one of the edges. We see, therefore, that there is a sense in which $\overline{\mathcal{C}}$ is an open Möbius band. We conclude that each point on a Möbius band (with its boundary edge removed) corresponds to a positioning of two distinct but indistinguishable points on a circle.

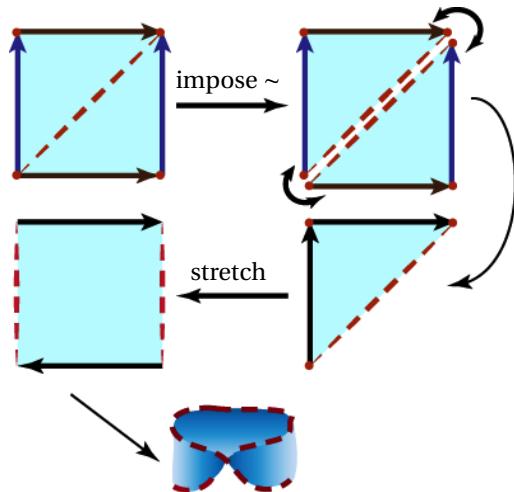


Figure 7.10: On the top left we have the ordered configuration space of two points on a circle. Moving to the top right, we impose an equivalence relation to obtain the unordered configuration space. We then manipulate the diagram to conclude that the unordered configuration space of two indistinguishable points on a circle can be represented as a Möbius band.

7.10 Additional Problems

“I will never write a student off or underestimate their ability to learn. I will never separate my students into the categories of those who can do math and those who cannot – only those who aspire to do the work that it takes to succeed in math and those who do not. I try to give generously of myself to my students and show them the grace that was shown to me so many years ago. In the end, this is all that any of us can do to make room in the mathematics community for everyone.” –Emille Davie Lawrence¹

1. Consider a graph G with a vertex set V and an edge set E . Define a relation \sim on V such that $a \sim b$ if and only if there is an edge $e \in E$ having endpoints a and b . What conditions must G satisfy in order for \sim to be an equivalence relation?
2. Suppose that G is a graph with vertex set V and edge set E . Define a relation \sim on V as follows. Declare $a \sim b$ if and only there is a list of vertices

$$v_0, v_1, \dots, v_n$$

(which can be however long or short we want) such that $a = v_0$, $b = v_1$ and for each $i \in \{0, \dots, n-1\}$, the vertices v_i and v_{i+1} are the endpoints of an edge in G . Prove that \sim is an equivalence relation.

3. The following concern partial orders. We use \leq to denote any partial order, not just the usual “less-than-or-equal-to” for real numbers.
 - (a) Let Y be a set and let $X = \mathcal{P}(Y)$. Define \leq on X by declaring $A \leq B$ if and only if $A \subset B$. Prove that \leq is a partial order. Give an example of a set Y and elements $A, B \in \mathcal{P}(Y)$ such that neither $A \leq B$ nor $B \leq A$. This indicates one substantial difference between partial orders in general and the notion of “less-than-or-equal-to” on \mathbb{R} .
 - (b) Let Y be a set and let $X = \mathcal{P}(Y)$. Define \leq on X by declaring $A \leq B$ if and only if $A \supseteq B$. Prove that \leq is a partial order.
 - (c) Define \leq on \mathbb{R}^3 by declaring $(x, y, z) \leq (a, b, c)$ if and only if one of the following occurs:
 - $(x, y, z) = (a, b, c)$,
 - $x < a$,
 - $x = a$ and $y < b$,
 - $x = a$, $y = b$, and $z < c$.

¹Emille Davie Lawrence is a mathematician in San Francisco. This quote is from an essay about how her own experience of exclusion in mathematics has shaped her work with students. She is an editor of *Living Proof: Stories of Resilience Along the Mathematical Journey* [68], from which this quote is taken.

Prove that \leq is a partial order. (This is called the **lexicographic order** or **dictionary order** on \mathbb{R}^3 .)

4. Define \sim on \mathbb{R}^2 by declaring $(a, b) \sim (c, d)$ if and only if there exist $k, \ell \in \mathbb{Z}$ such that $(c, d) = (a + k, b + \ell)$. Prove that \sim is an equivalence relation. Also do your best to draw a reasonable picture of the quotient set \mathbb{R}^2/\sim .
5. Define \sim on \mathbb{R}^2 by declaring $(a, b) \sim (c, d)$ if and only if there exist $k, \ell \in \mathbb{Z}$ such that $(c, d) = (a + k, (-1)^k(b + \ell))$. Prove that \sim is an equivalence relation. Also do your best to draw a reasonable picture of the quotient set \mathbb{R}^2/\sim .
6. Define \sim on \mathbb{R} by declaring $x \sim y$ if and only if $x - y \in \mathbb{Q}$. For equivalence classes $[x]$ and $[y]$, define $[x] + [y] = [x + y]$.
 - (a) Prove that \sim is an equivalence relation.
 - (b) Prove that $+$ is well-defined on \mathbb{R}/\sim . That is, assume that $[x] = [x']$ and $[y] = [y']$. Show that $[x] + [y] = [x'] + [y']$.
7. Is it possible to define “modular fractions”? Choose a prime number $p \geq 2$ and let $X = \mathbb{Z}/p\mathbb{Z}$. Define \sim on $X \times (X \setminus \{[0]\})$ by declaring $([a], [b]) \sim ([c], [d])$ if and only if $[a] \cdot [d] = [b] \cdot [d]$. Is \sim an equivalence relation? If so, is addition well defined on the quotient set?
8. Let $(G, \mathbb{1}, \circ)$ be a group and $H \subset G$ a subgroup. Define \sim on G by declaring $x \sim y$ if and only if there exists $h \in H$ with $x = h^{-1} \circ y \circ h$. Prove that \sim is an equivalence relation on G .
9. Let $(G, \mathbb{1}, \circ)$ be a group and $H \subset G$ a subgroup such that $h_1 \circ h_2 = h_2 \circ h_1$ for all $h_1, h_2 \in H$. Define \sim on G by declaring $x \sim y$ if and only if there exists $h \in H$ with $x = h^{-1} \circ h^{-1} \circ y \circ h \circ h$. Prove that \sim is an equivalence relation on G .
10. Recall that \mathbb{Q} is the quotient set for $\mathbb{Z} \times \mathbb{N}$ under the equivalence relation \sim where we define $(a, b) \sim (c, d)$ if and only if $ad = bc$. We write $\frac{a}{b}$ to denote the equivalence class $[(a, b)]$. Define \oplus (called “freshman addition”) on \mathbb{Q} by:

$$\frac{a}{b} \oplus \frac{c}{d} = \frac{a+c}{b+d}.$$
 Is \oplus well-defined? That is, if $\frac{a}{b} = \frac{a'}{b'}$ and $\frac{c}{d} = \frac{c'}{d'}$ is

$$\frac{a}{b} \oplus \frac{c}{d} = \frac{a'}{b'} \oplus \frac{c'}{d'}?$$
11. Suppose that X is a set with a metric d . Let \sim be an equivalence relation on X such that each equivalence class has only finitely many elements. Let $\overline{X} = X/\sim$ be the quotient set. Define \overline{d} on \overline{X} by

$$\overline{d}([x], [y]) = \min \{d(a, b) : a \in [x], b \in [y]\}$$

Prove that \bar{d} satisfies all the axioms of a metric, except possibly, the triangle inequality. Give an example of a specific metric space and equivalence relation such that all equivalence classes are finite, but where \bar{d} does not satisfy the triangle inequality.

12. Here is another example where division on quotient sets is not well-defined, even though multiplication is. (This example is taken from [17].) Let $X = \mathbb{Z} \setminus \{0\}$. For $a, b \in X$, define $a \sim a'$ if and only if either $a = a'$ or $|a| = |a'| \geq 2$. Thus, for example, $(-3) \sim 3$ but $(-1) \not\sim (1)$.

- (a) Prove that \sim is an equivalence relation.
- (b) For $[a], [b] \in X / \sim$, define $[a] \cdot [b] = [ab]$. Prove that this multiplication is well-defined.
- (c) Find an example of classes $[a], [b], [c]$ such that $[a] \cdot [b] = [a] \cdot [c]$ but $[b] \neq [c]$.

13. Given a set X , define an **EQREL** set for X to be a subset $A \subset X \times X$ such that the following hold:

- (ER1) For every $x \in X$, $(x, x) \in A$.
- (ER2) For every $x, y \in X$, if $(x, y) \in A$ then also $(y, x) \in A$.
- (ER3) For every $x, y, z \in X$, if $(x, y) \in A$ and $(y, z) \in A$, then $(x, z) \in A$.

Do the following:

- (a) Show that if A is an **EQREL** set for X , then there exists an equivalence relation \sim_A on X , such that $x \sim_A y$ if and only if $(x, y) \in A$.
- (b) Show that if \sim is an equivalence relation on X , then there is an **EQREL** set A_\sim for X , such that $(x, y) \in A_\sim$ if and only if $x \sim y$.
- (c) Suppose that we start with an **EQREL** set A , create the equivalence relation \sim_A and then, from that equivalence relation create the **EQREL** set A_{\sim_A} . Does this new set equal A ? Why or why not?
- (d) Suppose that we start with an equivalence relation \sim , create the **EQREL** set A_\sim , and then, from that set create the equivalence relation \sim_{A_\sim} . Is it the case that for all $x, y \in X$, we have that $x \sim y$ if and only if $x \sim_{A_\sim} y$? Why or why not?

We conclude that equivalence relations are essentially the same concept as equivalence relations, and thus also essentially the same concept as partitions.

14. Suppose that X is a set and that $B \subset X \times X$. We want to find an equivalence relation on X such that if $(x, y) \in B$ then $x \sim y$. We think of B as telling us the pairs of elements from X that we want to insist are related to each other. Can we expand that list out to ensure that we have an equivalence relation? One way to do so, would simply be to declare that $x \sim y$ for *every*

pair of elements $x, y \in B$. But declaring everything in X to be equivalent is unlikely to be useful. Is there another way? There is! And your challenge is to find it.

Prove that there is a relation \sim on X such that the following hold:

- \sim is an equivalence relation.
- For all $(x, y) \in B$, $x \sim y$.
- If \simeq is another equivalence relation on X such that $x \simeq y$ for all $x, y \in B$, then $a \simeq b$ implies that $a \sim b$ for all $a, b \in X$. In other words, \sim is the smallest equivalence relation on X such that a pair of elements from X are related whenever they are in B .

(Hint: Use **EQREL** sets instead of equivalence relations, but keep in mind that B may not be an **EQREL** set.)

15. (This problem is based on the exposition of chip-firing in [52]. That review lists a number of interesting questions regarding chip firing, but perhaps you can think of your own?) Let G be a graph without loops or multiple edges¹ having vertex set V and edge set E . For a vertex $v \in V$, the **neighbors** of v are those vertices $w \in V$ such that there is an edge $e \in E$ whose endpoints are v and w . The **degree** of a vertex v is the number of neighbors of v . Suppose that at each vertex $v \in V$ we have a number $N(v) \in \mathbb{Z}$ of chips. (If $N(v) < 0$, we think of the vertex v as being in debt.) We call the pair (G, N) a **configuration**. We define the operation of **firing at vertex v** to be the result of decreasing $N(v)$ by $\deg(v)$ and increasing $N(w)$ by 1 for each neighbor w of v . The operation that is inverse to chip firing at v is called **lending at v** . Suppose that (G, N) and (G, N') are configurations. Declare $(G, N) \sim (G, N')$ if and only if there is a sequence of chip firings and lendings that take us from (G, N) to (G, N') .

- (a) Prove that \sim is an equivalence relation. In what follows, let $[(G, N)]$ be the equivalence class of the configuration (G, N) .
- (b) Draw a connected graph G with at least four vertices, no loops, and no multiple edges. Find two configurations (G, N) and (G, M) such that $(G, N) \not\sim (G, M)$ and prove that no sequence of firings and lendings will convert (G, N) into (G, M) .
- (c) Suppose that G is a graph with no loops and no multiple edges. If (G, N) and (G, M) are configurations, let $(G, N + M)$ be the configuration where $N + M(v) = N(v) + M(v)$ for each vertex v . Define addition on equivalence classes by

$$[(G, N)] + [(G, M)] = [(G, N + M)].$$

Prove that this is well-defined.

¹That is, for each pair of distinct vertices v and w there is at most one edge with endpoints at v and w .

8 | Functions

Key Terms

- definition of a function and inverse function
- domain, codomain, range, graph of a function
- identity, constant, and coordinate functions
- function composition
- finite and infinite sequence
- injective, surjective, bijective function
- inverse function

“It is not necessary that y be subject to the same rule as regards x throughout the interval. Indeed one need not even be able to express the relationship through mathematical operations ... It doesn’t matter if one thinks of this [correspondence] so that different parts are given by different laws or designates it [the correspondence] entirely lawlessly.”

– Lejeune Dirichlet²

²Dirichlet (1805-1859) made important contributions to both number theory and analysis. I found this quotation in [36].

8.1 The definition of a function

"In searching out this matter, I found it by no means clearly laid down what is meant by the *solution of a differential equation*: and, on looking further, I found some degree of ambiguity attaching to the word *equation* itself."

-Augustus De Morgan¹

On the question, What is the Solution of a Differential Equation?

If X and Y are sets, a function $f: X \rightarrow Y$ is a way of transforming the elements of X into elements of Y . Beginning Calculus courses study functions $f: \mathbb{R} \rightarrow \mathbb{R}$, what it means to graph such functions, and how to determine if they are continuous or differentiable. More advanced Calculus classes study differentiable functions $f: \mathbb{R}^2 \rightarrow \mathbb{R}$ and $f: \mathbb{R}^3 \rightarrow \mathbb{R}$ (and perhaps other types of functions). Linear Algebra classes study *linear* functions $f: \mathbb{R}^n \rightarrow \mathbb{R}^m$. In this text, we study functions in complete generality. The key concepts from this section are used throughout pure and applied mathematics. In Chapter 6 we gave a formal definition of "function" in terms of sets. For most purposes, however, that formal definition is unnecessary and maybe even more of a hinderance than a help. In what follows, we give a slightly informal definition of function in terms of predicates and then explore ways of visualizing functions, their properties, and their applications. For particular types of functions, such as continuous functions, there are an enormous number of applications and we cannot possibly do justice to any of them.

8.1.1

Definition ▶ Function

Let X and Y be sets. A **function** $f: X \rightarrow Y$ is a rule¹ assigning an element $x \in X$ to an element $f(x) \in Y$ such the following conditions hold:

- (The domain condition) For each $x \in X$, there exists a $y \in Y$ such that $y = f(x)$.
- (The well-defined condition) If $a, b \in X$ and $a = b$, then $f(a) = f(b)$.

The set X is called the **domain** of f , the set Y is called the **codomain** of f , and the set

$$\text{range}(f) = \{y \in Y : \exists x \in X \text{ such that } y = f(x)\}$$

is called the **range** or **image** of f . The range of $f: X \rightarrow Y$ is also denoted (somewhat misleadingly) as $f(X)$. Two functions $f: X \rightarrow Y$ and $g: A \rightarrow B$ are **equal** if and only if $A = X$, $B = Y$, and $f(x) = g(x)$ for all $x \in X$.

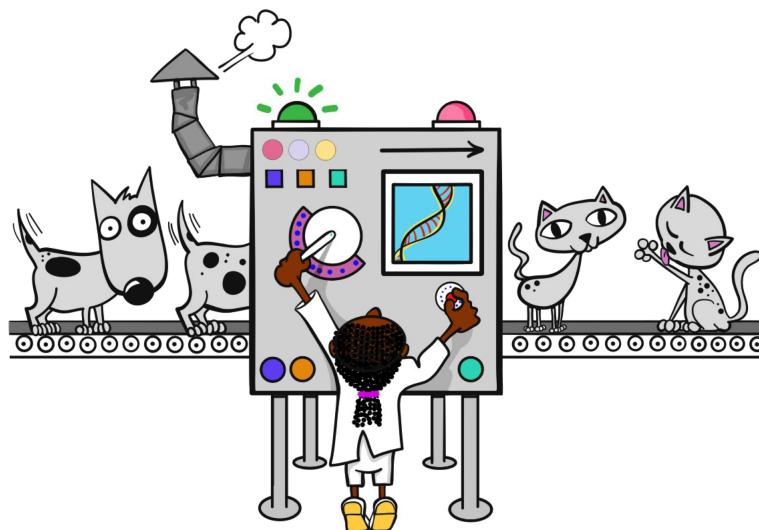
8.1.2

¹Augustus De Morgan (1806 - 1871) was responsible for giving a precise formulation of Mathematical Induction and made great strides toward putting mathematics on a firm logical foundation.

²More precisely, a predicate in two free variables $x \in X$ and $y \in Y$.

In Definition 8.1.1, we could combine the domain and well-defined conditions into the single requirement that for each $x \in X$ there exists a *unique* $y \in Y$ with $y = f(x)$. The way we have stated the definition, however, is a better guide for constructing proofs involving functions.

One popular metaphor is that a function is a machine for converting inputs to outputs. The domain is the set of all potential inputs to f . The domain condition requires that all potential inputs are indeed valid inputs. The codomain of f is the set of all potential outputs from f . The range of f is the set of actual outputs of f . The definition of function does not require that all possible outputs are actual outputs. A function for which the codomain equals the range is said to be “surjective” or “onto.” We’ll talk more about such functions later.



The well-defined condition ensures that putting the same input into the machine will always result in the same output. The well-defined condition is the basis for elementary algebra. For instance, since the function $f: \mathbb{R} \rightarrow \mathbb{R}$ defined by $f(x) = x^2$ is well defined, we can square both sides of any true equation and still have a true equation. (For example, if $x-3 = y+5$, then $(x-3)^2 = (y+5)^2$. The relation $f: [0, \infty) \rightarrow \mathbb{R}$ defined by $f(x) = \pm\sqrt{x}$ is not well-defined, since $-\sqrt{4} \neq +\sqrt{4}$. We will elaborate more on the notion of well-defined in what follows.

8.1.3 Example

Define $f: \mathbb{R} \rightarrow \mathbb{R}$ by $f(x) = 1/x$. Then f is not a function, since the domain condition is not satisfied. The number $f(0)$ is not defined, but 0 is an element of the domain. For $f: X \rightarrow Y$ to be a function it must be the case that $f(x)$ is defined for every $x \in X$. If, on the other hand, we define $f: \mathbb{R} \rightarrow \mathbb{R}$ by

$$f(x) = \begin{cases} 1/x & \text{if } x \neq 0 \\ 5 & \text{if } x = 0 \end{cases}$$

for every $x \in \mathbb{R}$, we do have a function. The range of f is $\mathbb{R} \setminus \{0\}$, since for each $y \in \mathbb{R} \setminus \{0\}$, if we set $x = 1/y$, we have $f(x) = y$. The codomain, on the other hand, is \mathbb{R} since that is what we specified when we initially wrote $f: \mathbb{R} \rightarrow \mathbb{R}$.

Risking possible confusion, once a function $f: X \rightarrow Y$ has been specified, we will often refer to $f: X \rightarrow Y$ using only the symbol f . Also, if f is understood from context, the notation $x \mapsto y$ means the same thing as $y = f(x)$. For example, if $f: \mathbb{R} \rightarrow \mathbb{R}$ is the function defined by $f(x) = x^2$ for all $x \in \mathbb{R}$, then $3 \mapsto 9$.

8.1.4 Example

Here are some examples of functions $f: \{1, 2, 3\} \rightarrow \{a, b, c, d\}$. Each definition is formatted in a slightly different way, for the sake of variety.

1. Define $f: \{1, 2, 3\} \rightarrow \{a, b, c, d\}$ by:

$$\begin{aligned} f(1) &= a \\ f(2) &= b \\ f(3) &= c \end{aligned}$$

2. Define $f: \{1, 2, 3\} \rightarrow \{a, b, c, d\}$ by $f(x) = b$ for all $x \in \{1, 2, 3\}$.

3. Define $f: \{1, 2, 3\} \rightarrow \{a, b, c, d\}$ by:

$$f(x) = \begin{cases} a & \text{if } x = 1 \\ b & \text{if } x = 2 \\ c & \text{if } x = 3 \end{cases}$$

8.1.5 Exercise

Find 3 more examples of functions $f: \{1, 2, 3\} \rightarrow \{a, b, c, d\}$. Use whatever method of formatting you prefer.

As in Calculus classes, we can sometimes specify a function by giving a formula.

8.1.6 Example

1. Define $f: \mathbb{R} \rightarrow \mathbb{R}$ by letting

$$f(x) = x^2 - 2x + 1$$

for all $x \in \mathbb{R}$.

2. Define $g: \mathbb{R}^2 \rightarrow \mathbb{R}$ by letting

$$g((x, y)) = x^2 y$$

for all $(x, y) \in \mathbb{R}^2$.

Then both f and g are functions.

When the domain of a function is a set of ordered pairs, the nested parentheses in the definition of a function can be difficult to read, so we will often drop the outer set of parentheses. Thus, in Part (2.) of Example 8.1.6 we would write $g(x, y) = x^2 y$ instead of $g((x, y)) = x^2 y$. If we do keep both pairs of parentheses, we will often write the outer pair slightly larger to aid readability. This is not, however, necessary.

8.1.7 Example

Define $f: \mathbb{Z} \rightarrow \mathbb{N}$ by letting

$$f(n) = n^2 + 1$$

for all $n \in \mathbb{Z}$.

Observe that since we specified that the domain of f is \mathbb{Z} , the value $f(1/2)$ is undefined, even though it makes sense to plug $1/2$ in for n in the formula $n^2 + 1$.

The next example shows that we can define functions without writing down a formula.

8.1.8 Example ▶ (Stereographic Projection)

Let S^2 be the unit sphere in \mathbb{R}^3 . That is,

$$S^2 = \{(x, y, z) \in \mathbb{R}^3 : x^2 + y^2 + z^2 = 1\}.$$

Let $\mathbf{N} = (0, 0, 1)$ be the north pole. Define a function (called **stereographic projection**) $\sigma: S^2 \setminus \{\mathbf{N}\} \rightarrow \mathbb{R}^2$ as follows. For $\mathbf{x} \in S^2$, draw the line passing through \mathbf{N} and \mathbf{x} . This line intersects the plane with equation $z = -1$ at some point $(a, b, -1)$. Let $\sigma(\mathbf{x}) = (a, b)$. See Figure 8.1. Stereographic projection is often used to make maps of the polar regions of Earth and its moon.

We will also often specify functions piecewise. What matters is that we specify a unique $f(x)$ for every element x of the domain.

8.1.9 Example

Define $f: \mathbb{N} \rightarrow \mathbb{N}$ by letting

$$f(n) = \begin{cases} n/2 & \text{if } n \text{ is even} \\ 3n - 1 & \text{if } n \text{ is odd.} \end{cases}$$

8.1.10 In the remainder of the text, you will often be required to define various kinds of functions. The previous examples give you some models for how to do that,

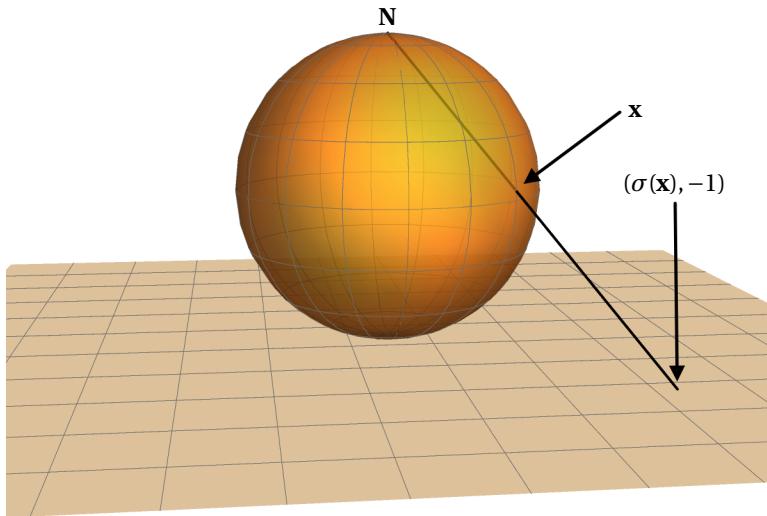


Figure 8.1: Defining stereographic projection by drawing a line passing through the north pole of the sphere and a given point in $S^2 \setminus \{N\}$.

but here is a summary. Observe how it is modelled on the general structure for existence proofs.

CONSTRUCTION OF A FUNCTION

To construct: A function $f: X \rightarrow Y$.

Structure of Proof: For each $x \in X$, define

$$f(x) = \langle \text{formula or description saying what } f(x) \text{ is} \rangle$$

To verify that $f: X \rightarrow Y$ is a function we show:

1. (domain condition) That $f(x)$ exists and that $f(x) \in Y$ for every $x \in X$.
2. (well-defined condition) That, for all $a, b \in X$, if $a = b$, then $f(a) = f(b)$.

(Prove all of the previous statements unless completely obvious.)

The structure suggested by the outline above involves defining a function by saying what it does to each element $x \in X$. In more abstract settings, the definition of $f(x)$, for a particular x , may not be given by a formula the way most functions in Calculus are. What matters is that you have specified exactly what $f(x)$ is for each $x \in X$: this can also be done by writing sentences or by using previously constructed functions. Also, in many cases the well-defined condition is actually obvious. However, we will see examples where it is important. Typically you only need to worry about this step if the elements of X can be represented in more than one way *and* the definition of f depends on a particular representation. We will elaborate on this in Section 8.6.

Since, for given sets X and Y , there are usually many different functions $f: X \rightarrow Y$, we usually do not simply have to show the existence of a function $f: X \rightarrow Y$. Instead, we usually have to show that there exists a function $f: X \rightarrow Y$ having some particular property (for instance an *injective* function, or a *continuous* function, etc.). To complete such a task we follow the Proof Structure above, but then also have to prove that the function we've defined has the particular property that we claim it has.

Finally, we recall from our definition that two functions $f: X \rightarrow Y$ and $g: A \rightarrow B$ are equal if and only if they have the same domain (i.e. $X = A$), the same codomain (i.e. $Y = B$), and take the same value at every element of the domain (i.e. for every $x \in X$, $f(x) = g(x)$.)

8.1.12 Example

Let $S^1 = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$ be the unit circle and let $\text{id}: S^1 \rightarrow S^1$ be the function defined by $\text{id}(z) = z$ for all $z \in S^1$. (The function id is called the **identity function** on S^1 .) Let $R: S^1 \rightarrow S^1$ be a rotation by 2π radians.

Observe that $\text{id}(z) = R(z)$ for every $z \in S^1$. Since id and R have the same domain, the same codomain, and the same effect on every point z of S^1 , the function id equals the function R . The functions are equal, even though applying id seems to mean that we don't move the circle at all and applying R seems to mean rotating the circle a full revolution. The definition of a function does not take into account how much work we put into doing the function - only what the domain, codomain, and end result are².

Here is a classic result concerning the geometry of \mathbb{R} . Recall that the distance between real numbers a and b is defined to be:

$$d(a, b) = |a - b| = \sqrt{(a - b)^2}$$

The point of the theorem is to show that if a function $T: \mathbb{R} \rightarrow \mathbb{R}$ preserves distance and doesn't move either 0 or 1, then T is equal to the identity function $\text{id}: \mathbb{R} \rightarrow \mathbb{R}$ defined by $\text{id}(x) = x$ for all $x \in \mathbb{R}$.

8.1.13 Theorem

Suppose that $T: \mathbb{R} \rightarrow \mathbb{R}$ is a function with the following properties:

1. for all $a, b \in \mathbb{R}$, $d(a, b) = d(T(a), T(b))$,
2. $T(0) = 0$,
3. $T(1) = 1$,

then $T = \text{id}$.

¹Maybe this is like academic work - your grade ostensibly depends only on the quality of the work you turn in and not on how much effort it took to complete it!

Proof. Assume that $T: \mathbb{R} \rightarrow \mathbb{R}$ is a function which is distance preserving and that $T(0) = 0$ and $T(1) = 1$. We will show that $T = \text{id}$. To do this, we must show that T and id have the same domain and codomain and that for all $x \in \mathbb{R}$, $T(x) = x$. Since, according to their definitions, T and id have the same domain and codomain, we need only show that $T(x) = \text{id}(x)$ for every $x \in \mathbb{R}$. Let $x \in \mathbb{R}$ be arbitrary. Recall that $\text{id}(x) = x$, so we need to show that $T(x) = x$. We may use the three given properties of T .

Claim 1: Either $T(x) = x$ or $T(x) = -x$.

(Prove the claim.)

Claim 2: Either $1 - T(x) = 1 - x$ or $1 - T(x) = x - 1$.

(Prove the claim.)

Claim 3: $T(x) = x$.

(Prove the claim using Claims 1 and 2.)

Since $T(x) = \text{id}(x)$ for every $x \in \mathbb{R}$ and since T and id have the same domain and codomain, $T = \text{id}$. □

8.2 Visualizing Functions

“Assessments of change, dynamics, and cause and effect are at the heart of thinking and representation. To understand is to know *what cause provokes what effect, by what means, at what rate*. How then is such knowledge to be represented?”

– Edward R. Tufte, *Visual Explanations* [125]

Graphs of functions

Most of us, as a result of our previous mathematical training, when confronted with the definition of a function will immediately try to graph it. In beginning Calculus courses, graphs are an incredibly useful tool for building our intuition for how limits, derivatives, and integrals work. In other mathematical situations, graphs are less useful. Nevertheless, even in our abstract setting, we can define the graph¹ of a function, even if we aren’t always able to use it.

8.2.1

Definition ► Graph of a function

If $f: X \rightarrow Y$ is a function, we define

$$\text{graph}(f) = \{(x, y) \in X \times Y : y = f(x)\}$$

to be the **graph**¹ of the function f .

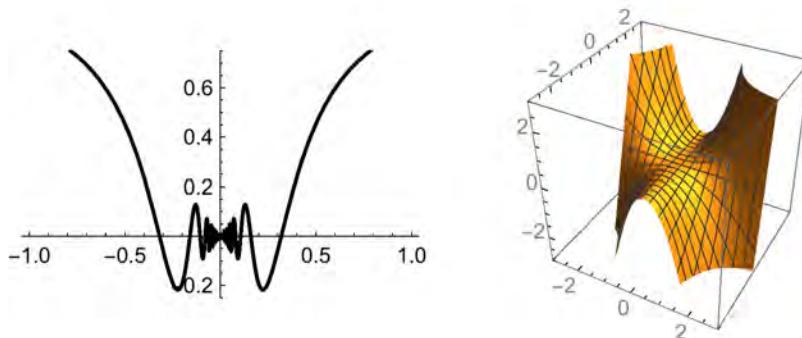


Figure 8.2: Graphs of the functions $f(x) = x \sin(1/x)$ and $g(x) = x^2 y$.

¹Don’t confuse this with a graph consisting of vertices and edges!

²If you studied Chapter 6, you’ll recognize that in the world of axiomatic set theory, the graph of a function is actually exactly the same as the function itself.

8.2.2

Example ▶ (Graphing)

If $X \subset \mathbb{R}$ and if $f: X \rightarrow \mathbb{R}$ is given by a relatively “nice” formula, we can plot each point of $\text{graph}(f) \subset \mathbb{R}^2$ (i.e. plot the graph of f). For example, the left of Figure 8.2 shows part of the graph of the function $f: \mathbb{R} \setminus \{0\} \rightarrow \mathbb{R}$ defined by $f(x) = x \sin(1/x)$. As can be seen from this example, even for functions given by simple formulas, the graph can be difficult to use.

Similarly, if $f: \mathbb{R}^2 \rightarrow \mathbb{R}$ is a function given by a “nice” formula then (after identifying $\mathbb{R}^2 \times \mathbb{R}$ with \mathbb{R}^3) we can draw the graph of f , as on the right of Figure 8.2, where the function given by $g(x, y) = x^2 y$ is pictured.

To see why the graph of a function is only rarely useful, observe that if $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ is a function, then $\text{graph}(f) \subset \mathbb{R}^2 \times \mathbb{R}^2$, which is a 4-dimensional space! Thus, even when the domain and the codomain are the easily visualized set \mathbb{R}^2 , $\text{graph}(f)$ is difficult (maybe even impossible!) to visualize. If X and Y are sets which themselves aren’t easy to visualize (for example, \mathbb{R}^{1000}), then $\text{graph}(f)$ is even less useful as a way of visualizing the graph. Truthfully, even in the case when we have a function $f: \mathbb{R} \rightarrow \mathbb{R}$, the graph may not be very useful.

8.2.3

Exercise

Define $f: \mathbb{R} \rightarrow \mathbb{R}$ by declaring, for all $x \in \mathbb{R}$,

$$f(x) = \begin{cases} 1/q & x = p/q \text{ where } q \in \mathbb{N}, p \in \mathbb{Z} \text{ and } p/q \text{ is in lowest terms.} \\ 0 & x \notin \mathbb{Q}. \end{cases}$$

Do your best to draw $\text{graph}(f)$.

Each branch of mathematics has its own ways of visualizing the functions relevant to that branch. In what follows, we will explore just a few examples of how different types of functions may be visualized. We should keep in mind, however, that there is no one way to visualize a given function $f: X \rightarrow Y$ and for “most” functions there is either no best way to visualize it or no way to usefully visualize the function at all.

Venn Diagrams

We can sometimes visualize functions similarly to how we visualize sets using Venn diagrams as in Figure 8.3. These schematics are very useful for thinking about the relationship between the domain and codomain of a function or the relationship between different functions.

Dots and arrows

If X and Y are (small) finite sets, we can draw a dot for each element of X and Y and draw arrows from each $x \in X$ to the corresponding $f(x) \in Y$. For example,

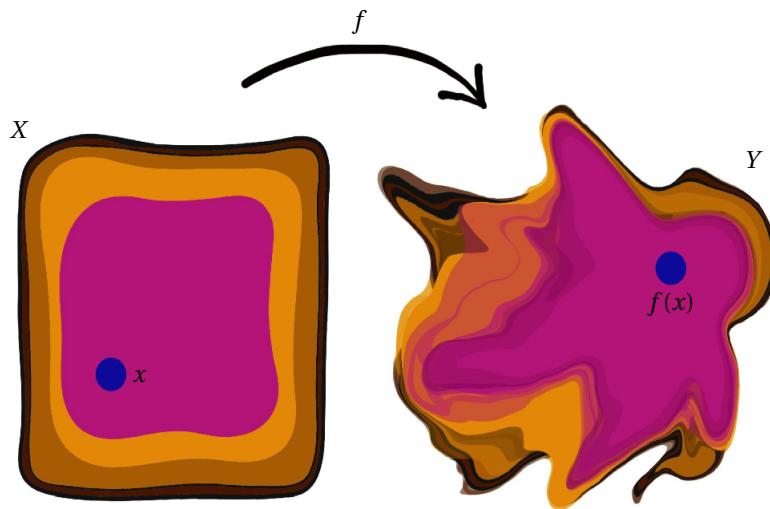
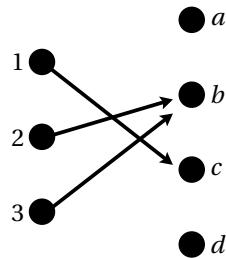
Figure 8.3: A schematic depiction of a function $f: X \rightarrow Y$ 

Figure 8.4: A function with finite domain and codomain.

the function $f: \{1, 2, 3\} \rightarrow \{a, b, c, d\}$ defined by $f(1) = c$ and $f(2) = f(3) = b$, can be visualized as in Figure 8.4.

Labels and lightbulbs

Suppose that $f: X \rightarrow Y$ is a function. By the definition of function, this means that every $x \in X$ is assigned to a $y \in Y$. We can think about the elements of Y as labels on the elements of X . Here are some examples.

8.2.4 Example

Let $G = (V, E)$ be the graph pictured on both the left and right of Figure 8.5. A function $f: V \rightarrow \mathbb{R}$ can be thought of as a way of labelling where a vertex v is given the label $f(v)$, which is a real number. The left side of the figure depicts just such a function $f: V \rightarrow \mathbb{N}$. The right side depicts a function $g: E \rightarrow \mathbb{R}$ by thinking of real numbers as labels on edges.

8.2.5

Example

Let $S = [-1, 1] \times [-1, 1]$ be a solid square in \mathbb{R}^2 and consider a function $f: S \rightarrow \{0, 1\}$. To visualize f we could, in principle, label each point of S with either a 0 or a 1. This however would result in something completely unreadable. Instead, we can think of each point of S as a light bulb. We associate the number 0 with the bulb being off (or black) and the number 1 with the bulb being on (or white). Figure 8.6 depicts the function $f: S \rightarrow \{0, 1\}$ which is defined by $f(x, y) = 0$ if and only if $(\sin(2\pi x) + \cos(2\pi y))^2 > 1$.

It is also possible to visualize a function $f: X \rightarrow Y$, by labelling each element $y \in Y$ with those elements $x \in X$ such that $f(x) = y$. This is typically much less useful than labelling the elements of X with the corresponding element of y as not every element $y \in Y$ may have an associated element $x \in X$ and there may be elements $y \in Y$ such that there is more than one element $x \in X$ with $f(x) = y$. That is, if we label the elements of Y , some elements of Y might have no labels and some might have more than one label. Figure 8.9 uses this method to depict a function with domain $\{1, \dots, 24\}$ and codomain \mathbb{R}^2 .

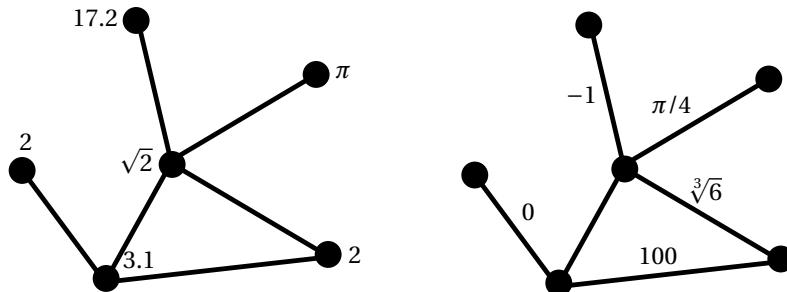


Figure 8.5: Both the left and right show a graph $G = (V, E)$. The left depicts a function $f: V \rightarrow \mathbb{R}$; the right depicts a function $g: E \rightarrow \mathbb{R}$.

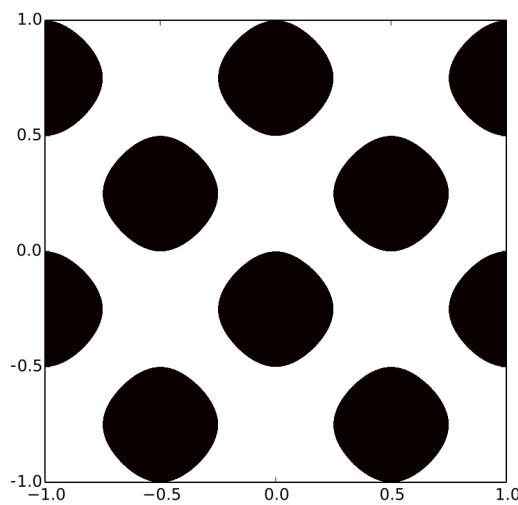


Figure 8.6: A depiction of a particular function $f: [-1, 1] \times [-1, 1] \rightarrow \{0, 1\}$.

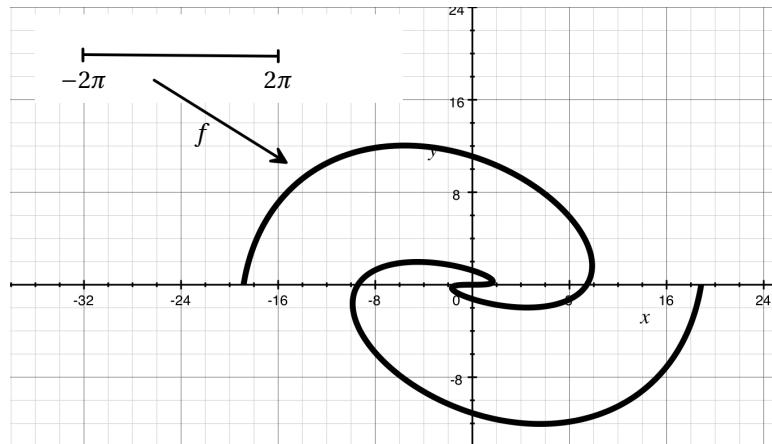


Figure 8.7: A depiction of a particular function $f: [-2\pi, 2\pi] \rightarrow \mathbb{R}^2$.

Transformations

In some cases, the domain X and codomain Y of a function $f: X \rightarrow Y$ can be easily visualized even when the graph of f cannot be. In this case, we think of f as a transformation and draw “before” and “after” pictures of the effect of f on a representative subset of X .

For example, if $f: [-2\pi, 2\pi] \rightarrow \mathbb{R}^2$ is the function defined by $f(t) = (3t \cos(t), t^2 \sin(t)/2)$ for all $t \in [-2\pi, 2\pi]$, we can draw, as in Figure 8.7, the before picture as the line segment extending from -2π to 2π and the after picture as the set of points \mathbb{R}^2 which are in the range of f .

As another example, if we define $g: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ by defined by

$$g(x, y) = (1.5x, (x^2 + 0.5)y)$$

for all $(x, y) \in \mathbb{R}^2$. we can get a sense for what g does by drawing its effect on either a circle or a grid of lines, as in Figure 8.8

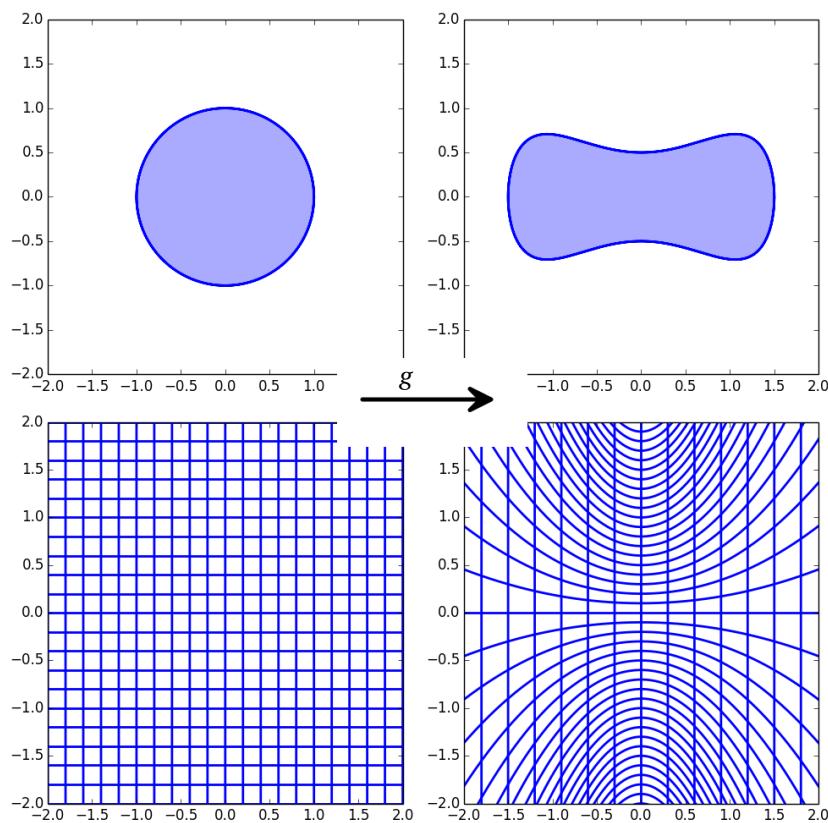


Figure 8.8: Two ways of visualizing the effect of a particular function $g: \mathbb{R}^2 \rightarrow \mathbb{R}^2$. The top row shows what g does to the unit disc; the bottom row shows what f does to a grid of lines.

8.3 Important Functions

“There is no passion like that of a functionary for his function.”
– attributed to Georges Clemenceau¹

We now turn to some of the most important and fundamental examples of functions.

Identity Functions

We have already seen identity functions in a few examples. Here is a general definition.

8.3.1 Definition ► Identity Function

For a set X , the **identity function** on X is the function $f: X \rightarrow X$ defined by $f(x) = x$ for all $x \in X$. We will sometimes denote the identity function on X by id_X .

Constant Functions

Constant functions aren't very interesting, but they are certainly useful and they almost always exist.

8.3.2 Definition ► Constant Function

Suppose that X and Y are sets. A function $f: X \rightarrow Y$ is a **constant function** if there exists $y_0 \in Y$ such that for all $x \in X$, $f(x) = y_0$.

8.3.3 Exercise

Prove that if X and Y are sets with Y non-empty, then there exists a constant function $f: X \rightarrow Y$. In particular, if $Y \neq \emptyset$, then there exists a function $f: X \rightarrow Y$.

Coordinate functions

Suppose that X and Y are sets. From the definition of the Cartesian product $X \times Y$, we know that if $a \in X \times Y$, there exist $x \in X$ and $y \in Y$ such that $a = (x, y)$. We can turn this observation into a pair of functions.

¹It is very difficult to find a source for this quote.

8.3.4

Definition ► Coordinate Functions

Suppose that X and Y are sets. Then the functions

$$\begin{aligned} p_X &: X \times Y \rightarrow X \\ p_Y &: X \times Y \rightarrow Y \end{aligned}$$

defined by $p_X(x, y) = x$ and $p_Y(x, y) = y$ for all $(x, y) \in X \times Y$ are called the **coordinate functions** of $X \times Y$.

Sequences

As a final example, we introduce sequences. These will play an important role in this book; indeed we have already used them implicitly several times. We will explore their properties more fully in Chapter 11.

8.3.5

Definition ► Sequences

Suppose that X is a set. An **infinite sequence** in X is a function $s: \mathbb{N} \rightarrow X$. A **finite sequence** in X is a function $s: \{1, \dots, n\} \rightarrow X$ for some $n \in \mathbb{N}$. If s is a sequence (finite or infinite) in X we will often write s_n in place of $s(n)$. Since sequences are completely defined by their terms, if we know the terms s_n of a sequence, we will often dispense with assigning another name (for example s) to the sequence and simply call the sequence (s_n) . The word **sequence** will, in this book, always mean an infinite sequence.

8.3.6

Example

Let $s: \mathbb{N} \rightarrow \mathbb{R}$ be defined by $s(n) = \sqrt{n}$. Then $s_1 = 1$, $s_2 = \sqrt{2}$, $s_3 = \sqrt{3}$, $s_4 = 2$, etc and $s = (s_n)$ is an example of a sequence in \mathbb{R} .

8.3.7

Example

The sequence $(1/n)$ in \mathbb{R} has terms:

$$1, 1/2, 1/3, 1/4, 1/5, \dots$$

8.3.8

Many mathematicians adopt the convention the domain of a sequence is $\mathbb{N}^* = \mathbb{N} \cup \{0\}$ rather than just \mathbb{N} . Upon occasion in this text we will also have occasion to consider the initial term of a sequence (x_n) to be x_0 . If needed, we can indicate the starting and ending term of a sequence using superscripts and subscripts:

$$(x_k)_{k=0}^n = x_0, x_1, \dots, x_n.$$

We can sometimes visualize sequences by numbering the points in the range of the sequence, as in Figure 8.9, which depicts a sequence $(x_k)_{k=1}^{24}$. Observe that in the figure, some points (namely x_{15} and x_{20}) of \mathbb{R}^2 are given more than one label. This is because this particular function $x: \{1, \dots, 24\} \rightarrow \mathbb{R}^2$ happens to have the property that $x(15) = x(20)$.

8.3.9

Warning

If (x_k) is a sequence in a set X , we must maintain a distinction between a term x_k of the sequence (this is an element of X), the location of the term in the sequence (the index k), and the sequence itself (denoted (x_k)).

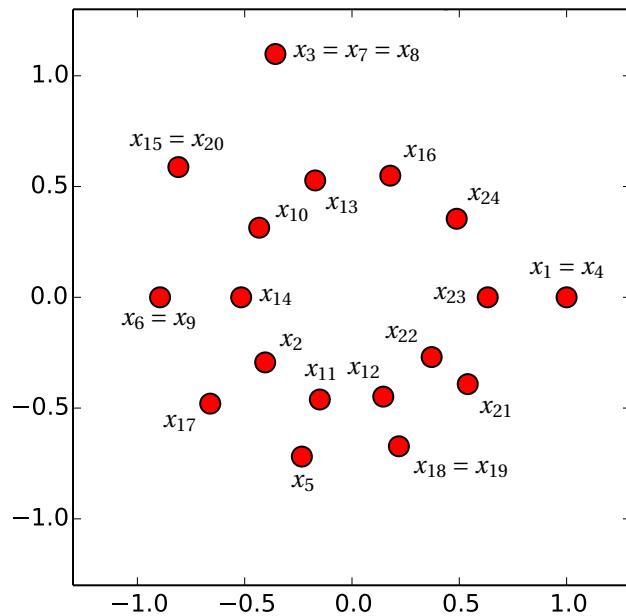


Figure 8.9: A finite sequence $(x_k)_{k=1}^{24}$ in \mathbb{R}^2

8.4 Extended examples

“No one can be convinced by a proof which is not understood, and to learn up a mathematical proof which has not convinced us adds nothing to our knowledge of mathematics. Indeed, no teacher will be satisfied with imparting a chain of formulae connected by formal operations as constituting a mathematical proof, and no student of mathematics should be satisfied with memorizing such sequences.”
–Michael Polanyi¹

Before proceeding with our study of functions, we consider two extended examples of sequences. The first concerns particular types of sequences in graphs and the second sequences in a circle. The first helps us see how we may visualize a sequence as a way of moving around in a space and the second helps us see how we may visualize a sequence as the result of repetitively applying a transformation.

Paths in graphs

Finite sequences (in this case, functions with domain $\{0, \dots, n\}$ for some n) play an especially important role in graph theory as they give us a way of discussing paths in graphs. In this section, we introduce the terminology and discuss what it means for a graph to be connected. In future sections we will explore this idea more. We begin with an example.

8.4.1

Example

Consider Figure 8.10. The arrows along the edges of the graph give a way of moving along edges through the graph from vertex a to vertex b . To specify our route, we can list all the vertices we pass through:

$$a, v_1, v_2, v_3, v_4, v_5, b$$

The vertex v_3 is the same as the vertex v_5 , so there are vertices that appear more than once in the list.

8.4.2

Definition ▶ Paths in Graphs

Suppose that $G = (V, E)$ is a graph such that there is at most one edge between any two vertices. A **path** in G is a finite sequence

$$\alpha = v_0, v_1, \dots, v_n$$

for some $n \in \mathbb{N}^*$ such that the following conditions hold:

¹Michael Polanyi (1891-1976) was a chemist and philosopher of science. This quote is part of Polanyi's larger analysis of what is meant by mathematical proof. He argues that a “*tacit understanding*” is a necessary component. To understand or create a proof, it is necessary to “*inhabit*” the mathematical ideas. [102]

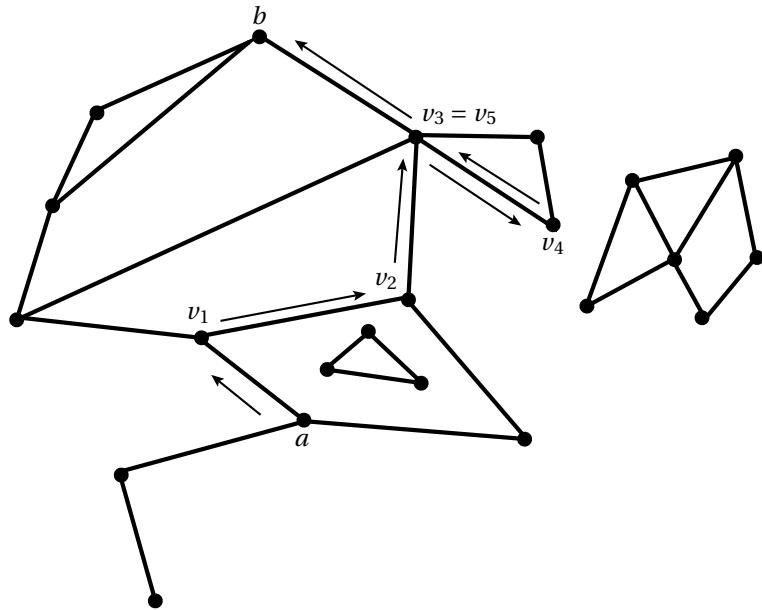


Figure 8.10: The finite sequence $a, v_1, v_2, v_3, v_4, v_5, b$ is a path from a to b of length 6.

8.4.2

- Each v_i (for $i \in \{0, \dots, n\}$) is a vertex of G .
- For all $i \in \{0, \dots, n - 1\}$, the vertices v_i and v_{i+1} are the endpoints of an edge in G .

The number n is the **length** of α . If e is an edge of G such that there exists $i \in \{0, \dots, n - 1\}$ with the endpoints of e equal to v_i and v_{i+1} , then we say that e is **traversed** by α . If a and b are vertices of G such that $v_0 = a$ and $v_n = b$, we say that α is a path **from** a **to** b . If $v_n = v_0$, we say that α is **closed**. See Figure 8.10 for an example.

8.4.3

Warning

Be sure to take the time to see how the picture of a path relates to the formal definition of a path. What aspects of the formal definition does the picture capture? What aspects doesn't it capture? Can you draw a different picture that captures those aspects missing from Figure 8.10?

8.4.4

Theorem

Let $G = (V, E)$ be a graph. Define a relation \sim on V by declaring $a \sim b$ if and only if there is a path from a to b . Then \sim is an equivalence relation on V .

By Theorem 7.5.1, the equivalence classes of V under \sim are a partition of V . Suppose that $v \in V$ and that $[v] = \{w \in V : v \sim w\}$ is its equivalence class. The set $[v]$ consists of all the vertices of G such that there is a path in G from v to that vertex. We can form a new graph by taking the vertex set to be $[v]$ and the edge set to be

all those edges in E such that both endpoints of the edge lie in $[v]$. The graph we get is called a **connected component** of G . A non-empty graph G is **connected** if it has exactly one connected component. A graph is **disconnected** if it is not connected.

8.4.5 Exercise

What are the connected components of the graph in Figure 8.10?

Here is another characterization of what it means for a graph to be connected.

8.4.6 Theorem

A non-empty graph G is connected if for any two vertices v and w , there is a path in G from v to w .

If e is an edge of a graph $G = (V, E)$, we let $G \setminus e$ denote the graph $(V, E \setminus \{e\})$ obtained by removing the edge e from G , but leaving its endpoints. This is an example of “abuse of notation” since, technically, e is not a subset of G and so we shouldn’t write $G \setminus e$. See Figure 8.11.

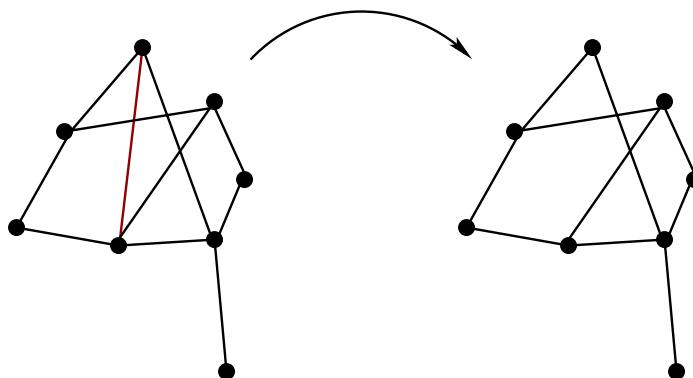


Figure 8.11: Removing the red edge from the graph on the left produces the graph on the right.

We conclude with two challenging theorems for you to prove. You may use the following fact, which is a consequence of the Well-Ordering Principle (Theorem 9.3.1).

Fact: If G is a graph and there is a path in G from a vertex a to a vertex b , then there is a shortest path from a to b . That is, there exists a path α in G from a to b such that if β is *any* path in G from a to b then the length of β is at least the length of α .

The fact should seem plausible since path lengths are always non-negative integers and if there were always a shorter path than whatever path we considered, eventually we’d be considering a path with negative length, which is impossible. We can prove it when it appears subsequently as Theorem 9.3.10 below. Use this fact to prove the following important results from graph theory. The main point is to show that taking an edge away from a connected graph results in a graph

with at most two connected components.

8.4.7

Theorem

Suppose that G is a connected graph.

1. Suppose $\alpha = v_0, v_1, \dots, v_n$ is a shortest path in G from a to b . If $v_i = v_j$ then $i = j$. (That is, α has no repeated vertices.)
2. Suppose that e is an edge of G and that $\text{ENDS}(e) = \{v, w\}$. Let a be any vertex of G . Let α be a path in G from a to either v or w such that no path in G from a to either v or w is shorter. Then α does not traverse e . That is, letting $\alpha = v_0, v_1, \dots, v_n$, there does not exist $i \in \{0, \dots, n-1\}$ such that $\{v_i, v_{i+1}\} = \{v, w\}$.
3. Suppose that e is an edge of G . Then $G \setminus e$ has at most two connected components.

A **cycle** in a graph G is a closed path of positive length such that no edge of G is traversed more than once. A non-empty connected graph without a cycle is called a **tree**. Trees are important tools for organizing information throughout mathematics and computer science. The next theorem gives a characterization of trees. Its contrapositive shows that a nonempty connected graph G is a tree if and only if every edge separates G into two pieces.

8.4.8

Theorem

Let $G = (V, E)$ be a nonempty connected graph. Then there exists a cycle in G if and only if there exists an edge e in G such that $G \setminus e$ is connected.

Rotations of a circle

In this subsection, we consider an extended example of a sequence in the unit circle $S^1 = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$. We will explore other aspects of this example in Section 11.5.

Choose some angle $\theta \in \mathbb{R}$ and let $x_0 = (1, 0) \in \mathbb{R}^2$. Create a sequence, by declaring, for each $n \in \mathbb{N}$, the point $x_n \in S^1$ to be the point obtained by rotating x_0 counter-clockwise by an angle of $n\theta$. See Figure 8.12.

Changing the angle θ or changing the initial point x_0 will give us a different sequence in S^1 . Typically, it is much more interesting to think about the effect of θ on the sequence than the effect of initial point, since two sequences given by the same angle but different initial points can be obtained from each other by applying a rotation of the circle.

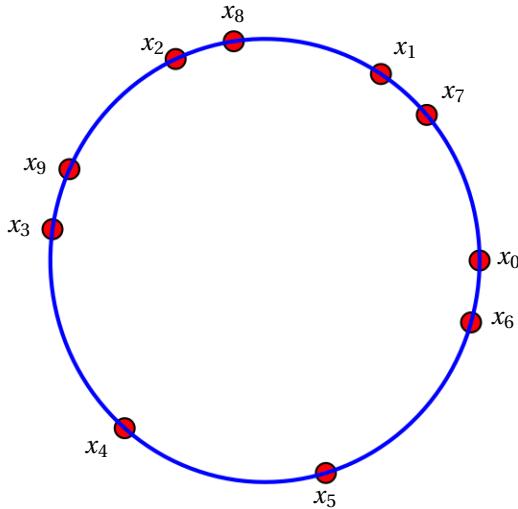


Figure 8.12: The first nine points x_1, \dots, x_9 of a sequence in the unit circle, together with the point x_0 .

8.4.9

Exercise

1. Find all angles $\theta \in \mathbb{R}$ such that (x_n) is a constant sequence.
2. Find an angle θ such that the sequence (x_n) has exactly four distinct terms.

Considering the effect of θ on raises some questions:

1. Is there an angle θ for which the sequence (x_n) is periodic (that is, there is some $N \in \mathbb{N}$ such that for all $m \in \mathbb{N}$, $x_{N+m} = x_m$)? What can you say about such angles?
2. Is there an angle θ for which the sequence (x_n) has no repetitions?
3. Is there an angle θ for which the sequence (x_n) contains every point on the unit circle? (i.e. Is there an angle such that $\text{range}(x_n) = S^1$?)
4. Is there an angle θ for which the sequence (x_n) contains points arbitrarily close to x_0 but does not contain x_0 ?

We will answer all of these questions over the remainder of the book. You can, however, prove the next theorem now.¹

¹In fact, it appeared previously as Exercise (8.) in Section 4.8.

8.4.10

Theorem

Let $\theta \in [0, 2\pi)$ and let (x_n) be the sequence where, for all $n \in \mathbb{N}$, x_n is the result of rotating $x_0 = (1, 0)$ by the angle $n\theta$. Prove that the following two statements are equivalent:

1. there exist $n, m \in \mathbb{N} \cup \{0\}$ such that $n \neq m$ and $x_n = x_m$.
2. there exists $r \in \mathbb{Q}$ such that $\theta = r\pi$.

8.5 Combining and adapting functions

“The acquisition of knowledge causes us to approach truth when it is a question of knowledge about something we love ... Truth is the radiant manifestation of reality ... To desire contact with a piece of reality is to love.”

– Simone Weil, *The Need for Roots* [134]

Whenever we encounter a new mathematical object we should always ask: how can we combine them or modify them to get more? With functions, two of the most common modifications are to change the domain or codomain or to compose two functions to create a third function.

Restricting Domains and Codomains

Although we insist on specifying the domain and codomain for a function $f: X \rightarrow Y$, there are times when we want to vary them without changing what f does to the elements we care about most.

8.5.1

Definition ► Restricted Functions

Suppose that $f: X \rightarrow Y$ is a function and that $A \subset X$ and that $B \subset Y$ such that range $f \subset B$. Then:

- the function $f|_A: A \rightarrow Y$ defined by $f|_A(a) = f(a)$ for all $a \in A$ is said to be the **restriction** of f to A , and
- the function $f: X \rightarrow B$ is said to be obtained from $f: X \rightarrow Y$ by **restricting** the codomain to B . (Note that we still call the function f - which might be confusing!)

8.5.2

Example

Let $f: \mathbb{R} \rightarrow \mathbb{R}$ be defined by

$$f(x) = \begin{cases} -x & x \leq -1 \\ 0 & x \in (-1, 1) \\ x & x \geq 1 \end{cases}$$

Then the restriction of f to $(-1, 1)$ is the function $f|_{(-1,1)}: (-1, 1) \rightarrow \mathbb{R}$ defined by $f|_{(-1,1)}(x) = 0$ for all $x \in (-1, 1)$.

8.5.3

Example

Let $f: \mathbb{R}^2 \rightarrow \mathbb{R}$ be the function defined by $f(x, y) = x^2 - y^2$ for all $(x, y) \in \mathbb{R}^2$. Let $D = \{(x, y) : |x| + |y| \leq 1\}$ be the diamond of radius 1 centered at the origin. Then the function

$$f|_D: D \rightarrow \mathbb{R}$$

is defined by $f|_D(x, y) = x^2 - y^2$ for all $(x, y) \in D$. Even though $f|_D$ and f are given by the same formula they are different functions since their domains differ.

8.5.4

Example

Let $f: \mathbb{R} \rightarrow \mathbb{R}$ be defined by $f(x) = \arctan(x)$. Recall that $\text{range}(f) = (-\pi/2, \pi/2)$. The function

$$f: \mathbb{R} \rightarrow (-\pi/2, \pi/2)$$

is obtained from $f: \mathbb{R} \rightarrow \mathbb{R}$ by restricting the codomain. Observe that it is still a function as it satisfies the domain and well-defined conditions. The two functions $f: \mathbb{R} \rightarrow \mathbb{R}$ and $f: \mathbb{R} \rightarrow (-\pi/2, \pi/2)$ are not equal since they have different codomains. However, they are given by the same “formula” and we denote them both by f . If the distinction between them is important, we would do better to introduce new notation. For instance, we could say: “Let $g: \mathbb{R} \rightarrow (-\pi/2, \pi/2)$ be the function obtained from f by restricting the codomain to the interval $(-\pi/2, \pi/2)$.”

8.5.5

Example

Let $f: \mathbb{R} \rightarrow \mathbb{R}$ be the function defined by $f(x) = x^3$ for every $x \in \mathbb{R}$. Then the relation

$$f: \mathbb{R} \rightarrow [-1, 1]$$

obtained by restricting the codomain to the interval $[-1, 1]$ is not a function since the domain condition is not satisfied. However,

$$f|_{[-1,1]}: [-1, 1] \rightarrow [-1, 1],$$

obtained by restricting both the domain and the codomain, is a function.

Composing Functions

We can also compose functions. You have seen this before in the context of functions with domain and codomain equal to \mathbb{R} (or possibly \mathbb{R}^n). We give a general definition.

8.5.6

Definition ► Composition of functions

Suppose that $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ are functions. Then $g \circ f: X \rightarrow Z$ defined, for all $x \in X$, by

$$g \circ f(x) = g(f(x))$$

is called the **composition** of g and f .

Observe that function composition is read from right to left. That is, the function on the right is the one that is applied first. Some mathematicians prefer to write function composition from left to right, but those authors, to be consistent, also write $(x)f$ rather than $f(x)$.

8.5.7

Example

Define $f: \mathbb{R}^2 \rightarrow \mathbb{R}$ by $f(x, y) = x^2 + y$ for all $(x, y) \in \mathbb{R}^2$. Define $g: \mathbb{R} \rightarrow \mathbb{R}$ by $g(x) = \cos(x)$. Then

$$g \circ f: \mathbb{R}^2 \rightarrow \mathbb{R}$$

is given by the formula

$$g \circ f(x, y) = \cos(x^2 + y)$$

for all $(x, y) \in \mathbb{R}^2$.

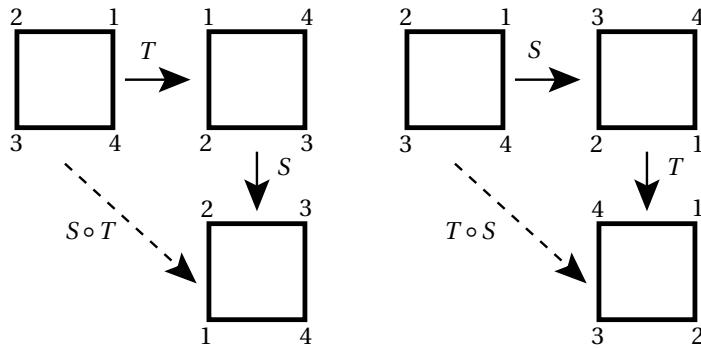
8.5.8

Example

Consider the following symmetries of \mathbb{R}^2 . Let $T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ be a counter-clockwise rotation by an angle of $\pi/2$ radians. Let $S: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ be reflection across the x -axis. We can visualize the effects of S and T on \mathbb{R}^2 by looking at their effect on a square centered at the origin with labels on its corners. See Figure 8.13. Observe that $S \circ T$ is a reflection of \mathbb{R}^2 across the line $y = x$, while $T \circ S$ is a reflection of \mathbb{R}^2 across the line $y = -x$.

The next theorem¹ guarantees that function composition is associative.

¹In the formalization of set theory known as ETCS (see Chapter 6) this is taken as an axiom, and many properties of sets are deduced on the basis of it.

Figure 8.13: Two compositions of symmetries of \mathbb{R}^2 .

8.5.9

Theorem

The following hold for all sets X, Y, Z and all functions $f: X \rightarrow Y$, $g: Y \rightarrow Z$, and $h: Z \rightarrow W$:

- $g \circ f: X \rightarrow Z$ is a function.
- $f \circ \text{id}_X = f$
- $\text{id}_Y \circ f = f$
- $(h \circ g) \circ f = h \circ (g \circ f)$.

Several times in the proof of the theorem we need to show that two functions are equal. Recall from Section 8.1 how to do this.

Proof. **Claim 1:** $g \circ f: X \rightarrow Z$ is a function.

For each $x \in X$, there is a unique element $y \in Y$ such that $f(x) = y$, since f is a function. Similarly, since g is a function, there is a unique element $z \in Z$ such that $g(y) = z$. Consequently, for each element $x \in X$, there is a unique element $z \in Z$ such that $g(f(x)) = z$. Thus, $g \circ f: X \rightarrow Z$ is a function.

Claim 2: $f \circ \text{id}_X = f$ and $\text{id}_Y \circ f = f$.

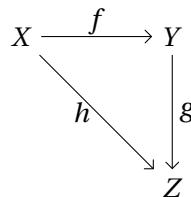
⟨ Prove these statements. ⟩

Claim 3: $(h \circ g) \circ f = h \circ (g \circ f)$

⟨ Prove this statement. ⟩

□

The relationship between various functions is often pictured using diagrams (the names of sets connected by arrows representing the functions). Here is a typical example. Suppose that $f: X \rightarrow Y$, $g: Y \rightarrow Z$ and $h: X \rightarrow Z$ are functions. If $h = g \circ f$, then the diagram:



is said to be **commutative**.

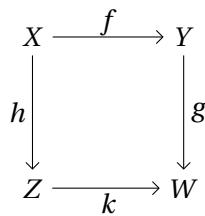
When there are more than 3 functions in play, we extend the definition of “commutative diagram” so that any two paths (i.e. sequences of function compositions) in the diagram that have the same beginning and ending sets and which follow arrows produce equal functions.

8.5.10

Exercise ▶ (Non-commutativity of composition)

Where does the name “commutative diagram” come from? It comes from the fact that function composition is, in general, not commutative.

1. Give examples of a set X and functions $f: X \rightarrow X$ and $g: X \rightarrow X$ such that $f \circ g = g \circ f$. (Composition is sometimes commutative)
2. Give examples of a set X and functions $f: X \rightarrow X$, $g: X \rightarrow X$ such that $f \circ g \neq g \circ f$. (Composition need not be commutative.)
3. Explain the connection between (1.) and (2.) and the statement that the following diagram is commutative if and only if $g \circ f = k \circ h$.



8.6 Being Well-defined

“One thing that topologists have learned in developing Topology is that it almost always pays to convert things into functions or mappings.”

- Daniel Henry Gottlieb [53]

The practice of specifying functions via formulas is so engrained in the mathematical practice of both mathematicians and non-mathematicians that a strange locution has developed. It applies when we talk about functions given by formulas in such a way that it is not immediately clear that the formula actually defines a function in the sense of Definition 8.1.1. The way it works is this. The writer (or speaker) will give a definition of something purported to be a function and will

then claim that it is **well-defined**. What this means is that the purported function is *actually* a function in the sense of Definition 8.1.1. This is most often an issue when elements of the domain can be represented in more than one way and the definition of the purported function relies on a particular representation. Here are some examples.

8.6.1 Example

Define $f: \mathbb{Q} \rightarrow \mathbb{Z}$ by

$$f\left(\frac{a}{b}\right) = a$$

for all $a/b \in \mathbb{Q}$.

Then f is not well-defined. (In other words, f is not a function.) To see this consider the number $1/2 = 3/6 \in \mathbb{Q}$. By the definition of f we have

$$f(1/2) = 1 \text{ and } f(3/6) = 3.$$

Since $1/2 = 3/6$ and since functions have the property that a single input from the domain has exactly one output in the codomain, f is not a function.

8.6.2 Example

Define $f: [0, 1] \rightarrow \mathbb{R}$ as follows. For each $r \in \mathbb{R}$, write r in decimal form as $r = .r_1 r_2 r_3 \dots$ where each $r_i \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Let

$$f(r) = r_1.$$

Then f is not well-defined since $.19\bar{9} = .20\bar{0}$ but $f(.19\bar{9}) = 1$ and $f(.20\bar{0}) = 2$.

Sometimes there is a way to rectify the ambiguity. Here is how we might fix the previous two examples.

8.6.3 Example

Define $f: \mathbb{Q} \rightarrow \mathbb{Z}$ as follows. For each $r \in \mathbb{Q}$, write $r = a/b$ so that $b \in \mathbb{N}$ and so that a and b have no common factors other than ± 1 . Then define $f(r) = a$. Since (by Theorem 9.3.7) each element of \mathbb{Q} has a unique representation as a fraction in lowest terms with positive denominator, f is well-defined. That is, $f: \mathbb{Q} \rightarrow \mathbb{Z}$ is a function.

8.6.4 Example

Define $f: [0, 1] \rightarrow \mathbb{R}$ as follows. For each $r \in \mathbb{R}$, write r in decimal form as $r = .r_1 r_2 r_3 \dots$ where each r_i is one of the digits $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. If there is a choice of decimal representations, we will always choose the

representation which ends in all zeros. Let

8.6.4

$$f(r) = r_1.$$

Then f is well-defined since we have stated precisely how to deal with numbers that have more than one decimal representation.

8.6.5

Exercise

Let $f: \mathbb{Z} \rightarrow \mathbb{Z}$ be defined by $f(n) = |n|$ for each $n \in \mathbb{Z}$. Define $g: \mathbb{Z} \rightarrow \mathbb{Z}$ so that, for all $m \in \mathbb{Z}$, $g(m) = n$ where $n \in \mathbb{Z}$ is the number such that $f(n) = m$. Explain why g is not well-defined and explain possible ways of modifying the definition so that it is well-defined.

When working with functions defined on quotient sets (see Chapter 7), the issue of a function being well-defined is particularly important.

8.6.6

Example

Let \equiv_5 be the equivalence relation on \mathbb{Z} defined by $x \equiv_5 y$ if and only if $x - y \in 5\mathbb{Z}$. Let $\mathbb{Z}/5\mathbb{Z}$ be the quotient set. Define

$$f: \mathbb{Z}/5\mathbb{Z} \rightarrow \mathbb{Z}/5\mathbb{Z}$$

by letting

$$f([x]) = [3x]$$

for all $[x] \in \mathbb{Z}/5\mathbb{Z}$. We claim that f is a well-defined function. We need to do some work to establish this claim, since a particular element in $\mathbb{Z}/5\mathbb{Z}$ is equal to an equivalence class $[x]$ for many different possible $x \in \mathbb{Z}$. Furthermore, it appears as though our definition of f depends on the particular $x \in \mathbb{Z}$ we choose.

To see that f is well-defined, suppose that $[a] = [b]$. By Theorem 7.3.10, we know that $a \equiv_5 b$. By the definition of the equivalence relation, there exists $k \in \mathbb{Z}$ such that $a - b = 5k$. Thus,

$$3a - 3b = 5(3k).$$

Hence, $3a \equiv_5 3b$. Therefore, by Theorem 7.3.10, $[3a] = [3b]$. Hence, $f([a]) = f([b])$, as desired.

8.6.7

Example

Let \equiv_5 be the equivalence relation on \mathbb{Z} defined by $x \equiv_5 y$ if and only if $x - y \in 5\mathbb{Z}$ and let $\mathbb{Z}/5\mathbb{Z}$ be the quotient set. Define

$$f: \mathbb{Z}/5\mathbb{Z} \rightarrow \mathbb{Z}/5\mathbb{Z}$$

by $f([n]) = [2^n]$. We claim that f is not well-defined. To see this, observe

8.6.7

that $f([0]) = [2^0] = [1]$ and

$$f([5]) = [2^5] = [32] = [2].$$

Since $[0] = [5]$ but $[1] \neq [2]$, the function f is not well-defined.

8.6.8

Example

If $a, b \in \mathbb{Z}$ with $b \neq 0$, let $a||b$ be the integer part of the real number a/b . For example, $3||2 = 1$. Let \equiv_{10} be the equivalence relation on \mathbb{Z} defined by $x \equiv_{10} y$ if and only if $x - y \in 10\mathbb{Z}$. Define $f: \mathbb{Z}/10\mathbb{Z} \rightarrow \mathbb{Z}/10\mathbb{Z}$ by

$$f([x]) = [x||2].$$

To show that f is *not* well-defined, we must find $[a], [b] \in \mathbb{Z}/10\mathbb{Z}$ such that $[a] = [b]$ but $f([a]) \neq f([b])$.

Observe that $0||2 = 0$ and $10||2 = 5$. Thus,

$$\begin{aligned} f([0]) &= [0] \text{ and} \\ f([10]) &= [5]. \end{aligned}$$

Recall that $[0] \neq [5]$, since $0 \not\equiv_{10} 5$. However, $[0] = [10]$, since $0 \equiv_{10} 10$. Since the same input produces two different outputs, our “function” is not well-defined (and, hence, is not a function).

8.6.9

Exercise

Let \equiv be the equivalence relation on \mathbb{Z} defined by declaring $x \equiv y$ if and only if $x - y \in 27\mathbb{Z}$. We can define multiplication by 3 on \mathbb{Z}/\equiv by letting

$$f([x]) = [3x]$$

for every $[x] \in \mathbb{Z}/\equiv$. As in Example 8.6.6, f is well-defined. What happens if we try to define division by 3? Recall that for real numbers, we say that $x \div 3 = y$ if and only if $3 \cdot y = x$. Inspired by that, define $g: \mathbb{Z}/\equiv \rightarrow \mathbb{Z}/\equiv$ as follows. For each $[x] \in \mathbb{Z}/\equiv$, let $g([x])$ be the equivalence class $[y]$ such that $[3y] = [x]$. Show that g satisfies neither the domain condition nor the well-defined condition for being a function. Thus, we cannot define division by 3 for the quotient set \mathbb{Z}/\equiv .

8.6.10

Exercise

Determine if the following definitions of f give well-defined functions.

1. Define \equiv_{15} on \mathbb{Z} by declaring $x \equiv_{15} y$ if and only if $x - y \in 15\mathbb{Z}$. For each $[x] \in \mathbb{Z}/15\mathbb{Z}$, let $f([x]) = [x^2 + 1]$. Consider $f: \mathbb{Z}/15\mathbb{Z} \rightarrow \mathbb{Z}/15\mathbb{Z}$
2. Define \equiv_{13} on \mathbb{Z} by declaring $x \equiv_{13} y$ if and only if $x - y \in 13\mathbb{Z}$. For

$[x] \in \mathbb{Z}/13\mathbb{Z}$, let $f([x]) = [y]$ where $[y] \in \mathbb{Z}/13\mathbb{Z}$ is the element such that $[2y] = [x]$. Consider $f: \mathbb{Z}/13\mathbb{Z} \rightarrow \mathbb{Z}/13\mathbb{Z}$

- 8.6.10
3. Define \equiv_{15} on \mathbb{Z} by declaring $x \equiv_{15} y$ if and only if $x - y \in 15\mathbb{Z}$. For $[x] \in \mathbb{Z}/15\mathbb{Z}$, let $f([x]) = [y]$ where $[y] \in \mathbb{Z}/15\mathbb{Z}$ is the element such that $[5y] = [x]$. Consider $f: \mathbb{Z}/15\mathbb{Z} \rightarrow \mathbb{Z}/15\mathbb{Z}$.
 4. Let $X = [0, 1] \subset \mathbb{R}$. Define \sim on X by declaring $x \sim y$ if and only if either $x = y$ or $\{x, y\} = \{0, 1\}$. Define $f: X/\sim \rightarrow \mathbb{R}$ by $f([x]) = \sin(2\pi x)$.
 5. Let $X = [0, 1] \subset \mathbb{R}$. Define \sim on X by declaring $x \sim y$ if and only if either $x = y$ or $\{x, y\} = \{0, 1\}$. Define $f: X/\sim \rightarrow \mathbb{R}$ by $f([x]) = \sin(x)$.

8.7 Properties of Functions

“You can resume your flight whenever you like,’ they said to me, ‘but you will arrive at another Trude, absolutely the same, detail by detail.’”

—Italo Calvino, *Invisible Cities* [23]

As we will see in Chapter 9, if X and Y are sets with n and m elements respectively, then there are m^n functions $X \rightarrow Y$. If X or Y is infinite, there are even more! Most of these functions, however, don’t capture much interesting about the relationship between X and Y or whatever properties they have. For example, if $y_0 \in Y$, then no matter what the set X is there is always the constant function defined by $f(x) = y_0$ for all $x \in X$. Such a function (by itself) tells us nothing useful about X or Y (except that $Y \neq \emptyset$). We will often want to only consider “useful” functions, but what that means depends on the context. In this section, we introduce terminology (much of which should be familiar from pre-calculus) which will allow us to specify what counts as “useful” in particular circumstances.

Injective/Surjective/Bijective

Two important properties that a function may or may not have are the property of being “injective” (also known as “one-to-one”) and “surjective” (also known as “onto”).¹

¹Some people think “injective” and “surjective” sound snooty, but “one-to-one” is too easy to confuse with “one-to-one correspondence”. Injective also has the sense that we are putting one set inside another set. Using “injective” and “onto” together would be just horrendous. Comments in [94] indicate that the widespread adoption of “injective” and “surjective” in the mathematical community was relatively recent.

8.7.1

Definition ▶ Injective/Surjective/Bijective

Suppose that $f: X \rightarrow Y$ is a function. It is:

- **injective** (or **one-to-one**) if for all $a, b \in X$, if $f(a) = f(b)$ then $a = b$.
- **surjective** (or **onto**) if for every $y \in Y$, there exists $x \in X$ such that $f(x) = y$.
- **bijective** if $f: X \rightarrow Y$ is both injective and surjective.

If $f: X \rightarrow Y$ is injective, we will often write $f: X \hookrightarrow Y$. If $f: X \rightarrow Y$ is surjective, we will often write $f: X \twoheadrightarrow Y$. To denote a bijection $f: X \rightarrow Y$, we could combine the symbols \hookrightarrow and \twoheadrightarrow and use a hooked, double-headed arrow. We call injective functions, **injections**; surjective functions **surjections**; and bijective functions **bijections**.

Some people use the term “one-to-one correspondence” to mean “bijective”, but this is easily confused with “one-to-one” and so we will avoid it.

8.7.2

For $f: X \rightarrow Y$ to be a *function*, it must have the property that, for all $a, b \in X$, if $a = b$, then $f(a) = f(b)$. To be injective it must have the property that, for all $a, b \in X$, if $f(a) = f(b)$ then $a = b$. That the property of having a unique output for each input and the property of being injective are converses is no accident - we'll see why when we discuss inverse functions!

Here are equivalent formulations of the three terms. Observe that surjectivity is related to a claim about existence and injectivity is related to a claim about uniqueness.

8.7.3

Theorem ▶ Equivalent Formulations

Suppose that $f: X \rightarrow Y$ is a function. Then:

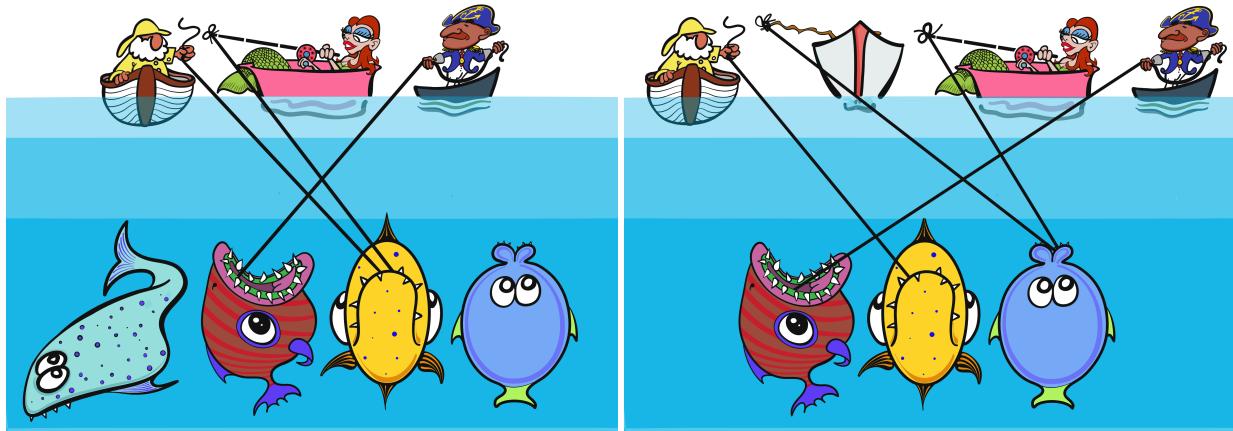
1. $f: X \rightarrow Y$ is injective if and only if for every $y \in Y$ there is at *most* one $x \in X$ with $f(x) = y$.
2. $f: X \rightarrow Y$ is surjective if and only if range $f = Y$.
3. $f: X \rightarrow Y$ is surjective if and only if for every $y \in Y$ there is at *least* one $x \in X$ with $f(x) = y$.
4. $f: X \rightarrow Y$ is bijective if and only if for every $y \in Y$ there is a unique $x \in X$ with $f(x) = y$.

It is often the case in mathematics that there are two (or more) possible formulations of a concept. One of the formulations is easy to use in proofs while the other formulation produces good intuition about what the concept is capturing. Definition 8.7.1 above is the formulation that is easy to use in proofs, while Theorem 8.7.3 conveys the essence of the ideas.

8.7.4

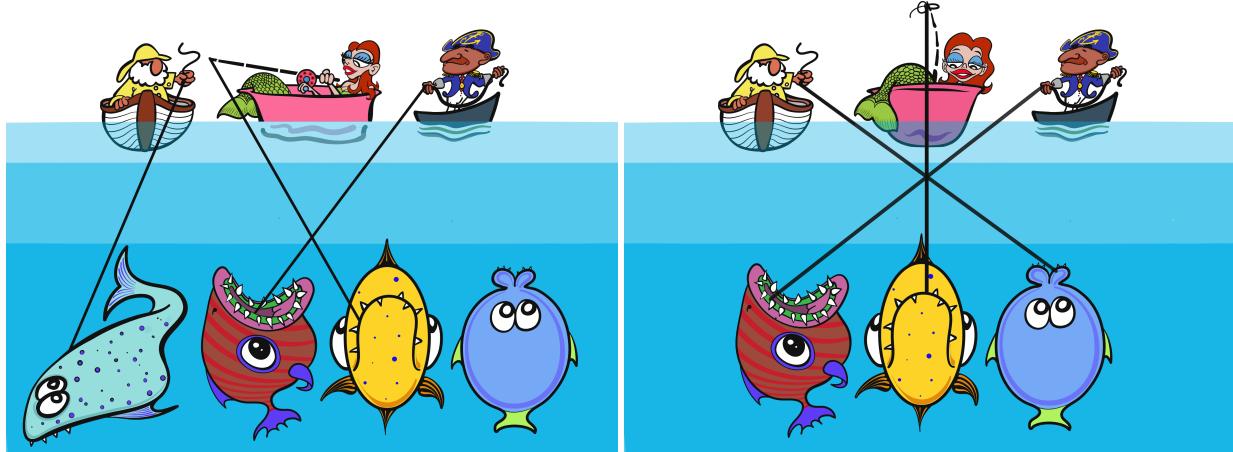
Example

Figure 8.14 shows four examples of functions from a set of fishermen to a set of fish. They show various combinations of being injective (or not) and surjective (or not). Be sure you look at each and say why each is or is not an injection, etc.



(a) Neither injective nor surjective.

(b) Surjective, but not injective.



(c) Injective, but not surjective.

(d) Bijective

Figure 8.14: Four examples of functions from a set of fishermen to a set of fish.

8.7.5

Example

Prove that the function $f: [0, \infty) \rightarrow \mathbb{R}$ defined by $f(x) = \frac{1}{x^2+1}$ is injective.

Proof. Assume that $a, b \in [0, \infty)$ and that $f(a) = f(b)$. We will show that $a = b$.

Since $f(a) = f(b)$, by the definition of f , we have:

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

Algebra then shows that

$$a^2 = b^2$$

Thus,

$$(a - b)(a + b) = 0.$$

Since the product of two real numbers is zero if and only if one of them is zero, either $a = b$ or $a = -b$. If $a = -b$, then since $a, b \geq 0$, we have $a = b = 0$. Thus, in any case, $a = b$. Consequently, f is injective. \square

Notice how we use Definition 8.7.1 to prove that f is injective. Although in some circumstances there may be another way to prove a function is injective, in general we follow the structure:

PROVING INJECTIVITY

To show: $f: X \rightarrow Y$ is injective.

Structure of Proof: Assume $a, b \in X$ and that $f(a) = f(b)$. We will show that $a = b$.

(Apply the definition of f and then do work.)

Thus, $a = b$. Since this is true for all $a, b \in X$, the function f is injective. \square

Proving the next theorem is an opportunity to practice using the proof structure.

8.7.6

Theorem ▶ Composition of injections is an injection

Suppose that $f: X \rightarrow Y$ is an injection and $g: Y \rightarrow Z$ is also an injection. Then $g \circ f: X \rightarrow Z$ is an injection.

Proofs of injectivity tend to be relatively straightforward. Many students find proving surjectivity to be harder. This is likely because a proof that a function is surjective is, at its heart, an existence proof. If we want to show a function $f: X \rightarrow Y$ is surjective we must show that if for every $y \in Y$ *there exists* an $x \in X$ such that $f(x) = y$.

8.7.7

Example

Let $f: (0, 1) \rightarrow (1, \sqrt{5})$ be defined by $f(x) = \sqrt{4x^2 + 1}$ for all $x \in (0, 1) \subset \mathbb{R}$. Prove that f is surjective.

Proof. Let $y \in (1, \sqrt{5})$. We will show that there exists $x \in (0, 1)$ such that $f(x) = y$.

Define $x = \sqrt{(y^2 - 1)/4}$.

Claim 1: $x \in (0, 1)$.

Since $1 < y < \sqrt{5}$, we have:

$$\begin{aligned} 1 &< y^2 && < 5 \Rightarrow \\ 0 &< y^2 - 1 && < 4 \Rightarrow \\ 0 &< (y^2 - 1)/4 && < 1 \Rightarrow \\ 0 &< \sqrt{(y^2 - 1)/4} && < 1 \Rightarrow \\ 0 &< x && < 1. \end{aligned}$$

Claim 2: $f(x) = y$.

$$\begin{aligned} f(x) &= \sqrt{4x^2 + 1} \\ &= \sqrt{4(y^2 - 1)/4 + 1} \\ &= \sqrt{y^2} \\ &= |y| \\ &= y. \end{aligned}$$

In the calculations above, we used the fact that $y^2 - 1 \geq 0$ and that $y \geq 0$. □

8.7.8

Usually, as in the example above, to prove that a function $f: X \rightarrow Y$ is surjective we follow a pattern much like any existence proof:

PROVING SURJECTIVITY

To show: $f: X \rightarrow Y$ is surjective.

Structure of Proof: Assume $y \in Y$. We will show that there exists $x \in X$ such that $f(x) = y$.

\langle Define a particular $x \in X$ \rangle

\langle Show $f(x) = y$ \rangle

Thus, f is surjective. □

Proving the next theorem is an opportunity to practice using the proof structure.

8.7.9

Theorem ▶ Composition of surjections is a surjection

Suppose that $f: X \rightarrow Y$ is a surjection and $g: Y \rightarrow Z$ is also a surjection. Then $g \circ f: X \rightarrow Z$ is a surjection.

To prove that a function $f: X \rightarrow Y$ is a bijection, often we show that it is an injection and a surjection. For example,

8.7.10

Theorem ▶ Composition of bijections is a bijection

Suppose that $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ are bijections. Then $g \circ f: X \rightarrow Z$ is a bijection.

Proof. Assume f and g are bijections. We will show that $g \circ f$ is a bijection.

By definition of “bijection,” f and g are both injections and are both surjections. By Theorem 8.7.6, $g \circ f$ is an injection. By Theorem 8.7.9, $g \circ f$ is a surjection. Since $g \circ f$ is both an injection and a surjection, it is a bijection. \square

After we discuss inverse functions, we will see that we can also prove a function is a bijection by producing an inverse function for it.

Here is an example where we show a function is a bijection. In the proof of surjectivity, the existence statement arises from an appeal to a previously proved theorem (the intermediate value theorem). With some effort and perhaps the use of WolframAlpha or similar software it is possible to write a proof following the general pattern. The injective proof is not particularly pretty, but we have decided to rely on some tedious, but straightforward algebra rather than appeal to theoretical results from Calculus, like we do in the surjective proof. Can you write such a proof? Which proof do you think is nicer?

8.7.11

Example

The function $f: \mathbb{R} \rightarrow \mathbb{R}$ defined by $f(x) = x(x^2 + 1)$ is a bijection.

We must show that f is both injective and surjective.

Injective: Assume that $a, b \in \mathbb{R}$ and that $f(a) = f(b)$. We will show that $a = b$.

Since $f(a) = f(b)$, by the definition of f :

$$a(a^2 + 1) = b(b^2 + 1).$$

By algebra, this is equivalent to:

$$(a^3 - b^3) + (a - b) = 0$$

Factoring out $(a - b)$ we obtain:

$$(a - b)(a^2 + ab + b^2 + 1) = 0.$$

The product of two real numbers is zero if and only if at least one of them is zero. Thus, either $a - b = 0$ or $a^2 + ab + b^2 + 1 = 0$. Assume, first, that

8.7.11

$a^2 + ab + b^2 + 1 = 0$. Using the quadratic formula to solve for a shows that

$$a = \frac{-b \pm \sqrt{b^2 - 4(b^2 + 1)}}{2} = \frac{-b \pm \sqrt{-3b^2 - 4}}{2}.$$

Since $-3b^2 - 4 < 0$ and since $a \in \mathbb{R}$, we have a contradiction. Thus, $a^2 + ab + b^2 + 1 \neq 0$. Consequently, $a - b = 0$. Thus, $a = b$, as desired.

Since $f(a) = f(b) \Rightarrow a = b$ for all $a, b \in \mathbb{R}$ we have shown that f is injective.

Surjective: Let $y \in \mathbb{R}$. We will show that there exists $x_0 \in \mathbb{R}$ such that $f(x_0) = y$.

The function $f(x) = x(x^2 + 1)$ is continuous and $\lim_{x \rightarrow \infty} f(x) = \infty$ and $\lim_{x \rightarrow -\infty} f(x) = -\infty$. Thus, for the given y , there is an x_+ such that $f(x_+) > y$ and there is an $x_- \in \mathbb{R}$ such that $f(x_-) < y$. Hence, by the Intermediate Value Theorem, there exists $x_0 \in (x_-, x_+)$ such that $f(x_0) = y$. Since this is true for all $y \in \mathbb{R}$, the function f is surjective. \square

8.7.12

Exercise

Define $f: \mathbb{N} \rightarrow [0, 1]$ so that, for all $n \in \mathbb{N}$,

$$f(n) = 1/n^2.$$

Prove that f is injective but not surjective.

8.7.13

Exercise

Define $f: \mathbb{N} \rightarrow \mathbb{N}$ by

$$f(n) = \begin{cases} n+1 & n \text{ is odd} \\ n-1 & n \text{ is even} \end{cases}$$

for all $n \in \mathbb{N}$. Prove that f is a bijection.

8.7.14

Exercise

Let $p \in \mathbb{N}$ be prime. Define $r: \mathbb{N}^* \rightarrow \{0, 1, \dots, p-1\}$ by letting $r(n)$ be the remainder of n after dividing by p . Prove that r is surjective.

8.7.15

Exercise

Let \equiv be the equivalence relation on \mathbb{Z} defined by declaring $x \equiv y$ if and only if $x - y \in 12\mathbb{Z}$. Define $f: \mathbb{Z}/\equiv \rightarrow \mathbb{Z}/\equiv$ by letting $f([x]) = [3x]$ for every $[x] \in \mathbb{Z}/\equiv$. Show that f is a function and that it is neither injective nor surjective.

8.7.16

Exercise

Let \equiv be the equivalence relation on \mathbb{Z} defined by declaring $x \equiv y$ if and only if $x - y \in 13\mathbb{Z}$. Define $f: \mathbb{Z}/\equiv \rightarrow \mathbb{Z}/\equiv$ by letting $f([x]) = [3x]$ for every $[x] \in \mathbb{Z}/\equiv$. Show that f is a function and that it is both injective and surjective.

8.7.17

Exercise

Find bijections between the following sets. You may assume whatever facts from calculus you need.

1. $\mathbb{N} \rightarrow \mathbb{N} \setminus \{1\}$
2. $\mathbb{N} \rightarrow 2\mathbb{N} = \{2, 4, 6, 8, \dots\}$.
3. $\mathbb{N} \rightarrow \mathbb{Z}$
4. $[2, 5] \rightarrow [-1, 6]$ (These are both intervals in \mathbb{R} .)
5. $(a, b) \rightarrow (c, d)$ where $a < b$ and $c < d$. (These are both intervals in \mathbb{R} .)
6. $(-\pi/2, \pi/2) \rightarrow \mathbb{R}$

The next exercise concerns finding a bijection between a closed interval and a non-closed interval. It is likely more challenging.

8.7.18

Exercise

Find a bijection $f: [0, 1] \rightarrow [0, 1)$.

(Hint: Consider trying to modify the identity map $\text{id}: [0, 1] \rightarrow [0, 1]$ so that it “misses” the number 1 in the codomain. Choose some number $r \in [0, 1)$ and declare $f(1) = r$. In order to guarantee f will be injective when we are done, you should then pick some $s \neq r$ in $[0, 1)$ and declare $f(r) = s$. Continue on in this manner, and don’t forget that f needs to be defined on every element of $[0, 1]$. You’ll want to define your function piecewise, as it is a fact from topology that there is no continuous surjection $[0, 1] \rightarrow [0, 1]$.)

By restricting the codomain of a function it is possible to make a function surjective. See Figure 8.15 for a schematic depiction.

8.7.19

Theorem

Suppose that $f: X \rightarrow Y$ is a function. The function $f: X \rightarrow \text{range } f$ obtained by restricting the codomain of f to the set $\text{range } f$ is surjective.

It would be nice to know that, without changing our codomain, it is possible to restrict the domain of a function to make it injective. Informally, we can do this fairly easily. Suppose that $f: X \rightarrow Y$ is a function, as in Figure 8.16. For each

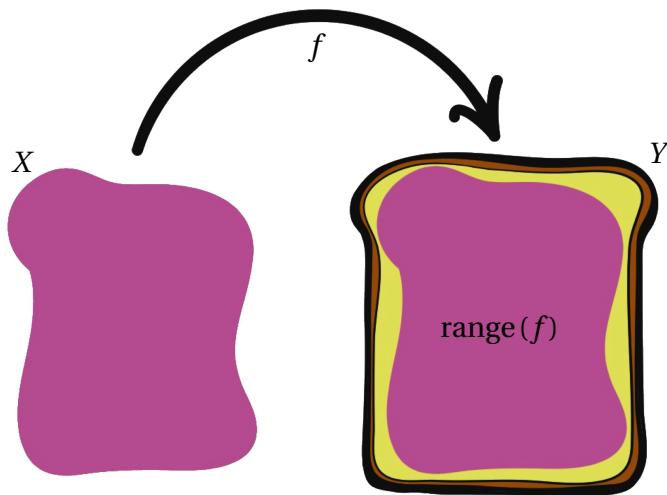


Figure 8.15: A schematic depiction of a non-surjective function $f: X \rightarrow Y$. The yellow set on the right is the codomain of f and the red proper subset indicates the range of f . If we ignore all the points of Y that are not in the red, f remains a function, now having its range as the codomain. So it is surjective.

element $y \in Y$, let $U_y \subset X$ be the set of all $x \in X$ such that $f(x) = y$. For each $y \in Y$, choose a single element $a_y \in U_y$ and let $A = \{a_y : y \in Y\}$. Then consider $g: A \rightarrow Y$ defined by $g(x) = f(x)$. If $g(x) = g(x')$ then $x = a_y = x'$ for $y \in f(x)$. We designed A so that there is a unique a_y for each $y \in Y$. Thus, g must be injective.

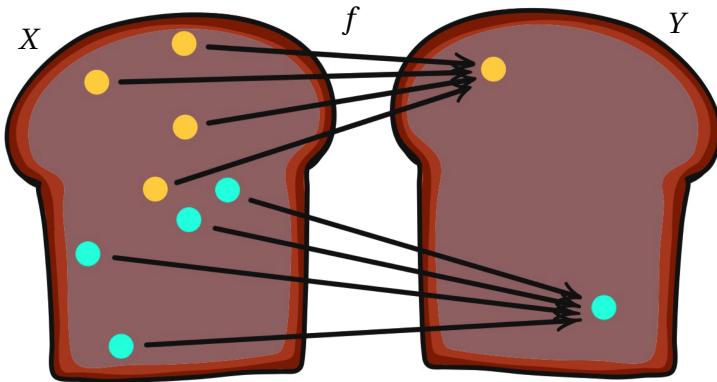


Figure 8.16: A schematic depiction of a non-surjective function $f: X \rightarrow Y$. Suppose that f takes each of the yellow points in X to the yellow point in Y and each of the aqua points in X to the aqua point in Y . When we create the set $A \subset X$ so that $f|_A: A \rightarrow Y$ is injective and has the same range as f , we will need to choose A so that it contains exactly one of the yellow points in X and exactly one of the aqua points in Y .

The difficulty with this line of argument is that we haven't given precise instructions for how to define each a_y . This means that it isn't clear that A is actually a

set. Might its existence lead to a logical contradiction such as Russell's paradox? The Axiom of Choice (mentioned in Chapter 6) says that we can define the set A in such a fashion. Unfortunately, in a completely general setting, there is no way to give explicit instructions for how to choose the a_y , so the Axiom of Choice is useful as a theoretical tool, but less useful as a practical one. Here is an example:

8.7.20 Example

Consider the set of lines in \mathbb{R}^2 . Each line can be expressed as the graph of an equation of the form $\alpha x + \beta y + \gamma = 0$, with not all three of α, β, γ equal to 0. This gives a function ϕ whose domain is the set $\mathbb{R}^3 \setminus \{0\}$ and whose codomain is the set of lines in \mathbb{R}^3 . That is, for $(\alpha, \beta, \gamma) \in \mathbb{R}^3$ with $\alpha\beta\gamma \neq 0$, the image $\phi(\alpha, \beta, \gamma)$ is the line which is the graph of $\alpha x + \beta y + \gamma = 0$. The function ϕ is not injective, since, for example, the equations $2x+3y+4=0$ and $2\pi x+3\pi y+4\pi=0$ have the same graph. Thus, $\phi(2, 3, 4) = \phi(2\pi, 3\pi, 4\pi)$. Is there a subset $A \subset \mathbb{R}^3 \setminus \{0\}$ such that the function $\phi|_A$ is injective? That is, each line in \mathbb{R}^2 is described by a unique choice of $(\alpha, \beta, \gamma) \in A$?

There is! For each line L , let $H(L)$ be the set of points $(\alpha, \beta, \gamma) \in \mathbb{R}^3$ such that L is the graph of the equation $\alpha x + \beta y + \gamma z = 0$. Then $\mathcal{H} = \{H(L)\}$ is a set whose elements are non-empty sets. By the Axiom of Choice, there exists a unique $c_L = (\alpha_L, \beta_L, \gamma_L) \in H(L)$ for each L such that

$$A = \{c_L : L \text{ is a line}\}$$

is a set. Then the function $\phi|_A$ with domain A and codomain the set of lines is a bijection.

We generalize the example as follows. The proof uses material from Chapter 6; so if you didn't study that chapter you should feel free to skip the proof of this theorem. The theorem itself will be useful in Chapter 10.

8.7.21 Theorem

Suppose that $f: X \rightarrow Y$ is a function. There exists a subset $A \subset X$ such that $f|_A: A \rightarrow Y$ is injective and $\text{range}(f|_A) = \text{range}(f)$.

Proof. Let $y \in Y$. Let $U_y = \{x \in X : y = f(x)\}$. It is a set by the Axiom of Subset Selection. The Axiom of Power Sets guarantees that the set $\mathcal{P}(X)$ of all subsets of X is a set. Applying the Axiom of Subset Selection again, we see that

$$\mathcal{H} = \{H \in \mathcal{P}(X) : \exists y \in Y \text{ s.t. } H = U_y \text{ and } U_y \neq \emptyset\}$$

is a set. By the Axiom of Choice, for each $U_y \in \mathcal{H}$, there exists $a_y \in U_y$ such that $A = \{a_y\}$ is a set. Since each $a_y \in X$, $A \subset X$.

We claim that $f|_A: A \rightarrow Y$ is injective. The key is that A was created by choosing exactly one element from each set in \mathcal{H} . Suppose that $a, b \in A$ and that $f|_A(a) = f|_A(b)$. Let $y = f|_A(a) = f|_A(b)$. We see that $f(a) = f(b) = y$ by the definition of what it means to restrict the domain of a function. Consequently, $a, b \in U_y$. Since $A \cap U_y = \{a_y\}$ has a unique element, $a = b = a_y$.

Thus, $f|_A$ is injective.

It remains to show that $f|_A$ has the same range as f . Clearly, $\text{range}(f|_A) \subset \text{range}(f)$, since $f|_A$ is the restriction of f to $A \subset X$. We will show that $\text{range}(f) \subset \text{range}(f|_A)$. Suppose that $y \in \text{range}(f)$. Recall that $A \cap U_y = \{a_y\}$. By the definition of U_y , $f(a_y) = y$. Thus, $\text{range}(f) \subset \text{range}(f|_A)$. Therefore, the ranges of f and $f|_A$ are equal. \square

Inverses

As we noted in the introduction, we often want to be able to “undo” the effect of a function. We make this precise through inverse functions. This is a generalization of standard facts about functions from pre-calculus or linear algebra.

8.7.22

Definition ▶ Inverse Function

Suppose that $f: X \rightarrow Y$ and $g: Y \rightarrow X$ are functions. They are **inverses** of each other if

$$\text{For all } x \in X, \quad g \circ f(x) = x, \text{ and}$$

$$\text{For all } y \in Y, \quad f \circ g(y) = y.$$

We also say that g is an inverse function for f and that f is an inverse function for g . Equivalently, f and g are inverses if $f \circ g = \text{id}_Y$ and $g \circ f = \text{id}_X$. See Figure 8.17

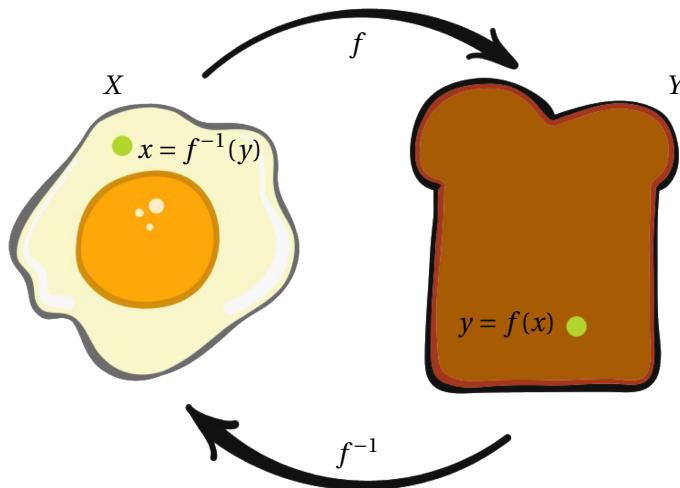


Figure 8.17: A commutative diagram showing the relationship of a function f to its inverse f^{-1} .

A function may or may not have an inverse, but if it does the inverse is unique. As a result of Theorem 8.7.23, if f has an inverse we denote it f^{-1} .

8.7.23

Theorem ▶ Inverse functions are unique

Suppose that $f: X \rightarrow Y$ has an inverse function $g: Y \rightarrow X$. Then g is the unique inverse function for f .

Here is the crucial theorem concerning inverse functions.

8.7.24

Theorem ▶ A function has an inverse iff it is a bijection

A function $f: X \rightarrow Y$ has an inverse function if and only if it is a bijection.

As a reminder, you should organize your proof of Theorem 8.7.24 as follows:

Proof. \Leftarrow Assume that $f: X \rightarrow Y$ has an inverse function $g: Y \rightarrow X$. We will show that f is a bijection by showing it is injective and surjective.

\langle Prove that f is injective \rangle

\langle Prove that f is surjective \rangle

\Rightarrow Assume that $f: X \rightarrow Y$ is a bijection. We will show that there is a function $g: Y \rightarrow X$ such that f and g are inverses.

\langle Define $g: Y \rightarrow X$ \rangle

\langle Prove that g is a function. \rangle

\langle Show that $f \circ g = \text{id}_Y$ \rangle

\langle Show that $g \circ f = \text{id}_X$ \rangle

□

8.7.25

Exercise

Suppose that $f: X \rightarrow Y$ has an inverse function $f^{-1}: Y \rightarrow X$. Prove the following:

1. f^{-1} is a bijection
2. f^{-1} has an inverse function $(f^{-1})^{-1}$.
3. $f = (f^{-1})^{-1}$.

A straightforward consequence concerns permutations.

8.7.26

Definition ▶ Permutations

Suppose that X is a set. A bijection $f: X \rightarrow X$ is called a **permutation** of X . The set of permutations of X is denoted $\text{Perm}(X)$.

8.7.27

Theorem

Suppose that X is a set. Then $\text{Perm}(X)$ is a group with $\text{id} = \text{id}_X$ and function composition as the operation.

Algebraic and Metric Structures

The property of being injective and the property of being surjective are properties that any function $f: X \rightarrow Y$ may or may not have, regardless of any particular properties of the sets X and Y . When we restrict consideration to sets X and Y having certain fixed properties (such as being groups or being metric spaces) it is natural to only consider functions between those sets which preserve the properties of X and Y . Here are two examples, both connected to concepts you've encountered in previous math classes.

Group homomorphisms

If X and Y are groups, a group homomorphism $f: X \rightarrow Y$ relates the group structure on X to the group structure on Y . If you have taken linear algebra, you may recognize that linear functions between vector spaces are examples of group homomorphisms.

8.7.28 Definition ► Group Homomorphism

Suppose that X is a group with operation denoted \circ and that Y is a group with operation denoted $*$. A **homomorphism** is a function $f: X \rightarrow Y$ such that for all $a, b \in X$,

$$f(a \circ b) = f(a) * f(b).$$

8.7.29 Example

Let X and Y be groups. If $\mathbb{1}_Y$ is the identity element of Y , then the constant function $f(x) = \mathbb{1}_Y$ (for all $x \in X$) is a homomorphism. No other constant function is a homomorphism.

8.7.30 Example

Let $m \in \mathbb{R}$ and consider $X = \mathbb{R}$ and $Y = \mathbb{R}$ as groups, both with $+$ as the operation. Then the function $f: X \rightarrow Y$ defined by $f(x) = mx$ for all $x \in X$ is a homomorphism. If we replace \mathbb{R} with \mathbb{Z} or \mathbb{Q} , f is still a homomorphism.

8.7.31 Example

Let $X = \mathbb{R}$ be considered as a group with operation $+$ and let $Y = (0, \infty) \subset \mathbb{R}$ be considered as a group with multiplication \cdot as the operation. Let $\exp: X \rightarrow Y$ be the exponential function, defined by $\exp(x) = e^x$ for all $x \in X$. Then \exp is a group homomorphism.

If $f: X \rightarrow Y$ is a group homomorphism, then the set $\ker f = \{x \in X : f(x) = \mathbb{1}_Y\}$ is called the **kernel** of f . The following theorem is an important tool in group theory. It is an analogue of theorems from linear algebra concerning the kernel and image of linear functions.

8.7.32

Theorem

If X and Y are groups and $f: X \rightarrow Y$ is a homomorphism, then $\ker f$ is a subgroup of X and $\text{range } f$ is a subgroup of Y .

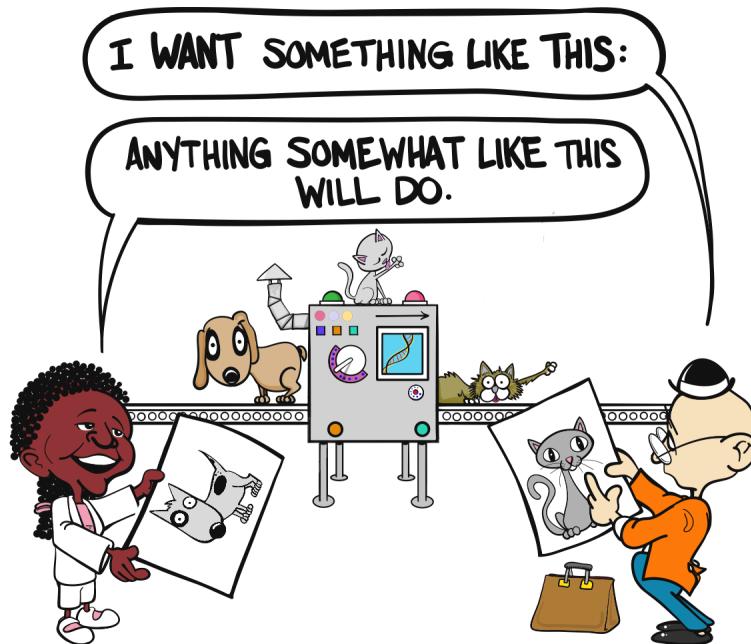
Continuity

Just as homomorphisms are the useful functions between groups, so continuous maps are the useful functions between metric spaces. You have encountered the notion of continuity previously in pre-calculus and calculus, we will consider a generalization of it to metric spaces. It turns out that continuity is such a useful concept that it can be generalized to settings beyond metric spaces, but we will not explore that here. Take a course in topology for more!

8.7.33

Definition ▶ Continuous Function

Suppose that X and Y are metric spaces with metrics d_X and d_Y respectively. A function $f: X \rightarrow Y$ is **continuous at $p \in X$** if for every $\epsilon > 0$, there exists $\delta > 0$ such that for all $x \in X$ if $d_X(x, p) < \delta$, then $d_Y(f(x), f(p)) < \epsilon$. If f is continuous at every $p \in X$, then f is continuous.



This definition is rather complex, so to gain an intuitive understanding of what it is conveying, consider the following problem. A company has a machine named f that takes inputs and produces outputs for customers. The machine is incredibly finely-tuned and, for a given input, is guaranteed to produce the specified

output. Unfortunately, the material which goes into the machine is imperfect, but the imperfections can be measured and, for a cost, screened out. A customer comes to the company and asks for a certain output $f(p) \in \text{range}(f)$. The company says, “Due to the imperfections of the inputs, we can’t guarantee that you will get precisely the output you ask for.” Since the machine f is continuous, they go on to add, “We can, however, get as close as you want, if you’re willing to pay enough.” The customer responds, “OK, I’ll accept outputs which differ by at most ϵ from my desired output $f(p)$.” The engineers working for the company then figure out what imperfections of inputs are allowable and determine that as long as the inputs x to the machine are within δ of p , the outputs $f(x)$ will be within ϵ of the desired output $f(p)$.

This definition is most easily visualized for functions $f: \mathbb{R} \rightarrow \mathbb{R}$, where we give both the domain and codomain the euclidean metric $d(a, b) = |a - b|$, for all $a, b \in \mathbb{R}$.

8.7.34 Example

Look at the graph of the function $f: \mathbb{R} \rightarrow \mathbb{R}$ in Figure 8.18.

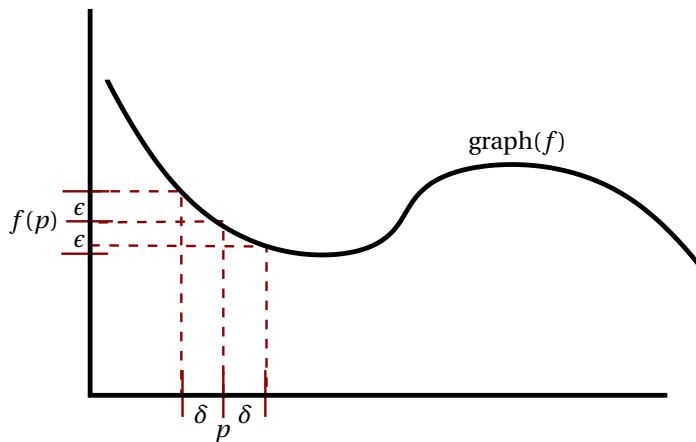


Figure 8.18: An example of a continuous function $f: \mathbb{R} \rightarrow \mathbb{R}$. Observe that for the given a_0 , whenever x is within δ of a_0 , the output $f(x)$ will be within ϵ of $f(a_0)$. Since for every choice of a_0 and $\epsilon > 0$, there is some $\delta > 0$ such that this is true, the function is continuous.

8.7.35 Example

To see how the definition of continuity breaks down for a discontinuous function, consider the function $f: \mathbb{R} \rightarrow \mathbb{R}$ depicted in Figure 8.19.

8.7.36 Exercise

Let \mathbb{R} have the usual euclidean metric. Let $f(x): \mathbb{R} \rightarrow \mathbb{R}$ be defined by $f(x) = 3x$. Prove that f is continuous at $a_0 = 0$.

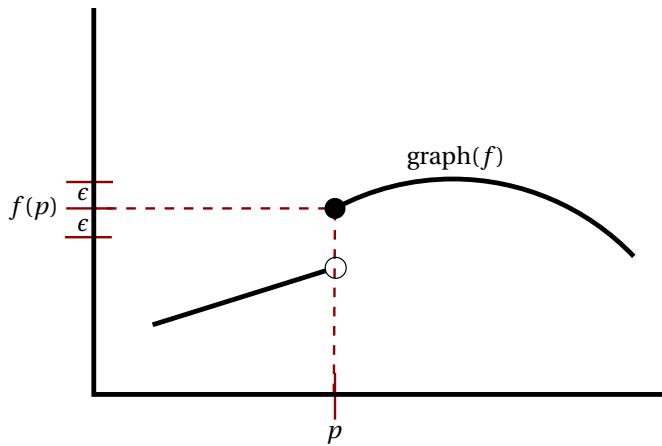


Figure 8.19: An example of a discontinuous function $f: \mathbb{R} \rightarrow \mathbb{R}$. Observe that for the given p , if $x \neq p$ is less than p , then $f(x)$ will never be within the given ϵ of $f(p)$. That is, there exists an $p \in \mathbb{R}$ and $\epsilon > 0$ such that for all $\delta > 0$, there exists $x \in \mathbb{R}$ such that $d_X(x, p) < \delta$ but $d_Y(f(x), f(p)) \geq \epsilon$.

8.7.37

Exercise

Let \mathbb{R} have the usual euclidean metric. Let $f(x): \mathbb{R} \rightarrow \mathbb{R}$ be defined by

$$f(x) = \begin{cases} x - 1 & x \leq 0 \\ x + 1 & x > 0 \end{cases}.$$

Prove that f is not continuous at $p = 0$.

Whether or not a given function is continuous depends heavily on the underlying metrics, as demonstrated by the next exercise.

8.7.38

Exercise

Let $X = \mathbb{R}$, with the usual euclidean metric and let $Y = \mathbb{R}$. Let $\text{id}: X \rightarrow Y$ be the identity function.

1. Give Y the discrete metric $d_Y(x, y) = \begin{cases} 1 & x \neq y \\ 0 & x = y \end{cases}$. Prove that id is discontinuous at every $p \in \mathbb{R}$.
2. Give Y the euclidean metric. Prove that id is continuous.

Just because a certain property of functions (such as continuity) is useful, doesn't mean that if a bijection f has the property than its inverse f^{-1} also does. See the next exercise.

8.7.39

Exercise

Let X and Y both equal \mathbb{R} and let $f: X \rightarrow Y$ be the identity function. Let $g: Y \rightarrow X$ also be the identity function. Observe that f and g are inverses.

8.7.39

Find metrics on X and Y such that $f: X \rightarrow Y$ is continuous, but $g: Y \rightarrow X$ is discontinuous.

In Chapter 11, we will discuss what it means for a sequence in a metric space to converge. It turns out that a function between metric spaces is continuous if and only if it takes convergent sequences to convergent sequences, but we do not explore that in this text.

8.8 Application: Affine Encryption

“We have this kind of superpower, this cultivated superpower to look at something technical and see what’s really going on. It gives us an ability to intervene on some black boxes. There are a lot of black boxes out there that mathematicians have the skills to open.”

– Moon Duchin¹ [90]

Cryptology is the study of encoding information in such a way that the intended recipient is the only one who can read the message. Modern cryptology is a blend of mathematics, computer science, business, and psychology. Affine ciphers are one of earliest and simplest ways to encode a message.

Suppose that Bob want to send the message:

“Mathematics is the queen of the sciences”

to his friend Alice², but he doesn’t care about the punctuation, capitalization, or spacing between words. One relatively simple way to encode it is to replace each letter with the successive letter of the alphabet. So, for instance, he would replace *a* with *b*, *b* with *c*, etc. If there were a *z* in the message, he would replace it with an *a*. Doing that Bob ends up with the message:

“nbuifnbujdtjtuifrvffopguiftdjfodft”

Of course, instead of shifting each letter by one, he could choose to encode by shifting by some other number of places. For instance, if he shifts by 5, he arrives at the coded message:

“rfymjrfynhxnxymjvzjjstkmjxhnjshjx”

Assuming that Alice knows the method used to encode the message, to decode the message she just needs to shift by the correct amount backwards through

¹Moon Duchin is a mathematician who has made important contributions to geometric group theory and the mathematics of political redistricting.

²The names Alice and Bob are traditional. According to Wikipedia, they first appeared in a paper by the inventors of the now ubiquitous RSA encryption system.

the alphabet. So if Bob encodes by replacing a with b , b with c and so forth, then Alice replaces a with z , b with a , and so forth. Similarly, if Bob shifted each letter forward by 5, then Alice shifts each letter backwards through the alphabet 5 places.

Since Alice and Bob ignore punctuation, capitalization, and spacing, they can identify each of the 26 letters of the alphabet with its position, beginning with a being identified with 0; b with 1 and so forth. The alphabet then is naturally identified with the quotient set $\mathbb{Z}/26\mathbb{Z}$. The method for encryption that we've discussed so far then corresponds with an encoding function

$$T: \mathbb{Z}/26\mathbb{Z} \rightarrow \mathbb{Z}/26\mathbb{Z}$$

defined by

$$T([x]) = [x] + [b]$$

where b is our choice of how much to forward shift each letter of the alphabet. Recall from Section 7.8, that by definition $[x] + [b] = [x + b]$ and that T is a well-defined function. Since Bob encodes his message by applying T to each letter, Alice decodes the message by applying T^{-1} to each letter, where T^{-1} is defined by

$$T^{-1}([y]) = [y] + [-b].$$

Since T and T^{-1} are inverse functions, upon decoding the encoded message Bob sends to her, Alice sees Bob's original, un-encoded message.

Of course, encodings using a simple shift are very easy to recognize and decode, whether or not we know how Bob encoded the message. Can we do something slightly more sophisticated?

Thinking about arithmetic in $\mathbb{Z}/26\mathbb{Z}$, suggests some possibilities. To encode our message letter-by-letter, Bob is looking for a function

$$T: \mathbb{Z}/26\mathbb{Z} \rightarrow \mathbb{Z}/26\mathbb{Z}.$$

Since he wants Alice to be able to decode it, the function T needs to have an inverse. One natural family of possibilities are the Caesar ciphers. These are functions T defined by a choice of $[m], [b] \in \mathbb{Z}/26\mathbb{Z}$ so that

$$T([x]) = [m][x] + [b]$$

for every $[x] \in \mathbb{Z}/26\mathbb{Z}$.

8.8.1

Exercise

Prove that T is well-defined, for each choice of $[m]$ and $[b]$.

8.8.2

Example

Let $m = 3$ and $b = 2$. Thus, $T[x] = [3][x] + [2]$ for each $[x] \in \mathbb{Z}/26\mathbb{Z}$. Thus, for example, a is encoded as c , b as f , c as i , and so forth.

When Bob encodes the message “Mathematics is the queen of the sciences” he obtains

“mchxomchaieaehxoykoopsrhxoeiaopioe”

Alice knows how Bob encoded the message using T . To decode the message, she needs to find T^{-1} . She tries using algebra. Let $[y] = T([x])$. Then

$$[y] + [-2] = [3][x].$$

To finish solving for $[x]$, she apparently needs to divide by $[3]$. Unfortunately, division doesn’t seem to be a well-defined operation in $\mathbb{Z}/26\mathbb{Z}$. What to do?

Alice recalls that for rational numbers, dividing is the same as multiplying by the reciprocal, but $1/3 \notin \mathbb{Z}$. For rational numbers, $1/3$ is the multiplicative inverse of 3. What is the equivalent in $\mathbb{Z}/26\mathbb{Z}$? Alice, under a flash of inspiration, realizes that $[3] \cdot [9] = [27] = [1]$. That is, $[9]$ is the multiplicative inverse of $[3]$ in $\mathbb{Z}/26\mathbb{Z}$. So instead of attempting to divide by $[3]$, she can multiply by $[9]$. She deduces that

$$T^{-1}([y]) = [9]([y] + [-2]) = [9][y] + [8].$$

8.8.3

Exercise

Let $T([x]) = [3][x] + [2]$ and $T^{-1}([y]) = [9][y] + [8]$ for all $[x], [y] \in \mathbb{Z}/26\mathbb{Z}$. Verify that T and T^{-1} are inverse functions.

8.8.4

Exercise

Prove that T is a bijection if and only if $[m]$ can be represented by an odd number $m \in \{0, \dots, 25\}$ other than 13.

8.8.5

The function $T: \mathbb{Z}/26\mathbb{Z} \rightarrow \mathbb{Z}/26\mathbb{Z}$ defined by $T([x]) = [m][x] + [b]$ for all $[x] \in \mathbb{Z}/26\mathbb{Z}$ is called an **affine cipher**. The numbers m and b are called the **key** for the cipher. With the choice $[m] = [1]$ and $[b] = [4]$, it is known as the “Caesar cipher,” since Caesar used it when communicating with close friends. Affine ciphers are very easy to decode using a method known as “letter frequency analysis.” For more on the history and mathematics of ciphers, see Holden’s excellent text [70]. This section is based on the first chapter of that book.

According to Exercise 8.8.4, there are many keys for affine ciphers which cannot be decoded using an inverse function. In that exercise, the values for m which cause a problem are those which share a common factor (other than ± 1) with 26, the number of letters in our alphabet. This suggests that we might have more

possibilities for affine ciphers if we use an alphabet having a prime number of letters. One simple way of doing that is to combine i and j into a single letter and eliminate the infrequently used letters q and z . This gets us down to an alphabet of 23 letters.

8.8.6 Exercise

Let $[m], [b] \in \mathbb{Z}/23\mathbb{Z}$. Define $T: \mathbb{Z}/23\mathbb{Z} \rightarrow \mathbb{Z}/23\mathbb{Z}$ by

$$T([x]) = [m][x] + [b]$$

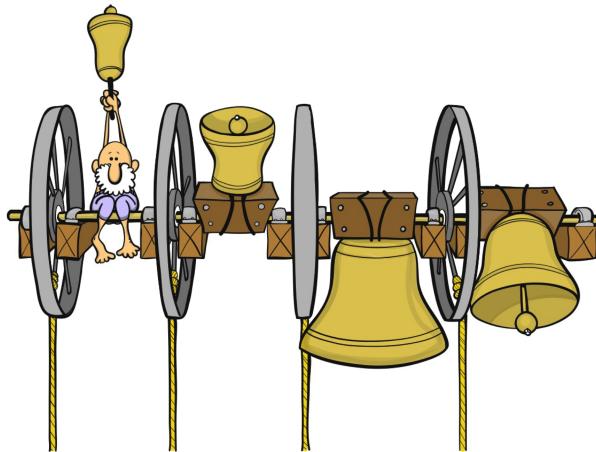
for all $[x] \in \mathbb{Z}/23\mathbb{Z}$.

Prove that T is a bijection if and only if $[m] \neq [0]$.

8.9 Application: Campanology

“To the ordinary man, in fact, the pealing of bells is a monotonous jangle and a nuisance, tolerable only when mitigated by remote distance and sentimental association. [But the change-ringer’s] passion – and it is a passion – finds its satisfaction in mathematical completeness and mechanical perfection, and as his bell weaves her way rhythmically up from lead to hinder place and down again, he is filled with the solemn intoxication that comes of intricate ritual faultlessly performed.

- Dorothy L. Sayers, *The Nine Tailors*.



Cathedral bells¹ in England (and elsewhere) come in different pitches. They are often very large and are permanently installed in a bell tower. They rest upside down and are rung by pulling on ropes which swing the bells around. Typically,

¹This section is an adaptation and development of Section 9.4 of [14] and Section 3.5 of [79]. None of the ideas here are original, though I have adapted them to suit the context of this text.

the bells are rung in a some order (called a “round”) where each bell is rung exactly once in each round. For example, if there are four bells S, A, T, and B (in order of decreasing pitch), the bells might be rung in the round

S then A then T then B

or in the round

A then S then B then T

A bell ringing pattern consists of a sequence of rounds such that no round is repeated. We will write out a pattern by listing a particular round horizontally and listing the rounds vertically, like so:

S	A	T	B	
A	S	B	T	

In this example, there are two rounds (SATB and ASBT) and the bells are rung:

S then A then T then B then A then S then B then T.

The bells are very heavy and so it is not easy to radically alter the round in which they are rung. Usually, only two operations can be used to move from one round to the next: plain changes and cross changes. In a plain change, one pair of adjacent bells has their order swapped. In a cross change, more than one pair of adjacent bells may have their order swapped.

One of the simplest bell-ringing patterns is “the plain lead”. The “S” bell has been colored red, to make it easier to track its position in the round.

S	A	T	B	
A	S	B	T	
A	B	S	T	
B	A	T	S	
B	T	A	S	
T	B	S	A	
T	S	B	A	
S	T	A	B	

We can use permutation groups (Theorem 8.7.27) to better understand the changes. We let $S_n = \text{Perm}\{1, \dots, n\}$ be the permutation group of the numbers $\{1, \dots, n\}$. The group S_4 has 24 elements. To list them we establish some notation conventions. If $\{x, y, z, w\} = \{1, 2, 3, 4\}$, we let the symbol $(xyzw)$ indicate the function $f: \{1, 2, 3, 4\} \rightarrow \{1, 2, 3, 4\}$ where:

$$\begin{aligned} f(x) &= y \\ f(y) &= z \\ f(z) &= w \\ f(w) &= x. \end{aligned}$$

8.9.1

Example

Let $f: \{1, 2, 3, 4\} \rightarrow \{1, 2, 3, 4\}$ defined by $f(1) = 3$, $f(3) = 2$, $f(2) = 4$, and $f(4) = 1$. Then f is represented by the symbols (1324) , (4132) , (2413) , and (3241) .

Similarly, we let the symbol (xyz) denote the function defined by $f(x) = y$, $f(y) = z$, $f(z) = x$, and $f(w) = w$. We let the symbol (xy) denote the function $f(x) = y$, $f(y) = x$, $f(z) = z$, and $f(w) = w$. Finally, the identity is denoted by $\mathbb{1}$. The 24 elements of S_4 are then:

$$\begin{array}{ccccccc} \mathbb{1} & (12) & (13) & (14) & (23) & (24) \\ (34) & (123) & (132) & (124) & (142) & (234) \\ (243) & (134) & (143) & (1234) & (1243) & (1324) \\ (1342) & (1423) & (1432) & (12) \circ (34) & (13) \circ (24) & (14) \circ (23) \end{array}$$

8.9.2

Exercise

Find the group elements in the list above which are equal to the following compositions:

- $(34) \circ (12)$
- $(123) \circ (23)$
- $(243) \circ (132)$

8.9.3

Exercise

In the list above identify the inverse of each element of S_4 .

Given a sequence of bells (such as $ATBS$) and a permutation $f \in S_4$, we can get a new sequence of bells by moving the bell which is in the 1st position to the new position $f(1)$, the bell in 2nd position to the new position $f(2)$, etc.

8.9.4

Example

Consider the sequence $ATBS$ and the element $(1234) \in S_4$. We obtain the sequence $SATB$ by applying the element (1234) to the sequence $ATBS$.

The plain lead on 4 bells:

S	A	T	B
A	S	B	T
A	B	S	T
B	A	T	S
B	T	A	S
T	B	S	A
T	S	B	A
S	T	A	B

can be obtained by starting with the sequence $SATB$ and then repeatedly alternating the application of the elements $g_1 = (12) \circ (34) = (12)(34)$ and $g_2 = (23)$.

Consider now the permutations in S_4 taking the initial row $S A T B$ to each of the rows in the plain lead. We have the following by inspection:

1	S	A	T	B
g_1	A	S	B	T
(1342)	A	B	S	T
(14)	B	A	T	S
$(14)(23)$	B	T	A	S
$(13)(24)$	T	B	S	A
(1243)	T	S	B	A
g_2	S	T	A	B

8.9.5

Theorem

The set $PL = \{g_1, (1342), (14), (14)(23), (13)(24), (1243), g_2\}$ is a subgroup of S_4 .

Recall that by Theorem 5.7.7, we need to show that PL satisfies the closure axiom and the inverses axiom for a group. It may seem like it will be horribly tedious to show that the closure axiom holds since we would have to compose all possible pairs of elements from PL and verify the result is an element of PL . But there's a less tedious way!

We begin with a lemma.

8.9.6

Lemma

Suppose that G is a group and that g_1 and g_2 are elements of G such that g_1^2 (i.e. $g_1 \circ g_1$) and g_2^2 are both equal to the identity 1 . Let H be the set of all possible alternating combinations of g_1 and g_2 . That is,

$$H = \left\{ \begin{array}{l} 1, g_1, g_2 \circ g_1, g_1 \circ g_2 \circ g_1, (g_2 \circ g_1)^2, g_1 \circ (g_2 \circ g_1)^2, \dots, \\ g_2, g_1 \circ g_2, g_2 \circ g_1 \circ g_2, (g_1 \circ g_2)^2, g_2 \circ (g_1 \circ g_2)^2, \dots \end{array} \right\}$$

Then H is a subgroup of G .

Proof. By Theorem 5.7.7, we need only show that given $a, b \in H$, we have $a \circ b \in H$ and given $a \in H$, $a^{-1} \in H$.

Suppose that $a, b \in H$. Then a and b are each an alternating combination of g_1 and g_2 . Thus, $a \circ b$ is some combination of g_1 and g_2 . If b ends (on the

left) with g_1 while a begins (on the right) with g_2 , then $a \circ b$ is the alternating combination of g_1 and g_2 and so $a \circ b \in H$.

⟨ Consider the situation when b ends (on the left) with g_2 while a begins (on the right) with g_1 . ⟩

⟨ Explain what to do when b ends (on the left) with the same term (i.e. g_1 or g_2) that a begins (on the right) with. ⟩

Now suppose that $a \in H$. We will show $a^{-1} \in H$. If $a = \mathbb{1}$, then $a^{-1} = \mathbb{1} \in H$. Otherwise, there is a $k \in \mathbb{N}^*$ such that a is one of the following:

$$(g_2 \circ g_1)^k, g_1 \circ (g_2 \circ g_1)^k, (g_1 \circ g_2)^k, g_2 \circ (g_1 \circ g_2)^k.$$

Notice, then, that the inverse of a is one of the following:

$$(g_1 \circ g_2)^k, (g_1 \circ g_2)^k \circ g_1, (g_2 \circ g_1)^k, (g_2 \circ g_1)^k \circ g_2.$$

⟨ Verify this for yourself by considering the different cases and showing that the relevant combinations produce the identity. ⟩

Since each of these are alternating combinations of g_1 and g_2 , $a^{-1} \in H$. \square

proof of Theorem 8.9.5. Observe that the elements of PL are precisely the elements of S_4 which we can obtain from the identity by alternately composing g_1 and g_2 , beginning with g_1 . Notice that $g_1^2 = g_2^2 = \mathbb{1}$. We will show PL is a subgroup by using Lemma 8.9.6. We will do this by showing that PL is, in fact, the subset H of S_4 which consists of all possible alternating combinations of g_1 and g_2 .

From the definitions, it is clear that $PL \subset H$. We now show that $H \subset PL$.

Suppose that $\sigma \neq \mathbb{1}$ is some element of S_4 which is the alternating composition of g_1 and g_2 some number of times, in some order. We must show that we can write it as the composition of g_1 and g_2 alternately but beginning with g_1 . If g_1 is used first, we are done. Suppose, therefore, that g_2 is used first. From above, we have $\sigma = g_2 \circ g_1 \circ g_2 \circ g_1 \circ g_2 \circ g_1$. If $\sigma = g_2$, we are now done. Assume, therefore, that we may write $\sigma = \sigma' \circ g_2$ where $\sigma' \notin \{g_2, \mathbb{1}\}$ is the alternating composition of g_1 and g_2 , beginning with g_1 . Thus,

$$\sigma = \sigma' \circ g_1 \circ g_2 \circ g_1 \circ g_2 \circ g_1 \circ g_2 \circ g_1.$$

Reading from right to left, some or even all of the initial copies of g_1 and g_2 appearing in σ' now cancel with the terminating copies of g_1 and g_2 appearing in the expression for g_2 . However, since $\sigma' \neq g_2$, we will not cancel the initial copy of g_1 . Thus, σ is the alternating composition of g_1 and g_2 beginning with g_1 , completing the proof. \square

We will see in Section 8.9 that the plain lead is closely connected to other changes having additional structure which can be profitably analyzed using permuta-

tions and group theory. For more on applications of group theory to music, including campanology, see the excellent texts [14] and [79].

8.10 Application: Probability Functions

“The more you think about randomness, the less random things become.” –Persi Diaconis¹

Recall that if X is a set, then an **event space** on X is a set $\mathcal{E} \subset \mathcal{P}(X)$ such that the following hold:

$$(E1) \quad \emptyset \in \mathcal{E}$$

$$(E2) \quad \text{If } A \in \mathcal{E} \text{ then } A^c \in \mathcal{E}$$

$$(E3) \quad \text{If } A_i \in \mathcal{E} \text{ for all } i \in \mathbb{N}, \text{ then } \bigcup_{i \in \mathbb{N}} A_i \in \mathcal{E}.$$

We now define probabilities.

8.10.1

Definition ▶ Probability Function

Let X be a set with event space \mathcal{E} . A function $P: \mathcal{E} \rightarrow [0, 1]$ is a **probability function** if the following hold:

1. $P(\emptyset) = 0$. (“The probability of nothing happening is zero.”)
2. $P(X) = 1$. (“The probability of something happening is one.”)
3. If E_i is an event for all $i \in \mathbb{N}$ and if for all $i, j \in \mathbb{N}$ with $i \neq j$, we have $E_i \cap E_j = \emptyset$, then

$$P\left(\bigcup_{i \in \mathbb{N}} E_i\right) = \sum_{i=1}^{\infty} P(E_i).$$

A triple (X, \mathcal{E}, P) where X is a set, \mathcal{E} is an event space, and P is a probability function is said to be a **probability space**.

The sum on the right of (3) is to be understood as the limit of partial sums, as in Calculus. Incidentally, if \mathcal{A} is a set whose elements are all sets, we say that the elements of \mathcal{A} are **pairwise disjoint** if whenever $A, B \in \mathcal{A}$, either $A = B$ or $A \cap B = \emptyset$. Condition (3) can be summarized as saying that a probability function is additive under pairwise disjoint unions.

¹Persi Diaconis (1945 –) is a prominent statistician and mathematician. He has also performed as a stage magician and has spent considerable effort investigating and debunking the performance, science, and mathematics of ESP experiments. The quote is from [82].

8.10.2

Example

1. Let $X = \mathbb{N}$, $\mathcal{E} = \mathcal{P}(X)$, and define $P: \mathcal{E} \rightarrow [0, 1]$ by:

$$P(E) = \begin{cases} 1 & \text{if } 17 \in E \\ 0 & \text{if } 17 \notin E \end{cases}.$$

Then (X, \mathcal{E}, P) is a probability space.

2. Let $X = \{1, 2, 3, 4, 5, 6\}$, $\mathcal{E} = \mathcal{P}(X)$ and let $P(E)$ be $1/6$ times the number of elements in E , for all $E \in \mathcal{E}$. Then (X, \mathcal{E}, P) is a probability space. (It is called the **uniform probability space** on X .)
3. Let $X = \mathbb{R}$ and let \mathcal{E} be the smallest event space on X containing all the open intervals in \mathbb{R} (see Theorem 5.7.23). For $E \in \mathcal{E}$, define:

$$P(E) = \int_E \frac{1}{\sqrt{2\pi}} e^{-x^2/2}.$$

Then (X, \mathcal{E}, P) is a probability space called the **standard normal probability distribution**. It is challenging to prove that it is a probability space (and even that the integral exists!)

8.10.3

Exercise

- Suppose that (X, \mathcal{E}, P) is a probability space and that $E \in \mathcal{E}$. Prove that $P(E^c) = 1 - P(E)$.

One of the basic tasks in probability is to determine the probability that two events both occur. For instance, what is the probability of rolling a fair die to get a “6” and then rolling it again to get a second “6”? We can model this scenario using Cartesian products. Working somewhat more generally, suppose that (X, \mathcal{E}_X, P_X) and (Y, \mathcal{E}_Y, P_Y) are probability spaces. Given $A \subset X$ and $B \subset Y$, the set $A \times B \subset X \times Y$. If A and B are events, we want the “rectangle” $A \times B$ to be an event, as well. Informally, we’ll interpret $A \times B$ as the event “ A happens, then B happens.” To that end, let \mathcal{E}_0 be the set of all “rectangles” in $X \times Y$; that is $z \in \mathcal{E}_0$ if and only if there exist $A \in \mathcal{E}_X$ and $B \in \mathcal{E}_Y$ such that $z = A \times B$. See Figure 8.20. We define the probability of a product to be the product of the probabilities. That is, define $P: \mathcal{E}_0 \rightarrow [0, 1]$ by $P(A \times B) = P_X(A)P_Y(B)$ for all $A \times B \in \mathcal{E}_0$.

By Theorem 5.7.23, there is a “smallest” event space $\mathcal{E} \subset (X \times Y)$ such that $\mathcal{E}_0 \subset \mathcal{E}$. The events in \mathcal{E} are obtained by taking complements and unions (over \mathbb{N}) of events in \mathcal{E}_0 . The function P can be extended to a function $P: \mathcal{E} \rightarrow [0, 1]$ on all of \mathcal{E} . The way to do this is, for each $E \in \mathcal{E}$, choose a way of writing E in terms of unions and complements of sets in \mathcal{E}_0 . Using the formulas defining a probability function, we can then define $P(E)$ in terms of the values of P on the elements of \mathcal{E} . The main difficulty is to prove that P is well-defined and still satisfies the definition of probability function. How do we know that our choices for how to express E in terms of the elements of \mathcal{E}_0 do not conflict with each other? Is

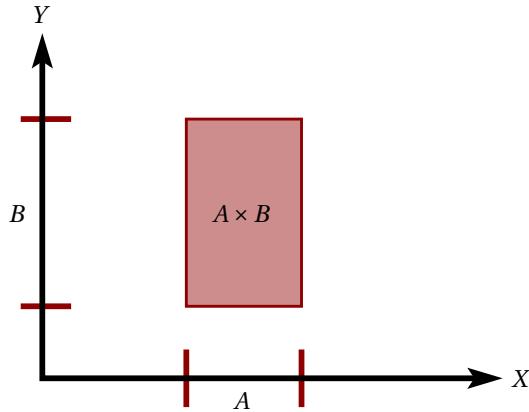


Figure 8.20: The rectangle $A \times B$ in the set $X \times Y$.

it possible that there are different possibilities for $P(E)$ depending on how we express E in terms of the elements of \mathcal{E}_0 ?

One situation where we can easily address these issues is when X and Y are non-empty finite sets. Let \mathcal{E}_X and \mathcal{E}_Y be the power sets of X and Y . If A is a subset of X or Y , let $|A|$ be the number of elements in A . For $A \subset X$ and $B \subset Y$, define $P_X(A) = |A|/|X|$ and $P_Y(B) = |B|/|Y|$, the ratios of the numbers of elements in A and B to the numbers of elements in X and Y , respectively. Notice that if $A \subset X$ and $B \subset Y$, the number of elements in $A \times B$ is $|A \times B| = |A||B|$. Let \mathcal{E} be the power set of $X \times Y$. If for any subset $E \subset X \times Y$, we define $P(E) = |E|/|X \times Y|$ we have a function with the property that $P(A \times B) = \frac{|A|}{|X|} \cdot \frac{|B|}{|Y|} = P(A)P(B)$.

When we apply the preceding considerations to problems derived from the natural or social sciences, we must of course be careful that our choice of probability function corresponds to the world we are modelling. For instance, multiplying the probabilities of subsequent events A and B is only a valid way of calculating the probability of the event “First A , then B ” if A and B are “independent.” Informally, this means that whether or not event B occurs is unaffected by whether or not A occurs. The U.S. economic crisis beginning in 2007-2008 had many causes, but one of them, as argued in [109], may have been the failure of people working in finance to account for dependencies among events. Great care must be taken to ensure the applicability and relevance of mathematical concepts when applying mathematics to subjects, such as the natural sciences and economics, which depend not only on logical deductions from initial assumptions but also on the degree to which the initial assumptions are accurate descriptions of what is actually the case.

8.11 Application: Electrical Circuits

“Before this I was not unacquainted with the more obvious laws of electricity. On this occasion a man of great research in natural philosophy was with us, and excited by this catastrophe, he entered on the explanation of a theory which he had formed on the subject of

electricity and galvanism, which was at once new and astonishing to me.”

– Mary Wollenscraft Shelley, *Frankenstein; or, a modern Prometheus*

Before discussing electrical circuits in particular, we discuss directed graphs and certain types of functions on directed graphs. In Section 2.3 we discussed undirected graphs. Informally, the edges in a directed graph have an orientation (i.e. an arrow or direction), whereas the edges in an undirected graph do not. We can formalize this by making an edge e into an ordered pair (v, w) where $v, w \in V$; in an undirected graph the corresponding edge would instead be the set $\{v, w\}$. More formally, a **directed graph** $G = (V, E)$ consists of a set V of vertices and a set of edges E such that for each edge $e \in E$, there exist vertices $v, w \in V$ so that $e = (v, w)$. The vertex v is the **initial endpoint** of e and the vertex w is the **terminal endpoint** of e .

Let $G = (\mathcal{V}, \mathcal{E})$ be a finite directed graph¹. For an edge e , let $\partial_+ e$ and $\partial_- e$ denote the endpoints of e so that e is directed from $\partial_- e$ to $\partial_+ e$. (In other words, $e = (\partial_- e, \partial_+ e)$.) Given a function $f: \mathcal{V} \rightarrow \mathbb{R}$ we can define a function $\nabla f: \mathcal{E} \rightarrow \mathbb{R}$, called the **gradient** of f by declaring that, for all $e \in \mathcal{E}$,

$$\nabla f(e) = f(\partial_+ e) - f(\partial_- e).$$

Letting $\mathcal{F}(\mathcal{V})$ be the set of functions with domain \mathcal{V} and codomain \mathbb{R} and $\mathcal{F}(\mathcal{E})$ the set of functions with domain \mathcal{E} and codomain \mathbb{R} , then $\nabla: \mathcal{F}(\mathcal{V}) \rightarrow \mathcal{F}(\mathcal{E})$ is a function (where $\nabla(f) = \nabla f$.) The function ∇ is analogous to the gradient function from calculus as $\nabla f(e)$ is positive if f increases as we move from $\partial_- e$ to $\partial_+ e$ and negative if f decreases.

We can also turn functions in $\mathcal{F}(\mathcal{E})$ into functions in $\mathcal{F}(\mathcal{V})$ as follows via a function $J: \mathcal{F}(\mathcal{E}) \rightarrow \mathcal{F}(\mathcal{V})$. We call J the **junction function**. To define J , first consider a vertex $v \in \mathcal{V}$. Let $E_+(v)$ denote the set of edges $e \in \mathcal{E}$ such that $\partial_+ e = v$. Similarly, let $E_-(v)$ denote the set of edges $e \in \mathcal{E}$ such that $\partial_- e = v$. The set $E_+(v)$ is the set of edges pointing into v and $E_-(v)$ pointing out of v .

Now suppose that $g \in \mathcal{F}(\mathcal{E})$. Let $J(g) \in \mathcal{F}(\mathcal{V})$ be the function defined, for all $v \in \mathcal{V}$, so that

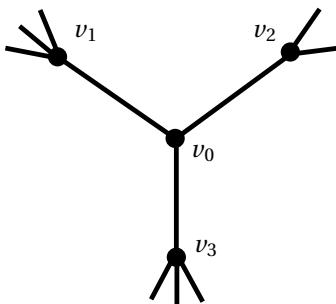
$$J(g)(v) = \sum_{e \in E_+(v)} g(v) - \sum_{e \in E_-(v)} g(v).$$

The function J is the analogue of divergence from vector calculus, as, for a given vertex $v \in \mathcal{V}$, it measures the difference in values of g coming into v and exiting from v .

8.11.1 Exercise

Assume that $G = (\mathcal{V}, \mathcal{E})$ and $G' = (\mathcal{V}, \mathcal{E}')$ are two directed graphs, such that for all $v, w \in \mathcal{V}$, the edge $(v, w) \in \mathcal{E}$ if and only if $(v, w) \in \mathcal{E}'$ or $(w, v) \in \mathcal{E}'$. (That is, the graphs differ only in how directions are assigned to edges.) Suppose that $f \in \mathcal{F}(\mathcal{V})$ and $f' \in \mathcal{F}(\mathcal{V})$ are functions such that for every

¹We have switched to using the script typeface for the set of vertices and edges since we will reserve the non-script V for voltage.

Figure 8.21: A portion of a the graph G from Exercise 8.11.2

- 8.11.1 edge $e = (v, w) \in \mathcal{E}$ and $e' = (v, w)$ or $e' = (w, v)$ in \mathcal{E}' , we have $f(e) = f'(e')$. Let J be the function function for G and J' the junction function for G' . Prove that for every vertex $v \in \mathcal{V}$, we have $J(v) = J'(v)$.

This exercise shows that, at least with regard to the junction function, the directions on the edges of a graph are immaterial.

A function $f \in \mathcal{F}(\mathcal{V})$ is said to be **discretely harmonic** if $J(\nabla f)(v) = 0$ for every $v \in \mathcal{V}$.

8.11.2 Exercise

Suppose that $f, g \in \mathcal{F}(\mathcal{V})$ are both discretely harmonic on a directed graph G . Suppose also that G has a subgraph consisting of four vertices v_0, v_1, v_2, v_3 such that there is an edge between v_0 and each of v_1, v_2, v_3 and there are no other edges incident to v_0 . See Figure 8.21. Finally, assume:

$$\begin{aligned} f(v_1) &= g(v_1) \\ f(v_2) &= g(v_2) \\ f(v_3) &= g(v_3). \end{aligned}$$

Prove that $f(v_0) = g(v_0)$.

8.11.3 Exercise

How far can you generalize Exercise 8.11.2?

Functions with domains the vertices or edges of a graph play an important role in the study of networks. We consider a simple example: the voltage, resistance, and current of an electrical circuit.

Simple electrical circuits can be modelled using directed graphs without loops and with a finite number of vertices. The edges \mathcal{E} of the graph represent wires joining the vertices (or nodes) of the circuit. The direction on the edge is for ease of explanation below and is not marked on circuit diagram below. In the picture some of the wires are pictured with voltage sources or resistors on them. The sources are denoted with two vertical line segments and the resistors with the jagged line segment. The nodes are denoted with solid discs. The resistance

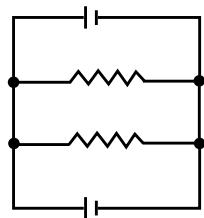


Figure 8.22: We label the sources and resistors with the values of I and Ω respectively. Give each edge of the graph a direction so that the horizontal line segments are directed from left to right.

(measured in Ohms Ω) of each resistor is written near the resistor and the voltage (measured in volts V) generated by each source is written near the source. See Figure 8.22.

The amount of current flowing along a wire in each circuit, this can be modelled by a function $I: \mathcal{E} \rightarrow \mathbb{R}$. For a given edge $e \in \mathcal{E}$, $I(e) \in \mathbb{R}$ is measured in amperes (A). The sign of $I(e)$ indicates the direction of current flow. If $I(e) > 0$, then current is flowing according to the direction of the edge and if $I(e) < 0$ it is flowing in the opposite direction. If $I(e) = 0$ then no current is flowing through the edge. We will assume for simplicity that current flows through every edge of the graph and that every edge of the graph is directed in the direction of current flow along that edge. Hence, $I(e) > 0$ for every edge $e \in \mathcal{E}$.

To each vertex $x \in \mathcal{V}$ of the graph we associate a voltage $V(x)$. Then $V \in \mathcal{F}(\mathcal{V})$ is a function. The **voltage drop** along an edge $e \in \mathcal{E}$ is defined to be $-\nabla V(e)$. An edge with a voltage source and no resistor has negative voltage drop (i.e. the source increases voltage). An edge with a resistor and no source has positive voltage drop (i.e. the resistor decreases voltage). The **resistance** of an edge e is defined to be $\Omega(e) = \nabla V(e)/I(e)$. This ensures that (for our idealized circuit) Ohm's Law ($\nabla V(e) = I(e)\Omega(e)$) holds. In general, Ohm's law is not a mathematical theorem, but rather a physical principle applicable to certain kinds of circuits which is deduced from physical considerations and the precise definitions of volts, ohms, and amperes (the units of current I). In our simplified setting, we have chosen our definitions so that it holds.

Two other physical principles, known as Kirchoff's Laws, also govern the behavior of idealized electrical circuits. Like Ohm's Law, Kirchoff's First Law is not a mathematical theorem, it is a physical principle which is derived from the conservation of electric charge. We'll examine the first of Kirchoff's laws.

Kirchoff's First Law states that vertices do not influence the current:

8.11.4

Kirchoff's First Law

Voltage $V \in \mathcal{F}(\mathcal{V})$ is a discretely harmonic function.

One consequence of this law (as in Exercise 8.11.2) is that if you know the voltages at all vertices of G except for one $v \in \mathcal{V}$, then the voltage at the remaining vertex is completely determined.

8.12 Additional Problems

“I prove a theorem and the house expands:
 the windows jerk free to hover near the ceiling,
 the ceiling floats away with a sigh.”
 – Rita Dove¹, *Geometry*

1. Suppose that $f: X \rightarrow Y$ is a function. A **left inverse** to f is a function $g: Y \rightarrow X$ such that $g \circ f = \text{id}_X$.
 - (a) Prove that f has a left inverse if and only if it is injective
 - (b) Prove that if f has a left inverse, the left inverse is surjective.
 - (c) Give examples of sets X and Y and a function $f: X \rightarrow Y$ such that f has two distinct left inverses.
2. Suppose that $f: X \rightarrow Y$ is a function. A **right inverse** to f is a function $g: Y \rightarrow X$ such that $f \circ g = \text{id}_Y$.
 - (a) Prove that f has a right inverse if and only if it is surjective. (You will need the Axiom of Choice.)
 - (b) Prove that if f has a right inverse, the right inverse is injective.
 - (c) Give examples of sets X and Y and a function $f: X \rightarrow Y$ such that f has two distinct right inverses.
3. Prove that a function $f: X \rightarrow Y$ has an inverse if and only if it has both a left inverse and a right inverse.
4. Prove that there is a bijection $[0, 1] \rightarrow (0, 1)$ (these are both intervals in \mathbb{R}).
5. Suppose that T is a set such that there is a unique element $t_0 \in T$. Let X be any set. Prove that there is a bijection $h: X \rightarrow \mathcal{F}(T, X)$. This exercise suggests that it is possible to define “elements” in terms of “functions.” This is precisely the approach taken in the ETCS axiomatization of set theory.
6. Suppose that X and Y are nonempty sets such that $f: X \rightarrow Y$ is a surjective function. For each $y \in Y$, let $f^{-1}(y) = \{x \in X : f(x) = y\}$. (Notice that we are not claiming f has an inverse function.) Prove that $P = \{f^{-1}(y) : y \in Y\}$ is a partition of X .
7. Suppose that X and Y are nonempty sets such that $f: X \rightarrow Y$ is a function. Define a relation \sim on X by declaring $x_1 \sim x_2$ if and only if $f(x_1) = f(x_2)$.
 - (a) Prove that \sim is an equivalence relation.
 - (b) Let X/\sim be the quotient set. Define $\bar{f}: X/\sim \rightarrow Y$ by letting $\bar{f}([x]) = f(x)$. Prove that \bar{f} is well-defined and injective.

¹Rita Dove (b. 1952) was the Poet Laureate for the United States in 1993. She was both the youngest person and the first African-American in that position. I am grateful to the blog [59] for providing the text of the poem.

- (c) Suppose that $f: X \rightarrow Y$ is surjective. Prove that \bar{f} is a bijection.
8. Suppose that $f: X \rightarrow Y$ is a function from set X to set Y . For a subset $A \subset Y$, let $F(A) = \{x \in X : f(x) \in A\}$. Notice that $F(A) \subset X$.
- Suppose that $A, B \subset Y$. Prove that $F(A \cap B) = F(A) \cap F(B)$.
 - Prove that $F: \mathcal{P}(Y) \rightarrow \mathcal{P}(X)$ is a function.
 - Prove that if f is surjective, then F is injective.
9. Suppose that X and Y are sets and that Q is a set such that there exist functions $q_X: Q \rightarrow X$ and $q_Y: Q \rightarrow Y$. Prove that there is a unique function $h: Q \rightarrow X \times Y$ so that the following diagram commutes:

$$\begin{array}{ccccc} & & Q & & \\ & q_X \swarrow & \downarrow h & \searrow q_Y & \\ X & \xleftarrow{p_X} & X \times Y & \xrightarrow{p_Y} & Y \end{array}$$

10. Let $B = \{0, 1\}$ and let X be any set. Let $\mathcal{F} = \mathcal{F}(X, B)$ be the set of functions from X to B . (Elements of \mathcal{F} are called **characteristic functions** on X .) Prove that there is a bijection $h: \mathcal{P}(X) \rightarrow \mathcal{F}(X, B)$.

Hint: For a subset $A \subset X$, we must define a function $h(A) \in \mathcal{F}$. Functions are usually defined by declaring what they do to elements of the domain, so for each $x \in X$ we must specify $h(A)(x)$. Since the codomain of the function $h(A)$ is to be $\{0, 1\}$, for each $x \in X$ you should specify whether $h(A)(x)$ is to be 0 or 1. Of course, your definition should have something to do with the relationship between x and A , as otherwise h would be a constant function and constant functions are almost never bijections.

11. A function $f: \mathbb{N} \rightarrow X$ (i.e. a sequence in the set X) is **periodic** if there exists $P \in \mathbb{N}$ such that for all $n \in \mathbb{N}$, $f(n + P) = f(n)$. Suppose that $f_1, \dots, f_k: \mathbb{N} \rightarrow \mathbb{N}^*$ are periodic functions. Define $f: \mathbb{N} \rightarrow \mathbb{N}^*$ by

$$f(n) = f_1(n) + f_2(n) + \cdots + f_k(n),$$

for all $n \in \mathbb{N}$. Prove that f is periodic.

12. In the problem, you will construct a proof (due to Northshield [96]) that there are infinitely many primes. You may use the previous problem as well as the fact that every natural number other than 1 has a prime factor.

For a prime p , define a function $f_p: \mathbb{N} \rightarrow \mathbb{N}^*$ by

$$f_p(n) = \begin{cases} 1 & \text{if } n \text{ is a multiple of } p \\ 0 & \text{if } n \text{ is not a multiple of } p. \end{cases}$$

- (a) Prove that for every prime p , the function f_p is periodic.

- (b) Assume there are only finitely many primes p_1, \dots, p_k . Let $f(n) = f_{p_1}(n) + f_{p_2}(n) + \dots + f_{p_k}(n)$ for every $n \in \mathbb{N}$. Observe that $f(1) = 0$. Explain why the previous problem shows that f is periodic and also why this contradicts the fact that every natural number other than 1 is a multiple of a prime.
13. Let \mathcal{C} denote the set of continuous functions with domain and codomain equal to the interval $[0, 1] \subset \mathbb{R}$. Define $G: \mathcal{C} \rightarrow \mathcal{C}$ by
- $$G(f)(x) = \int_0^x f(t) dt.$$
- By appealing to well-known theorems from Calculus, prove that G is injective but not surjective.
14. Suppose that $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ are functions such that $g \circ f: X \rightarrow Z$ is an injection. Must both g and f be injections? If so, prove it. If not, give a counter-example. Must one of them be an injection? Why or why not?
15. Suppose that $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ are functions such that $g \circ f: X \rightarrow Z$ is an surjection. Must both g and f be surjections? If so, prove it. If not, give a counter-example. Must one of them be a surjection? Why or why not?
16. Suppose that $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ are functions such that $g \circ f: X \rightarrow Z$ is a bijection. Must both g and f be bijections? If so, prove it. If not, give a counter-example. Must one of them be a bijection? Why or why not?
17. Use inverse functions to give another proof of Theorem 8.7.10.
18. Suppose that G is a finite directed graph with vertex set V and edge set E . G being directed, means that each edge $e \in E$ has a direction associated to it, and thus has a **head**, denoted $\partial_+ e$ and **tail**, denoted $\partial_- e$. Let $\mathcal{F}(V)$ denote the set of functions $f: V \rightarrow \mathbb{R}$. Let $\mathcal{F}(E)$ denote the set of functions $g: E \rightarrow \mathbb{R}$. As in Section 8.11, define $\nabla: \mathcal{F}(V) \rightarrow \mathcal{F}(E)$ as follows¹. For each $f \in \mathcal{F}(V)$, let $\nabla f: E \rightarrow \mathbb{R}$ be the function defined by
- $$\nabla f(e) = f(\partial_+ e) - f(\partial_- e).$$
- (a) Suppose that G has at least one edge. Prove that ∇ is not injective.
- (b) Suppose that G has exactly three edges, which together form a triangle (like Δ). Prove that ∇ is not surjective.
- (c) Suppose that G has exactly three edges which together form a line segment. Prove that ∇ is surjective.
19. Let X be a set. A **binary operation** on X is a function $\otimes: X \times X \rightarrow X$. Instead of writing $\otimes(a, b)$, we usually write $a \otimes b$. Let G be a group with group operation \circ . Explain how \circ can be thought of as a binary operation.

¹You do not necessarily need to have studied Section 8.11, to do this problem.

20. A **quandle** (X, \triangleleft) consists of a set X and a binary operation (as in the previous problem) \triangleleft on X such that the following hold:

(Q1) For all $a, b, c \in X$, we have

$$(a \triangleleft (b \triangleleft c)) = (a \triangleleft b) \triangleleft (a \triangleleft c)$$

(Q2) For every $a, b \in X$ there exists a unique $c \in X$ such that $a \triangleleft c = b$

(Q3) For every $a \in X$, $a \triangleleft a = a$.

Answer the following, assuming X has at least two elements.

- (a) As a function $\triangleleft: X \times X \rightarrow X$, is \triangleleft surjective?
- (b) Choose some $a \in X$. Define $f: X \rightarrow X$ by $f(x) = a \triangleleft x$. Is f injective? surjective?
- (c) For $(x, y), (a, b) \in \mathbb{R}^2$, define $(x, y) \triangleleft (a, b) = (2x - a, 2y - b)$. Prove that $(\mathbb{R}^2, \triangleleft)$ is a quandle.

21. Suppose that G is a group. Let $\text{AUT}(G)$ be the set of all bijective homomorphisms $f: G \rightarrow G$. Prove that $\text{AUT}(G)$ is a subgroup of $\text{Perm}(G)$.

22. Suppose that G is a group and that H is a subgroup. For each $g \in G$, define $\phi_g: G \rightarrow G$ by $\phi_g(a) = g \circ a \circ g^{-1}$.

- (a) Prove that, for all $g \in G$, the function ϕ_g is an bijective homomorphism.
- (b) Define $\phi: G \rightarrow \text{AUT}(G)$ by $\phi(g) = \phi_g$. Prove that ϕ is a homomorphism.
- (c) Prove that

$$\ker \phi = \{g \in G : \forall a \in G, g \circ a = a \circ g\}.$$

23. Suppose that X is a metric space with metric d_X and Y is a metric space with metric d_Y . Define d so that for all $(x, y), (a, b) \in X \times Y$:

$$d((x, y), (a, b)) = \max(d_X(x, a), d_Y(y, b)).$$

- (a) Prove that d is a metric on $X \times Y$.
- (b) Prove that the coordinate functions $p_X: X \times Y \rightarrow X$ and $p_Y: X \times Y \rightarrow Y$ are continuous.
- (c) Let A be a metric space with metric d_A and suppose that $f: A \rightarrow X \times Y$ is a function. Notice that this means that for all $a \in A$,

$$f(a) = (p_X(f(a)), p_Y(f(a))).$$

Prove that f is continuous if and only if both of the compositions $p_X \circ f$ and $p_Y \circ f$ are continuous.

This result is used in Calculus when considering curves in $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ of the form $f(t) = (x(t), y(t))$ where $t \in \mathbb{R}$. We can evaluate the continuity of such a curve f by simply examining the continuity of the coordinate functions $x = p_X \circ f$ and $y = p_Y \circ f$.

24. Let X be a set. Let \mathcal{F} denote the set of functions $f: X \rightarrow \mathbb{R}$. For $f, g \in \mathcal{F}$, define $f \sim g$ if and only if there exists $M \in \mathbb{R}$ such that $|f(x) - g(x)| \leq M$ for every $x \in X$. Prove that \sim is an equivalence relation.

9 | Proof Techniques II

Key Terms

- Induction
- Complete induction
- Well-ordering principle
- Proof by minimal counter-example
- Recursive definition

“Induction applied to the physical sciences is always uncertain, because it is based on the belief in a general order of the universe, an order which is external to us. Mathematical induction ... is, on the contrary, necessarily imposed on us, because it is only the affirmation of a property of the mind itself.” - Henri Poincaré [101]

In philosophy and science, inductive reasoning is the process of arriving at probable (rather than certain) truths by generalizing from particular examples or premises. For example, the belief that the sun will rise tomorrow is an example of a probable conclusion based on generalizing from the fact that the sun has come up on all previous days. The sun may not, in fact, come up tomorrow. As investment councilors say, “Past performance is no guarantee of future results.” Deductive reasoning, however, results in arriving at certain² truths given true premises. Every proof in this book is an example of deductive reasoning. Perhaps confusingly, mathematical induction is a type of deductive reasoning. Induction is one of our most powerful mathematical tools. It allows us to prove statements about sets having more elements than we can possibly imagine. It comes in several equivalent forms, each of which we explore in the sections that follow.

²Well, as certain as things can be given that “to err is human.”

9.1 Regular old induction

“Is this a seven or a five
 an eight or twenty-two
 What happens in position n
 What happens after it, like when
 n yields to $n + 1$, and then
 $n + 1$ to $n + 2$? ”
 – Eugene Ostashevsky, *The Pirate who does not Know the Value of Pi*
 [98]



During a class field trip, a large number of first-graders are standing in a line. It so happens that the following are true:

- **Base Fact:** The leftmost first-grader knows a secret.
- **Inductive Fact:** If some first-grader knows the secret, then they will share the secret with the child to the right.

Since the leftmost first-grader knows the secret (by the Base Fact), by the Inductive Fact, she will share it with the child to the right, so 1st grader number two knows the secret. Applying the Inductive Fact again, he will share it with the child to the right and so 1st grader number three knows the fact. By repeatedly applying the Inductive Fact, we can be confident that (given enough time) all the first graders in the line will know the secret. Of course, if weren't told that the Base Fact and the Inductive Fact were true, we would not be able to draw that conclusion.

Similarly, suppose that there is an exceedingly tall ladder having equally spaced rungs which is suspended from the side of an exceedingly tall building and hanging some distance off the ground. We would like to be able to climb up the ladder to a certain height. Suppose that the following facts are true:

- **Base Fact:** We can get onto the first rung of the ladder.
- **Inductive Fact:** If we are on the k th rung of the ladder, then it is possible to climb to the $(k + 1)$ st rung of the ladder.

Assuming those two facts then we can climb to whichever rung of the ladder (and thus to whatever height) we want. The Base Fact guarantees that we can get to the first rung of the ladder. The Inductive Fact then guarantees that once we are on the first rung we can make it to the second rung. Applying the second fact again, we see that since we have made it to the second rung, we can also make it to the third rung. Indeed, applying the second fact as many times as we wish allows us to ensure that we can climb to whichever rung of the ladder we wish. Again, unless we know that the Base Fact and the Inductive Fact are true, we cannot know for certain that we can climb to whatever rung of the ladder we wish.

These principles are enshrined in the following theorem whose proof uses Peano's axioms for \mathbb{N} (Section 2.4). The use of Mathematical Induction to prove other theorems, as we do in the remainder of this chapter, is much more important than its proof, however. That is, in common mathematical practice we assume that the following theorem is true and we spend our time showing that the Base Case and Inductive Fact are true in different contexts.

9.1.1

Theorem ▶ Mathematical Induction

Suppose that $n_0 \in \mathbb{Z}$ and that for each integer $n \geq n_0$, $P(n)$ is a statement. Assume also that the following two statements hold:

- (Base Fact) $P(n_0)$ is true.
- (Inductive Fact) If, for some $k \geq n_0$, the statement $P(k)$ is true then $P(k + 1)$ is true.

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

Proof. Let $N = \{n \in \mathbb{Z} : n \geq n_0\}$ and let $A \subset N$ be the set such that $n \in A$ if and only if $P(n)$ is true. We want to show that $A = N$. Recall from Exercise 2.4.8, that $(N, n_0, n \mapsto n + 1)$ satisfies the Peano axioms. We will apply the third Peano axiom to A . To see that this is possible, observe that since $P(n_0)$ is assumed to be true $1 \in A$. Furthermore, we are assuming that if $k \in A$ then $k + 1 \in A$. These two facts are all that are required to show that A satisfies the hypotheses of the third Peano axiom. Thus, the axiom guarantees that $A = N$. Hence, for all $n \in N$, $P(n)$ is true. \square

When we construct a proof by induction we must show that the Base Fact and Inductive Fact are true. The step where we show the Base Fact is true is called the **Base Case**. The step where we show the Inductive Fact is true is called the **Inductive Step**. The assumption " $P(k)$ is true" is called the **inductive hypothesis**. Proving the implication $P(k) \Rightarrow P(k + 1)$ is called the **inductive task**. Often, but not always, our base case will be either $n_0 = 0$ or $n_0 = 1$.

Here are some examples showing how to use induction to prove facts about the

natural numbers. When we use Mathematical Induction, we need to show that the assumptions in Theorem 9.2.1 hold. That is, we need to prove the Base Case and the Inductive Step.

9.1.2

Example

Prove that for every $n \in \mathbb{N}$, $(n+1)/2 \leq n^2$.

Proof. We prove this by induction on n .

Base Case: Let $n = 1$. We observe that

$$(n+1)/2 = 1 = 1^2 = n^2.$$

So, when $n = 1$, $(n+1)/2 \leq n^2$.

Inductive Step: Assume that for some $k \in \mathbb{N}$, $(k+1)/2 \leq k^2$. (This is the inductive hypothesis.) We will show that

$$\frac{(k+1)+1}{2} \leq (k+1)^2.$$

(This is the inductive task.)

To that end, observe that

$$\begin{aligned} (k+1)^2 &= k^2 + 2k + 1 \\ &\geq (k+1)/2 + 2k + 1 \quad (\text{IH applied to } k^2) \\ &\geq (k+1)/2 + 3 \quad (*) \\ &= \frac{k+2}{2} + \frac{5}{2} \\ &\geq ((k+1)+1)/2 \end{aligned}$$

The inequality marked (IH) follows from the Inductive Hypothesis and the inequality marked (*) follows from the fact that the natural number $2k$ is at least 2.

Since we have shown that both the Base Case and the Inductive Step hold, Mathematical Induction affirms that

$$(n+1)/2 \leq n^2$$

for every $n \in \mathbb{N}$.

□

In the previous proof, note the following essential features of a proof by induction.

- We begin by saying that we are doing a proof by induction and state the quantity we are inducting on.
- We prove both the Base Case and the Inductive Step.
- In the Inductive Step, we clearly state the inductive hypothesis and the inductive task.

- We say exactly where we use the Inductive Hypothesis.

A typical feature of a proof by induction is also present in the example above:

9.1.3

Inductive Proof Guideline: When proving the Inductive Step, we begin with an object involving $(k + 1)$ (in this case the quantity $(k + 1)^2$), find a way to express it in terms of k , apply the inductive hypothesis, and then find a way to express the result in terms of $(k + 1)$.

To summarize:

PROOF BY INDUCTION

To show: $P(n)$ is true for all integers $n \geq n_0$.

Structure of Proof: We do a proof by induction on n .

Base Case: Let $n = n_0$.

⟨ Prove that the statement is true when $n = n_0$. ⟩

Inductive Step: Assume that $P(k)$ is true. We will show that $P(k + 1)$ is true.

⟨ Rephrase $P(k + 1)$ as a statement about k . Use the inductive hypothesis (emphasizing where you do so) for $P(k)$ and then do some work to show that $P(k + 1)$ is true. ⟩

Since we have shown both the Base Case and the Inductive Step, mathematical induction implies that $P(n)$ is true for all n . \square

At first glance, it may seem as though a proof by induction involves a logical circle: Isn't the inductive hypothesis assuming what we are trying to prove? The reason why it is not a circular argument is that the inductive hypothesis assumes that the statement is true for *some* integer and, once the base case and inductive steps have been proven, mathematical induction allows us to conclude that the statement is true for *all* integers at least n_0 .

One good application of induction is to show that every integer is either even or one more than an even integer. We used this result back in the proof of Theorem 4.2.1.

9.1.4

Theorem ▶ Even vs. Odd

If $n \in \mathbb{Z}$, then there exists $m \in \mathbb{Z}$ such that $n = 2m$ or there exists $m \in \mathbb{Z}$ such that $n = 2m + 1$, but not both.

¹We actually did this before as Lemma 4.1.1.

²Often in mathematical writing, the word "trick" means a clever argument which avoids hard

If there exists $m \in \mathbb{Z}$ such that $n = 2m$, we say that n is **even**. If there exists $m \in \mathbb{Z}$ such that $n = 2m + 1$, we say that n is **odd**.

Proof. We begin by proving that a number cannot be both even and odd². Suppose, for a contradiction, that $n \in \mathbb{Z}$ has the property that there exists $m, \ell \in \mathbb{Z}$ such that $n = 2m$ and $n = 2\ell + 1$. Algebra shows that

$$2(m - \ell) = 1.$$

Since 1 is a multiple of only itself and -1 (and, in particular, not of 2), this is impossible. Thus, no integer is both even and one more than an even number.

The rest of the proof is consumed with showing that every integer is either even or odd. We first prove this for all $n \in \mathbb{N}^* = \mathbb{N}^*$ by induction on n and then extend the result to all of \mathbb{Z} by a trick².

Base Case: $n = 0$.

When $n = 0$, we can define $m = 0$ so that

$$n = 0 = 2 \cdot 0 = 2 \cdot m.$$

Inductive Step: Assume that for some $k \in \mathbb{N}^*$, there exists $m' \in \mathbb{Z}$ such that $k = 2m'$ or $k = 2m' + 1$. We will show that there exists $m \in \mathbb{Z}$ such that $k + 1 = 2m$ or $k + 1 = 2m + 1$.

There are two cases to consider: when $k = 2m'$ and when $k = 2m' + 1$. First suppose that $k = 2m'$. Let $m = m'$. Then

$$k + 1 = 2m' + 1 = 2m + 1.$$

Thus, we are done in this case.

Second, suppose that $k = 2m' + 1$. Let $m = m' + 1$. Then,

$$k + 1 = 2m' + 2 = 2m.$$

Hence, we are done in this case as well.

By the principle of mathematical induction, for each $n \in \mathbb{N}^*$, there is some $m \in \mathbb{Z}$ so that $n = 2m$ or $n = 2m + 1$.

We next show that if $n \in \mathbb{Z}$ and $n < 0$ then the result also holds. Suppose, therefore, that $n \in \mathbb{Z}$ and $n < 0$. Then $-n \in \mathbb{N}$. By our previous work, there exists $m' \in \mathbb{Z}$ such that $-n = 2m'$ or $-n = 2m' + 1$. If $-n = 2m$, let $m = -m'$. Then

$$n = 2(-m') = 2m.$$

If $-n = 2m' + 1$, let $m = -m' - 1$. Then

$$n = -(2m' + 1) = 2(-m' - 1) + 1 = 2m + 1.$$

Thus, in either case, there is an $m \in \mathbb{Z}$ such that $n = 2m$ or $n = 2m + 1$. \square

work. It signifies to the reader that they are not necessarily expected to have thought of this approach themselves.

9.1.5

Exercise

Prove that for every integer $n \in \mathbb{Z}$ there exists $m \in \mathbb{Z}$ such that $n \in \{3m, 3m+1, 3m+2\}$. Model your proof on that of Theorem 9.1.4.

Use induction to prove the following theorem from Euclid's *Elements*.

9.1.6

Theorem ▶ The Division Algorithm

Suppose that $a, b \in \mathbb{N}$. Prove that there exists $q, r \in \mathbb{N}^*$ such that $b = aq + r$ and $r < a$. (The number q is the **quotient** and r is the **remainder**.)

Sometimes sequences are defined recursively, that is each term of the sequence is defined using previous terms. Induction is often helpful for proving facts about such sequences. We'll study recursively defined sequences more in Section 9.4.

9.1.7

Theorem

Let $x_0 = \sqrt{2}$ and, for $n \geq 0$, let $x_{n+1} = \sqrt{x_n + 2}$. Then for all $n \in \mathbb{N}^*$,

- $x_n < 2$, and
- $x_n < x_{n+1}$.

Proof. We first prove that $x_n < 2$ for all $n \in \mathbb{N}^*$ by induction on n .

Base Case: $n = 0$.

In this case, $x_n = \sqrt{2}$ which is strictly less than 2, as desired.

Inductive Step: Suppose that for some $k \in \mathbb{N}^*$, $x_k < 2$. We show that $x_{k+1} < 2$.

Observe that $x_{k+1}^2 = x_k + 2$. By the inductive hypothesis, we have

$$x_{k+1}^2 < 2 + 2 = 4.$$

Thus, since $f(x) = \sqrt{x}$ is an increasing function,

$$x_{k+1} < 2,$$

as desired. By the principle of mathematical induction, we are done.

Now we show that for all $n \in \mathbb{N}^*$, $x_n < x_{n+1}$ by induction on n .

Base Case: $n = 0$. In this case, $x_1^2 = 2 + \sqrt{2} > 2 = x_0^2$. Thus, taking square roots, we see that $x_1 > x_0$.

Inductive Step: Assume that for some $k \in \mathbb{N}^*$, $x_k < x_{k+1}$. We will show that $x_{k+1} < x_{k+2}$.

Observe that, by the inductive hypothesis and the fact that $f(x) = \sqrt{x}$ is a increasing function,

$$x_{k+1} = \sqrt{x_k + 2} < \sqrt{x_{k+1} + 2} = x_{k+2}.$$

Thus, by the principle of mathematical induction, we have shown that for all $n \in \mathbb{N}^*$, $x_n < 2$ and $x_n < x_{n+1}$. □

9.1.8

Exercise

The Fibonacci numbers are defined as follows. Let $f_1 = f_2 = 1$. For $n \geq 3$, let $f_n = f_{n-1} + f_{n-2}$. Prove that for all $p \geq 2$, we have

$$f_{2p}f_{2p-3} \geq f_{2p-2}f_{2p-1}.$$

Conclude that for all $p \geq 2$, we have

$$\frac{f_{2p}}{f_{2p-1}} \geq \frac{f_{2p-2}}{f_{2p-3}}$$

Induction is often used to count the number of elements in a particular set. We'll use it to count the number of elements in the power set of a finite set. Since we don't yet have a precise definition of "number of elements of a finite set," we technically should defer this example to Chapter 10. However, we've been working with finite sets for most of our lives, so we should have a good enough intuition for what this means. This example involves such a nice use of induction that it is too good to pass up.

9.1.9

Theorem

Suppose that X is a set with exactly $n \in \mathbb{N}^*$ elements. Then $\mathcal{P}(X)$ has exactly 2^n elements.

Before starting a proof by induction, it's good to work out a few examples to get a feel for the pattern. To begin, notice that if X has 0 elements, then $X = \emptyset$ and $\mathcal{P}(X) = \{\emptyset\}$. Thus, $\mathcal{P}(X)$ has one element. Since $1 = 2^0$, the result holds. Now consider something harder. Suppose X has four elements. For the purpose of working our example, we may as well assume that $X = \{1, 2, 3, 4\}$. The power set of X has elements:

$$\begin{aligned} & \emptyset, \\ & \{1\}, \{2\}, \{3\}, \{4\}, \\ & \{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}, \\ & \{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}, \\ & \{1, 2, 3, 4\}. \end{aligned}$$

The goal of induction is to take something difficult and reduce it to something easier. One way to make set simpler is to remove an element. Let's say we remove 4 from $\{1, 2, 3, 4\}$ to get $\{1, 2, 3\}$. The power set of $\{1, 2, 3\}$ has elements:

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

Notice that each of these sets is also a subset of $\{1, 2, 3, 4\}$. Furthermore, each subset of $\{1, 2, 3, 4\}$ that is not one of these can be obtained by inserting "4" into one of these subsets. We see that we can organize the subsets of $\{1, 2, 3, 4\}$ into those that don't contain "4" and those that do and that there must be the same number

of each. Hence, $\mathcal{P}(\{1, 2, 3, 4\})$ has twice the number of elements as $\mathcal{P}(\{1, 2, 3\})$. We use this observation as the basis for our proof.

Proof. We prove this by induction on n .

Base Case: $n = 0$.

In this case, $X = \emptyset$ and $\mathcal{P}(X) = \{\emptyset\}$. Clearly, $\mathcal{P}(X)$ has exactly $1 = 2^0$ elements.

Inductive Step: Assume that there exists $k \in \mathbb{N}^*$ such that every set with exactly k elements has exactly 2^k elements in its power set. Let X be a set with exactly $k + 1$ elements. We will show that $\mathcal{P}(X)$ has exactly 2^{k+1} elements.

Since $k \in \mathbb{N}^*$, $k + 1 \geq 1$. Thus, there exists $x_0 \in X$. Let $X' = X \setminus \{x_0\}$. Then X' has exactly k elements¹. By our inductive hypothesis, $\mathcal{P}(X')$ has 2^k elements.

Partition $\mathcal{P}(X)$ into two subsets Y and Y' . Let $Y' = \{A \in \mathcal{P}(X) : x_0 \notin A\}$ and $Y = \{A \in \mathcal{P}(X) : x_0 \in A\}$.

$\langle \text{ Show that } Y' = \mathcal{P}(X) \rangle$

Notice that for each $A \in Y$, the set $A \setminus \{x_0\}$ is an element of Y' . Conversely, for each $A \in Y'$, the set $A \cup \{x_0\} \in Y$. Since we can match the elements of Y with the elements of Y' , the sets Y and Y' have the same number of elements². Since Y and Y' have no elements in common and since $\mathcal{P}(X) = Y \cup Y'$, we have³ that the set $\mathcal{P}(X)$ has exactly $2^k + 2^k = 2^{k+1}$ elements.

By induction, for every $n \in \mathbb{N}^*$, if X has exactly n elements, then $\mathcal{P}(X)$ has exactly 2^n elements. \square

¹We actually don't know how to prove this at the moment.

²Again, in Chapter 10 we'll be able to give a better proof of this fact.

³This is Exercise 5 in Section 9.9.

9.1.10 Exercise

Adapt the proof of Theorem 9.1.9 to show the following. If X is a set with n elements and Y is a set with m elements, then there are exactly m^n functions $f: X \rightarrow Y$. (Hint: Let m be fixed, but arbitrary and induct on n . You will need to use the fact, which is Exercise 6 in Section 9.9, that if P is a partition of a finite set Z , then the number of elements in Z is equal to the sum of the number of elements in each of the sets in P .)

Here is another counting fact which can be proved using induction.

9.1.11 Theorem

Suppose that P is a convex polygon with $n \geq 3$ sides. Then P can be tiled by $n - 2$ triangles.

Here we say that a polygon is convex if for any two distinct vertices v and w of P , the line segment \overline{vw} is contained inside the polygon (possibly as the union of edges). (Can you prove that this is equivalent to saying that the interior of

the polygon is convex in the sense of Definition 5.7.2?) The idea of the proof is depicted in Figure 9.1. We cut off a vertex, use our inductive hypothesis to triangulate and then put the vertex back. The theorem is also true if we drop the requirement that the polygon be convex; see Theorem 9.2.6.

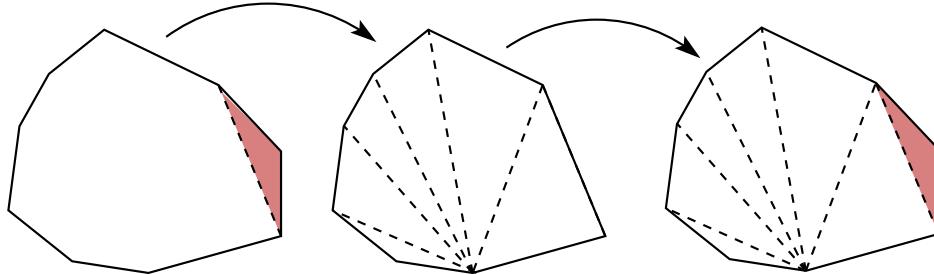


Figure 9.1: Inductively triangulating a $(k+1)$ -gon by cutting off a vertex, triangulating, and then putting the vertex back.

Proof. We induct on the number n of sides of P . We show, in fact, that the triangulations can always be taken to have all their vertices at the vertices of P .

Base Case: $n = 3$.

In this case, P is a single triangle so it can clearly be tiled by $(n-2) = 1$ triangles with all its vertices at the vertices of P .

Inductive Step: Assume that every convex polygon P' with k sides, can be tiled by $(k-2)$ triangles, each with its vertices also a vertex of P' . We show that every polygon P with $k+1 \geq 4$ sides can be tiled by $(k+1)-2 = k-1$ triangles, each with its vertices also a vertex of P .

Suppose that P is a polygon with $k+1$ sides. Let v_0, v_1, v_2 be three consecutive vertices of P . Let e be the edge joining v_0 and v_2 . Since P is not a triangle, this is not an edge of P . Since P is convex, e is contained inside P .

Let T be the triangle (or line segment which is the union of two edges) with vertices v_0, v_1, v_2 . Let P' be the polygon obtained by removing $T \cap P$ from P and replacing it with e . Thus, P' is a polygon with n sides. To see that it is convex, suppose that f is a line segment joining two vertices of P' . The vertices of P' are also vertices of P , so f is inside P . Two line segments in \mathbb{R}^2 are either disjoint, intersect in a single point, or extend to the same line in \mathbb{R}^2 . Since f does not have an endpoint at v_1 , it cannot cross e . Thus, the edge f must be contained in P' . Hence, P' is convex.

By the inductive hypothesis, P' has a triangulation with $n-2$ triangles, each with its vertices at a vertex of P . Since the interior of e does not contain any vertex of the triangulation, the triangulation shares an edge with T . Thus the union of T with that triangulation is a triangulation of P with $(n-1) = (n-2)+1$ vertices, each also a vertex of P .

By induction, we are done. □

The next example concerns permutations. Recall (Definition 8.7.26) that a per-

mutation of a set is simply a bijection of the set to itself. We will show that every permutation of a finite set can be accomplished by performing a sequences of swaps (also known as transpositions). More formally, if X is a set, a **transposition** of X is a bijection $\tau: X \rightarrow X$ such that there exist distinct $a, b \in X$ such that $\tau(a) = b$, $\tau(b) = a$ and for all $x \neq a, b$ we have $\tau(x) = x$. Note that $\tau \circ \tau = \text{id}_X$, so a transposition is always its own inverse.

Before embarking on the proof, it's good to have the general idea. The case when $n = 2$ is pretty easy as there are only two possible permutations of a two element set (including the identity permutation). Let's consider the case when we have a lot of elements. Consider a bijection $f: \{1, \dots, n\} \rightarrow \{1, \dots, n\}$. In Figures 9.2 and 9.3 we depict a situation when $n = 4$. We consider two possibilities: either $f(n) = n$ or $f(n) \neq n$. If $f(n) = n$, as in Figure 9.2, then there's a sense in which f is really just a permutation of $n - 1$ elements (in the case of the figure, 3 elements.) Our inductive hypothesis will allow us to dispose of that case easily. In the case when $f(n) \neq n$, we observe as in Figure 9.3, that there is a transposition $\tau: \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ such that $\tau \circ f(n) = n$. Then we can apply the first case to the bijection $\tau \circ f$. We then have to do a little bit of work to deduce the result for f . The main challenge in writing this argument carefully is that, according to our definitions, if the domain of a function is a set with 4 points (for example), it is not equal to a function whose domain is a set with three points - two functions with different domains are different! To get around this minor annoyance, we work with permutations of the infinite set \mathbb{N} .

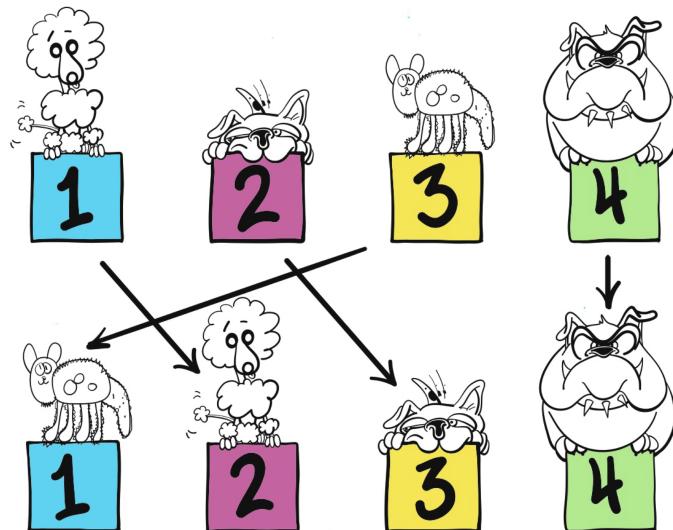


Figure 9.2: An example of a permutation of 4 points which does not move the last point. It is essentially a permutation of the first 3 points.

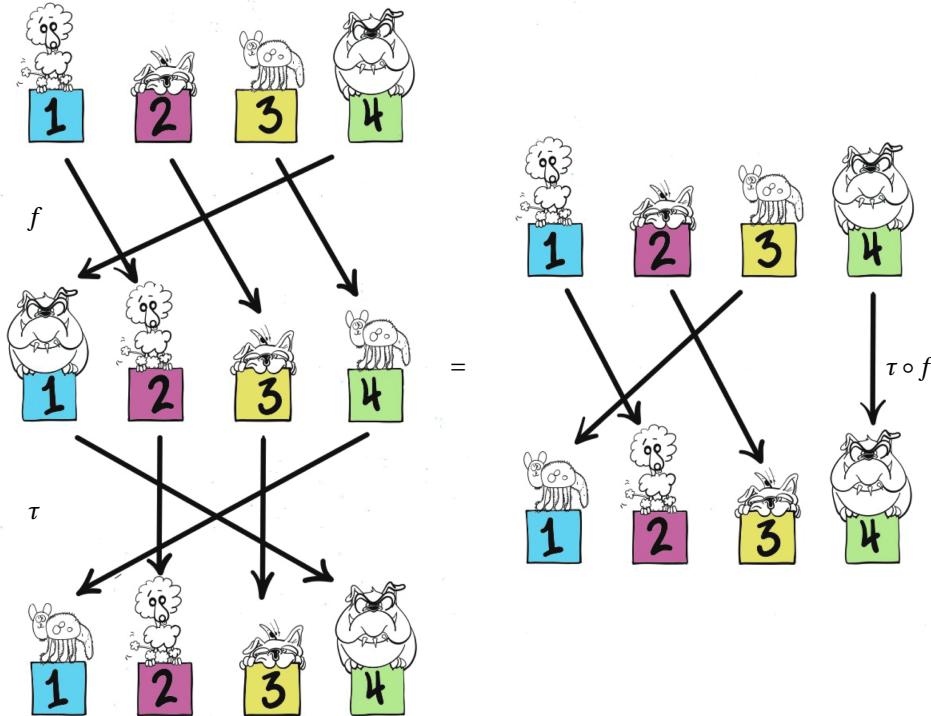


Figure 9.3: On the left, we see the composition of a bijection f which does move the last point with a carefully chosen transposition τ . On the right, we see that the composition is a bijection which does not move the last point.

9.1.12

Theorem

Suppose that $\hat{f}: \mathbb{N} \rightarrow \mathbb{N}$ is a permutation such that there exists $n \geq 2$ so that $\hat{f}(i) = i$ for all $i > n$. Then there exist transpositions $\sigma_1, \dots, \sigma_m$ of \mathbb{N} such that

$$\hat{f} = \sigma_m \circ \dots \circ \sigma_1.$$

Furthermore, none of these transpositions move any number greater than n . That is, for all $i > n$, $\sigma_m(i) = \dots = \sigma_1(i) = i$.

Proof. We induct on n . For convenience, let

$$S(n) = \{\hat{f}: \mathbb{N} \rightarrow \mathbb{N} : \hat{f} \text{ is a bijection, and } \hat{f}(i) = i \text{ for all } i > n\}.$$

Notice that if $n < m$, then $S(n) \subset S(m)$.

Base Case: $n = 2$.

When $n = 2$, there are precisely two functions in $S(n)$. There is the identity function $\text{id}: \mathbb{N} \rightarrow \mathbb{N}$ and there is the transposition $\tau: \mathbb{N} \rightarrow \mathbb{N}$ defined by

$$\tau(i) = \begin{cases} 2 & \text{if } i = 1 \\ 1 & \text{if } i = 2 \\ i & \text{if } i > 2 \end{cases}$$

Observe that $\text{id} = \tau \circ \tau$, and that both id and τ are elements of $S(2)$. Thus, the result holds for the base case.

Inductive Step: Assume that there exists $k \geq 2$ such that whenever $f' \in S(k)$, then f' is the composition of transpositions in $S(k)$. We will show that if $\hat{f} \in S(k+1)$, then \hat{f} is the composition of transpositions in $S(k+1)$.

Let $\hat{f} \in S(k+1)$ be arbitrary. We consider three cases: $\hat{f}(k+1) > k+1$, $\hat{f}(k+1) = k+1$ and $\hat{f}(k+1) < \hat{f}(k+1)$.

Case 1: $\hat{f}(k+1) > k+1$

We show, using a proof by contradiction, that this case cannot occur. Let $i = \hat{f}(k+1)$. Our assumption for this case is that $i > k+1$. By the definition of $S(k+1)$, we have $\hat{f}(i) = i$. But then, $i \neq k+1$ but $\hat{f}(i) = \hat{f}(k+1)$. Hence, \hat{f} is not injective, contradicting the assumption that it is a permutation.

Case 2: $\hat{f}(k+1) = k+1$.

In this case, observe that \hat{f} is a permutation of \mathbb{N} such that for all $i > k$, $\hat{f}(i) = i$. That is, $\hat{f} \in S(k)$. By our inductive hypothesis (with $f' = \hat{f}$) our permutation \hat{f} is the composition of transpositions in $S(k)$. Since $S(k) \subset S(k+1)$, the permutation \hat{f} is the composition of permutations in $S(k+1)$, as desired.

Case 3: $\hat{f}(k+1) < k+1$.

Let $\tau: \mathbb{N} \rightarrow \mathbb{N}$ be the transposition defined by:

$$\tau(i) = \begin{cases} k+1 & \text{if } i = \hat{f}(k+1) \\ \hat{f}(k+1) & \text{if } i = k+1 \\ i & \text{if } i \neq k+1, \hat{f}(k+1) \end{cases}$$

Notice that τ does not move any number greater than $k+1$. Hence, $\tau \in S(k+1)$. Furthermore, $\tau \circ \hat{f}$ is a bijection since the composition of bijections is a bijection. Amazingly, we also have

$$\tau \circ \hat{f} \in S(k).$$

(Check this!)

By our inductive hypothesis, applied to the permutation $f' = \tau \circ \hat{f}$, there exist transpositions $\sigma_1, \dots, \sigma_m \in S(k) \subset S(k+1)$ so that

$$\tau \circ \hat{f} = \sigma_m \circ \dots \circ \sigma_1.$$

Apply τ to the left of both sides of the equation and recall that $\tau \circ \tau = \text{id}$ since τ is a transposition. Thus,

$$\hat{f} = \tau \circ \sigma_m \circ \dots \circ \sigma_1.$$

Hence, \hat{f} is the composition of transpositions in $S(k+1)$.

By induction, the theorem is proven. □

For the sake of completeness, we now show how to convert Theorem 9.1.12 into a theorem about permutations of finite sets. First, some notation. If $p: \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ is a permutation for some $n \in \mathbb{N}$, define $\hat{p}: \mathbb{N} \rightarrow \mathbb{N}$ by

$$\hat{p}(i) = \begin{cases} p(i) & \text{if } i \leq n \\ i & \text{if } i > n \end{cases}.$$

We call \hat{p} the **extension** of p . On the other hand, if $g: \mathbb{N} \rightarrow \mathbb{N}$ is a permutation such that there exists $n \in \mathbb{N}$ with $g(i) = i$ for all $i \geq n$ (that is, g does not move any number greater than n), define

$$g|_n: \{1, \dots, n\} \rightarrow \{1, \dots, n\}$$

to be the function where $g|_n(i) = g(i)$ for all $i \leq n$. It is straightforward to show that $g|_n$ is also a permutation. We call $g|_n$ the **n th restriction** of g . The next exercise deduces some basic properties and is another opportunity to prove two functions are equal.

9.1.13 Exercise

Prove the following:

1. If $p: \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ is a permutation, then $\hat{p}|_n = p$.
2. If $g: \mathbb{N} \rightarrow \mathbb{N}$ is a permutation that does not move any number greater than n , then $(\widehat{g|_n}) = g$.
3. If g_1, g_2 are permutations of \mathbb{N} that do not move any number greater than n , then

$$(g_2 \circ g_1)|_n = (g_2|_n) \circ (g_1|_n).$$
4. If g_1, g_2, \dots, g_m are permutations of \mathbb{N} that do not move any number greater than n , then

$$(g_m \circ \dots \circ g_1)|_n = (g_m|_n) \circ \dots \circ (g_1|_n).$$

(Hint: Use induction on m .)

9.1.14 Theorem

Suppose that $f: \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ for some $n \geq 2$ is a permutation. Then there exist transpositions τ_1, \dots, τ_m of $\{1, \dots, n\}$ such that

$$f = \tau_m \circ \dots \circ \tau_1.$$

Proof. Suppose that $n \geq 2$ and that $f: \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ is a permutation. Let $\hat{f}: \mathbb{N} \rightarrow \mathbb{N}$ be the extension of f . Since $\hat{f}(i) = i$ for all $i > n$, we may apply Theorem 9.1.12 to \hat{f} . We conclude that there exist transpositions $\sigma_1, \dots, \sigma_m$ of \mathbb{N} such that none move any number greater than n and so that

$$\hat{f} = \sigma_m \circ \dots \circ \sigma_1.$$

For each $j \in \{1, \dots, m\}$, let $\tau_j = (\sigma_j)|_n$. Each τ_j is a permutation. Furthermore, since $\tau_j(i) = \sigma_j(i)$ for all $i \leq n$, each τ_j is a transposition of $\{1, \dots, n\}$. By the exercise above,

$$\begin{aligned} f &= (\widehat{f})|_n \\ &= (\sigma_m \circ \dots \circ \sigma_1)|_n . \\ &= \tau_m \circ \dots \circ \tau_1 \end{aligned}$$

Thus f is the composition of transpositions of $\{1, \dots, n\}$. \square

9.1.15 Exercise

For each of the following statements, identify the base case, write the inductive hypothesis, and write the goal of the inductive step. You do not need to prove the result and there may be more than one right way to set these up as proofs by induction. Some of the statements are false; some are true and all known proofs are very difficult; some are open problems. Sentences in parentheses are explanatory and are not part of the statement.

1. For every $n \in \mathbb{N}$, $2^{2^n} - 1$ is prime.
2. For every $a, b, c \in \mathbb{N}$ and $n \geq 3$, $a^n + b^n \neq c^n$.
3. (The **crossing number** $c(K)$ of a knot K is the number $n \in \mathbb{N}^*$ such that every diagram depicting K has at least n crossings. Given two knots K and L , the connected sum $K \# L$ is the knot obtained by first tying K and then tying L .) For every pair of knots K and L , $c(K) + c(L) = c(K \# L)$.
4. For every polygon P in \mathbb{R}^2 , there exist distinct points $p_1, p_2, p_3, p_4 \in P$ such that the square with vertices p_1, p_2, p_3, p_4 has the property that each edge of the square is inside P (except for its endpoints which are on P .)
5. (Given $p \in \mathbb{N}$, the **radical** of p , denoted $\text{rad}(p)$ is the product of distinct prime factors of p . For example, $\text{rad}(24) = 6$.) For every $n \in \mathbb{N}$, there exists $N \in \mathbb{N}$ such that for all $a, b, c \in \mathbb{N}$ where a, b, c share no prime factors, $a + b = c$, and $a \geq N$, we have

$$c > \text{rad}(abc)^{1+1/n}.$$

We conclude with several examples showing the dangers of induction misapplied.

9.1.16 Exercise

Find the logical errors in the following argument purporting to show that every natural number is even.

Clearly, $0 = 2 \cdot 0$ is even. Assume that some natural number is even. Call it $2k$. Then $2(k+1)$ is also a multiple of 2 and so is even. Hence, by induction

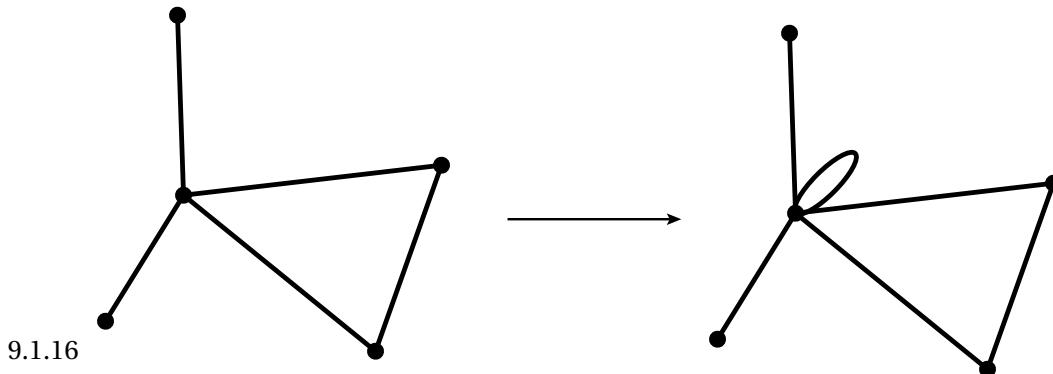


Figure 9.4: An example showing how to insert a loop.

every natural number (as well as zero) is even.

9.1.17 Exercise

Find the logical errors in the following argument purporting to show that every non-empty graph with finitely many vertices and edges can be drawn in the plane so that the edges don't cross. See Figure 9.4 for an example.

We induct on the number of edges. If the number of edges of a graph G is zero, then G consists just of vertices. If there are $n \in \mathbb{N}$ vertices, we can place them at the points $(1, j) \in \mathbb{R}^2$ for $j \in \{1, \dots, n\}$. Clearly none of the edges of G cross since there are no edges.

Now suppose that whenever G is a graph with finitely many edges and vertices and having k edges, then G can be drawn in the plane so that the edges don't cross. Let v be a vertex of G . Very close to v , we can insert a very short edge with both endpoints at v , forming a loop, so that the edge doesn't cross any of the other edges of G . The new graph, call it G' , has $k + 1$ edges and finitely many vertices. We have drawn it in the plane so that no edges cross. Thus, by induction, every graph with finitely many edges and vertices can be drawn in the plane so that edges don't cross.

9.1.18 Exercise

Suppose that $G = (V, E)$ is a finite graph with n vertices and with no loops. Assume that $n \geq 3$. If v is a vertex of the graph G its **valence** is equal to the number of edges having an endpoint at v . We say that G is a **cycle** if the vertices can be numbered v_1, \dots, v_n so that for each $i \in \{2, \dots, n - 1\}$, the vertex v_i is joined by edges to the vertices v_{i-1} and v_{i+1} and is not joined by an edge to any other vertex. Consider the following claim. Find the error in the purported proof and then find a counter-example to the claim. (Hint: You'll need to have $n \geq 6$ before you can find a counter-example.)

Claim²: If $G = (V, E)$ is a finite graph with $n \geq 3$ vertices having the property that the valence of every vertex is 2 then G is a cycle.

We prove this by induction on n . If $n = 3$, let v_1 , v_2 , and v_3 be the vertices of G . Since each has valence equal to 2 and there are no loops, each one of v_1 , v_2 , and v_3 is joined by edges to the other two. Thus, G is a cycle.

Now suppose that the claim is true for some $k \in \mathbb{N}$ with $k \geq 3$. That is, assume that every finite graph G' with k vertices, each having valence 2, and without loops is a cycle. Let G be a finite graph with $k + 1$ vertices, each having valence 2, and having no loops. We will prove that G is a cycle.

9.1.18

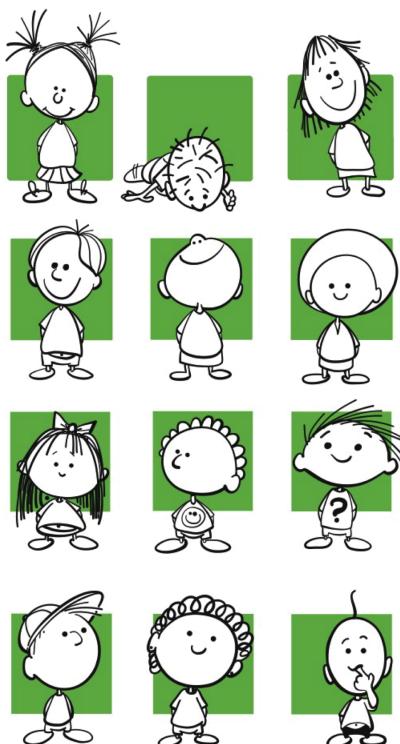
Notice that $k + 1 \geq 4$. Let v be a vertex of G . Since G has no loops and v has valence 2, there exist vertices u and w joined by edges to v . Let G' be the graph obtained from G by removing the vertex v , removing the edges joining v to u and w , and adding in an edge joining u to w . Notice that G' has k vertices, is without loops, and that every vertex has valence 2. By our inductive hypothesis, G' is a cycle.

We can obtain G from G' by inserting the vertex v into the edge of G' joining u to w . Since G' was a cycle and inserting a vertex into an edge of a cycle still preserves the fact that the graph is a cycle, G is a cycle.

¹This example is due to P.D. Johnson and Arthur Schlam and is taken from [10].

9.2 Complete Induction

"[T]ravellers traditionally count like this: one, two, three, many and people assume this means they can have no grasp of higher numbers. They don't realize that many can *be* a number. As in: one, two, three, many, many-one, many-two, many-three, *many many*, many-many-one, many-many-two, many-many-three, *many many many*, many-many-many-one, many-many-many-two, many-many-many-three, LOTS." – Terry Pratchett, *Men At Arms*



A classroom of first-graders lines up and then is made to sit in rows with the first children in line sitting in the first row. After they sit, the first-grader in the very first spot of the very first row learns a secret. First-graders are inquisitive and will talk with any other first-grader nearby, even if they are in a different row. If it is possible for each child to talk with someone to their left and right or directly in front or behind them, then each child will eventually learn the secret. Unlike in the situation when the children are in a row, they do not necessarily learn the secret from the child directly before them in line; they may learn the secret from a child who was far in front of them in line. This is the set-up for Complete Induction (also called "Strong Induction"), a tool which in some instances is more powerful than regular-old-induction. It comes at the cost of a slightly more involved inductive hypothesis. Even though in practice complete induction is more powerful proof technique, its validity follows from regular-old induction (Theorem 9.2.1.)

9.2.1

Theorem ▶ Complete Induction

Suppose that for each $n \in \mathbb{N}$, $P(n)$ is a statement and that the following two statements hold:

- (Base Fact) $P(1)$ is true.
- (Inductive Fact) If, for some $k \in \mathbb{N}$, the statement $P(j)$ is true for all $j \leq k$, then $P(k + 1)$ is true.

Then $P(n)$ is true for all $n \in \mathbb{N}$.

The proof structure of a proof using Complete Induction is very similar to the proof structure for regular old induction. The main difference is in the statement of the Inductive Hypothesis.

PROOF BY COMPLETE INDUCTION

To show: $P(n)$ is true for all $n \in \mathbb{N}$.

Structure of Proof: We do a proof by complete induction on n .

Base Case: Let $n = 1$.

(Prove that the statement is true when $n = 1$.)

Inductive Step: Assume that there is some $k \in \mathbb{N}$ such that for all $j \in \mathbb{N}$ with $1 \leq j \leq k$, the statement $P(j)$ is true. We will show that $P(k + 1)$ is true.

(Rephrase $P(k + 1)$ as a statement about j for some $j \in \{1, \dots, k\}$. Use the inductive hypothesis (emphasizing where you do so) for $P(j)$ and then do some work to show that $P(k + 1)$ is true.)

Since we have shown both the Base Case and the Inductive Step, mathematical induction implies that $P(n)$ is true for all n . □

9.2.2

Most authors will not distinguish between complete induction and regular old induction and will use the word “induction” to refer to either method of proof. In this text we maintain the distinction. When should you use complete induction rather than regular old induction? One good strategy is to start out writing your proof using complete induction. After you’ve written a draft, see if you only ever used the inductive hypothesis when $j = k$. If so, then you can rewrite your proof using regular old induction.

Although you likely already know that natural numbers have prime factorizations, you probably haven’t seen an actual proof. Here is one. Observe that the proof shows that prime factorizations exist, but not that they are unique. That will have to wait for Theorem 9.3.8.

9.2.3

Theorem ▶ Existence of Prime Factorizations

If $n \geq 2$ is a natural number, then there exists $m \in \mathbb{N}$ and prime numbers p_1, \dots, p_m such that

$$n = p_1 \cdot p_2 \cdots \cdot p_m$$

The list of primes p_1, p_2, \dots, p_m is called a **prime factorization** of n .

Proof. We prove the theorem by complete induction on n .

Base Case: $n = 2$.

Since 2 is prime, we can set $m = 1$ and $p_m = 2$ so that 2 has the prime factorization p_m .

Inductive Step: Assume that there is a natural number $k \geq 2$ such that for every $j \in \mathbb{N}$ with $2 \leq j \leq k$, the natural number j has a prime factorization. We will show that $k + 1$ has a prime factorization.

The proof of the inductive step is divided into two cases.

Case 1: $k + 1$ is prime.

In this case, as in the base case, $k + 1$ is its own prime factorization.

Case 2: $k + 1$ is not prime.

By the definition of prime, there exist $a, b \in \mathbb{N}$ such that $k + 1 = ab$ and so that neither a nor b are 1 or $k + 1$.

⟨ Explain why a and b have prime factorizations and use these to construct a prime factorization of $k + 1$. ⟩.

Thus, by complete induction every natural number at least 2 has a prime factorization. \square

Recall that the abstract definition of \mathbb{N}^* is that it is a set (together with a successor function) satisfying the Peano axioms. In Section 2.4, we explained how to define the addition of natural numbers using only the successor function. Similarly, since multiplication of natural numbers can be defined as repeated addition (e.g. 14 is equal to the sum of 2 with itself 7 times), the ability to multiply natural numbers is a consequence of the Peano axioms and judicious choices of definitions. What's definitely not clear from the axioms is why natural numbers can be written in a place value system. For example, how do we know that every number less than 100 can be written in the form $d_0 + d_1 \cdot 10$ for some choice of base-10 digits d_0 and d_1 from the set $\{0, \dots, 9\}$? The next theorem guarantees that we can. Based on our work in Section 2.4, we assume that we know how to add and multiply natural numbers and that we know the numbers $\{0, \dots, 10\}$. (Here 10 is defined to be $9 + 1$.) You will be asked to adapt this theorem to show that natural numbers also have a base 5 representation. Similarly, natural numbers can be represented in any base $b \in \mathbb{N}$ as long as $b \geq 2$.

Before starting the proof, it may help to consider an example. Suppose we know,

somehow, that $k \in \mathbb{N}$ can be written in base-10 place value notation. Perhaps,

$$\begin{aligned} k &= 670,198 \\ &= 8 + 9 \cdot 10 + 1 \cdot 10^2 + 0 \cdot 10^3 + 7 \cdot 10^4 + 6 \cdot 10^5. \end{aligned}$$

To see how to write $k+1$ in base-10 place value notation, observe:

$$\begin{aligned} k+1 &= 1 + 670,198 \\ &= 1 + (8 + 9 \cdot 10 + 1 \cdot 10^2 + 0 \cdot 10^3 + 7 \cdot 10^4 + 6 \cdot 10^5) \\ &= 9 + 9 \cdot 10 + 1 \cdot 10^2 + 0 \cdot 10^3 + 7 \cdot 10^4 + 6 \cdot 10^5. \end{aligned}$$

Since 9 is a base-10 digit, this is valid base-10 place value notation for $k+1$. On the other hand, what would happen if $k = 970,198$? If we try the same thing, we end up with:

$$\begin{aligned} k+1 &= 1 + 670,199 \\ &= 1 + (9 + 9 \cdot 10 + 1 \cdot 10^2 + 0 \cdot 10^3 + 7 \cdot 10^4 + 6 \cdot 10^5) \\ &= 10 + 9 \cdot 10 + 1 \cdot 10^2 + 0 \cdot 10^3 + 7 \cdot 10^4 + 6 \cdot 10^5 \end{aligned}$$

and that is not valid base-10 place value notation since 10 is not a digit when working base 10. We could define what it means to “carry,” but as you can see in this example we might have to carry across multiple place values. There is a much simpler way! To handle this situation, instead of using the fact that we can write k in base-10 notation, we use the fact that $k+1$ is a multiple of 10 and we can write the number $(k+1)/10$ in base-10 notation. For

$$\begin{aligned} (k+1)/10 &= 67020 \\ &= 0 + 2 \cdot 10 + 0 \cdot 10^2 + 7 \cdot 10^3 + 6 \cdot 10^4. \end{aligned}$$

Multiply by 10 to see that

$$\begin{aligned} k+1 &= 0 + 0 \cdot 10 + 2 \cdot 10^2 + 0 \cdot 10^3 + 7 \cdot 10^4 + 6 \cdot 10^5 \\ &= 670200. \end{aligned}$$

In other words, we have the well-known fact that multiplying by 10 simply appends a 0 to base-10 notation. These two situations (when $k+1$ is not a multiple of 10 and when it is) are key to a proof by complete induction that every natural number can be written in base-10 notation. If we didn’t have to worry about the carrying issue, we could use a proof by regular old induction. But since when $k+1$ is a multiple of 10, the number $(k+1)/10$ is strictly less than k , we need to use complete induction.

9.2.4

Theorem ▶ Place Value Notation

Let $n \in \mathbb{N}^*$. Then there exists $m \in \mathbb{N}^*$ and integers $d_0, \dots, d_m \in \{0, \dots, 9\}$ such that

$$n = d_0 + d_1 \cdot 10 + \dots + d_m \cdot 10^m = \sum_{q=0}^m d_q \cdot 10^q.$$

The numbers d_1, \dots, d_m are the (base 10) **digits** of n .

Proof. We use complete induction on n .

Base Case: If $n = 0$ we choose $m = 0$ and $d_m = n$. The result follows immediately.

Inductive Step: Suppose that there exists $k \in \mathbb{N}^*$, such that for all $0 \leq j \leq k$, there exist $m' \in \mathbb{N}^*$ and $d'_0, \dots, d'_{m'} \in \{0, \dots, 9\}$ such that

$$j = \sum_{q=0}^{m'} d'_q \cdot 10^q.$$

We will prove that there exist $m \in \mathbb{N}^*$ and digits $d_0, \dots, d_m \in \{0, \dots, 9\}$ such that

$$k + 1 = \sum_{q=0}^m d_q \cdot 10^q.$$

Case 1: $k + 1$ is not a multiple of 10.

By our inductive hypothesis, there exists $m' \in \mathbb{N}^*$ and digits $d'_0, \dots, d'_{m'} \in \{0, \dots, 9\}$ so that

$$k = \sum_{q=0}^{m'} d'_q \cdot 10^q.$$

Since $k + 1$ is not a multiple of 10, $d'_0 \neq 9$. Let $d_0 = d'_0 + 1$, $m' = m$, and for $q \in \{1, \dots, m'\}$ and $d_q = d'_q$. Then

$$k + 1 = 1 + d'_0 + \sum_{q=1}^{m'} d'_q \cdot 10^q = \sum_{q=0}^m d_q \cdot 10^q.$$

Thus, the result hold for $k + 1$.

Case 2: $k + 1$ is a multiple of 10.

By assumption, there exists j such that $k + 1 = 10j$. Since $k + 1 \geq 10$, $1 \leq j \leq k$. Thus, we may apply the inductive hypothesis to j .

(Finish this case with an appropriate use of the inductive hypothesis.)

By complete induction, we conclude that the theorem holds for all $n \in \mathbb{N}^*$. \square

9.2.5

Exercise

Prove that every number $n \in \mathbb{N}^*$ has a base 5 representation. That is, there exists $m \in \mathbb{N}^*$ and integers $d_0, \dots, d_m \in \{0, 1, 2, 3, 4\}$ such that

$$n = d_0 + d_1 \cdot 5 + \dots + d_m \cdot 5^m = \sum_{q=0}^m d_q \cdot 5^q.$$

Here is a geometric example. Back in Theorem 9.1.11 we proved that the interiors of convex polygons can be triangulated with a certain number of edges. Here we

prove that we can drop the hypothesis that the polygon be convex.

9.2.6

Theorem

Suppose that $P \subset \mathbb{R}^2$ is a polygon with $n \geq 3$ vertices and edges. Then there is a triangulation of the interior of P using $n - 2$ triangles and such that every vertex of the triangulation is also a vertex of P .

As we expect, we'll use complete induction to prove the theorem. The key idea for the inductive step is that we can find a line segment joining two vertices v_0 and v_1 of the polygon which is contained completely inside the polygon (and is not one of its edges.) We'll use this line segment to cut the polygon into two smaller polygons to which we can apply the inductive hypothesis. The left side of Figure 9.5 depicts an example of such an edge and the right side gives an idea of part of the argument we use to show such an edge always exists. You are encouraged to draw your own pictures to help understand the proof. As you go through the proof, you'll encounter several assertions (which we mark with a *) about how polygons divide the plane into two pieces. This is a special case of a deep theorem from topology called the Jordan Curve Theorem. In our settings, the assertions should all be quite plausible; however a totally rigorous proof does require more background.

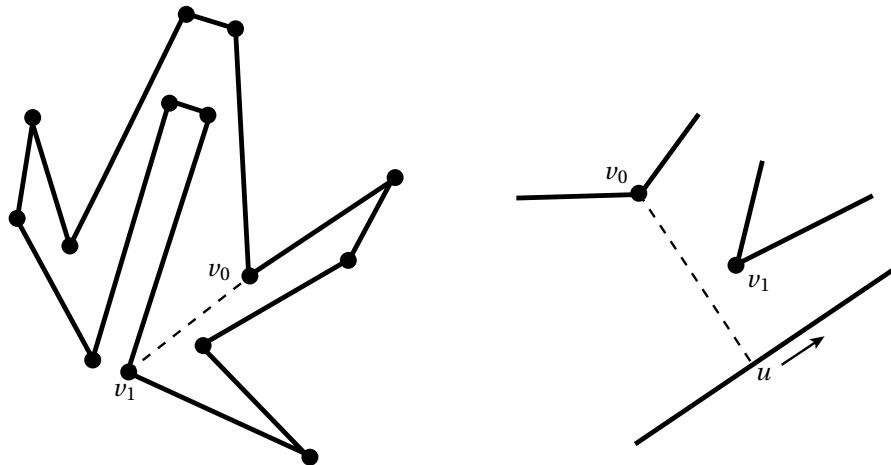


Figure 9.5: On the left is an example of an edge we can use to cut a polygon into two smaller polygons. On the right is a detail of how we might find such an edge in general.

Proof. We use complete induction on n .

Base Case: $n = 3$.

Let P be a polygon with 3 vertices. Then P is a triangle and so is its own triangulation with $1 = n - 2$ triangles and each vertex of the triangulation is also a vertex of P .

Inductive Step: Assume that there is some $k \in \mathbb{N}$ with $k \geq 3$ such that for all $j \in \mathbb{N}$ with $3 \leq j \leq k$, every polygon P' with j vertices has a triangulation with $j - 2$ triangles and with every vertex of the triangulation also a vertex of P' . Suppose that P is a polygon with $k + 1$ vertices. We show that P has a triangulation with $k - 1$ triangles and with each vertex of the triangulation also a vertex of P .

Claim: There exist vertices v_0 and v_1 of P such that the line segment $\overline{v_0 v_1}$ from v_0 to v_1 lies interior to P , is not an edge of P , and does not intersect any vertices of P other than v_0 and v_1 .

Assume the claim for the moment. We will show why P satisfies the conclusion of the theorem.

The line segment $\overline{v_0 v_1}$ divides P into two polygons* P_a and P_b . The interiors of P_a and P_b are disjoint* since $\overline{v_0 v_1}$ is interior to P . Let n_a and n_b be the number of vertices of P_a and P_b respectively. Since P_a and P_b share only the vertices v_0 and v_1 we have

$$n_a + n_b - 2 = k + 1$$

Since $\overline{v_0 v_1}$ is not an edge of P , P_a and P_b each have at least three sides. Thus, $n_a \leq k$ and $n_b \leq k$.

By our inductive hypothesis, P_a has a triangulation \mathcal{T}_a with $n_a - 2$ triangles and with the property that each vertex of \mathcal{T}_a is also a vertex of P_a . Likewise, P_b has a triangulation \mathcal{T}_b with $n_b - 2$ triangles and with the property that each vertex of \mathcal{T}_b is also a vertex of P_b . Observe that this implies that $\overline{v_0 v_1}$ is an edge of both P_a and P_b . Since P_a and P_b have disjoint interiors and since the interior of $\overline{v_0 v_1}$ is disjoint from the vertices of P , every triangle in \mathcal{T}_a is disjoint from every triangle in \mathcal{T}_b , except that one triangle in \mathcal{T}_a shares the edge $\overline{v_0 v_1}$ with one of the triangles in \mathcal{T}_b . Thus, $\mathcal{T} = \mathcal{T}_a \cup \mathcal{T}_b$ is a triangulation of P having all of its vertices at the vertices of P . The triangulation \mathcal{T} has

$$n_a + n_b - 2 = k + 1$$

vertices, as desired. Subject to proving the claim, complete induction guarantees that the result holds whenever $n \geq 3$.

Proof sketch of Claim: We give a rather intuitive proof sketch of the claim. Making this precise requires more results from topology or analysis. Let v_0 be any vertex of P and let R be a ray in \mathbb{R}^2 extending from v_0 , disjoint from the edges of P having v_0 as an endpoint and which begins by heading into the interior of P . Since P is a closed polygon, the ray R must eventually leave P . In particular, the ray R must intersect some point of P other than v_0 . The

ray R may intersect P in isolated points contained in the interior of edges, in vertices of P , or in complete edges of P . If R contains an edge E of P , then R also contains the endpoints of E . Since P has only finitely many vertices and edges, there exists a point u of P other than v_0 which is the point of $R \cap P$ closest to v_0 . Furthermore, u is either an interior point of an edge E of P or is a vertex of P . If it is a vertex of P , set $v_1 = u$ and we are done.

Assume, therefore, that u is interior to an edge E of P . See the right side of Figure 9.5. Observe that E is not contained in R and is not one of the edges adjacent to v_0 . Since $k+1 \geq 4$, the edge E shares at most one endpoint with an edge adjacent to v_0 . Now, begin rotating R around v_0 , so that the point $u = R \cap E$ slides along E . If E shares an endpoint with an edge adjacent to v_0 , choose the direction of the rotation so that u moves toward the other endpoint of E . Consider the line segment $\overline{v_0u}$. This line segment begins with its interior contained inside of P . If we rotate R so that u gets all the way to an endpoint of E without having the interior of $\overline{v_0u}$ intersect a point of P , then we may set v_1 to be the endpoint of E that u reaches and we are done. (This relies on the fact that we ensured that this endpoint was not an endpoint of an edge adjacent to v_0 .) If at some point the line segment $\overline{v_0u}$ has its interior intersect P , let $u_0 \in E$ where $\overline{v_0u}$ first has its interior intersect P . When it does so, the intersection of $\overline{v_0u_0}$ consists of vertices of P and entire edges of P (none of which is adjacent to v_0). Thus, the point v_1 in the interior of $\overline{v_0u_0}$ and which lies on P is a vertex of P . The line segment $\overline{v_0v_1}$ then satisfies the conclusion of the claim. This concludes the proof sketch of the claim. \square

9.2.7

Exercise

For each of the following statements (which are the same as in Exercise 9.1.15) write the inductive hypothesis as you would for a proof by complete induction. You do not need to prove the result and there may be more than one right way to set these up as proofs by induction. Some of the statements are false; some are true and all known proofs are very difficult; some are open problems. Sentences in parentheses are explanatory and are not part of the statement.

1. For every $n \in \mathbb{N}$, $2^{2^n} - 1$ is prime.
2. For every $a, b, c \in \mathbb{N}$ and $n \geq 3$, $a^n + b^n \neq c^n$.
3. (The **crossing number** $c(K)$ of a knot K is the number $n \in \mathbb{N}^*$ such that every diagram depicting K has at least n crossings. Given two knots K and L , the connected sum $K \# L$ is the knot obtained by first tying K and then tying L .) For every pair of knots K and L , $c(K) + c(L) = c(K \# L)$.
4. For every polygon P in \mathbb{R}^2 , there exist distinct points $p_1, p_2, p_3, p_4 \in P$ such that the square with vertices p_1, \dots, p_4 has the property that each edge of the square is inside P (except for its endpoints which are on P .)

5. (Given $p \in \mathbb{N}$, the **radical** of p , denoted $\text{rad}(p)$ is the product of distinct prime factors of p . For example, $\text{rad}(24) = 6$.) For every $n \in \mathbb{N}$, there exists $N \in \mathbb{N}$ such that for all $a, b, c \in \mathbb{N}$ where a, b, c share no prime factors, $a + b = c$, and $a \geq N$, we have

$$c > \text{rad}(abc)^{1+1/n}.$$

The next two examples concern graphs. Recall from Section , that a graph G is connected if for any two vertices $a, b \in G$ there exists a path in G from a to b . A **tree** is a connected graph T such that for every edge e of T , if we remove e from T (leaving its endpoints) then the graph becomes disconnected. A vertex v in a tree T is called a **leaf** if there is exactly one edge of T having v as an endpoint.

9.2.8

Theorem

Suppose that T is a finite tree with $E(T) \geq 1$ edges. Then T has at least 2 leaves.

Proof. We induct on the number $E(T)$ of edges of T .

Base Case:

(State and prove the Base Case)

Inductive Step: Suppose that there exists $k \geq 1$ such that whenever T' is a tree with $1 \leq E(T') \leq k$ then $E(T')$ has at least two leaves. Let T be a tree with $E(T) = k + 1$ edges. We will show that T has at least two leaves.

(Prove the Inductive Step.)

Thus by complete induction the theorem is true. □

9.2.9

Exercise

Find an infinite tree without any leaves at all.

The basic strategy of the proof of Theorem 9.2.8 can be used to prove the next theorem which is a foundational theorem for low-dimensional topology and geometry. See, for example, [105]. Recall that a finite graph is **planar** if we can place the vertices of the graph as points in \mathbb{R}^2 and place the edges into \mathbb{R}^2 as non-crossing curves. (This placement is called an **embedding** of the graph in \mathbb{R}^2 .) A **face** of an embedded planar graph is the region of the plane bounded by edges and having no vertices or edges in its interior. A finite planar graph has one face which is on the “outside”. Using more sophisticated definitions and results from topology a more precise definition of face could be given. See Figure 9.6.

If G is a graph and if e is an edge of G , we will write $G \setminus e$ for the graph obtained by removing the edge e from the set of edges, but leaving its endpoints in the set of vertices. We also let $V(G)$, $E(G)$, and $F(G)$ be the sets of vertices, edges, and

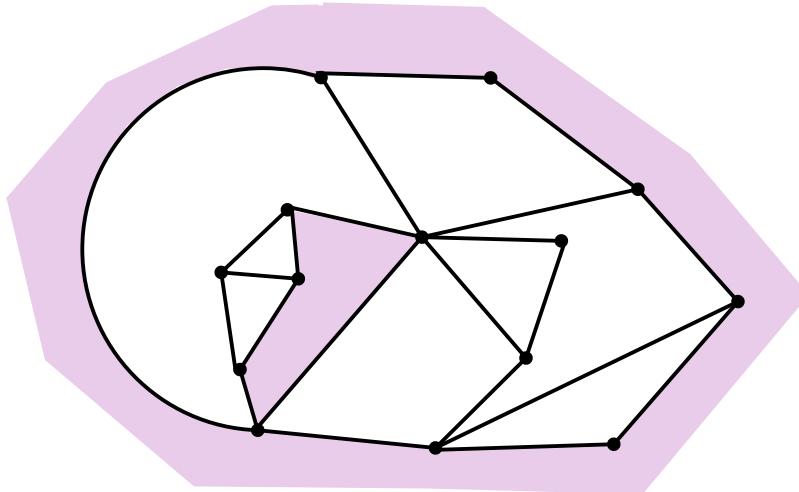


Figure 9.6: An example of a connected non-empty finite planar graph. Two faces have been shaded - one is on the inside of the graph and the other is on the outside. This graph has 10 faces altogether.

faces of G , respectively. We let $|V(G)|$ denote the number of vertices of G ; $|E(G)|$ the number of edges of G ; and $|F(G)|$ the number of faces of G .

9.2.10

Theorem ▶ Euler's Theorem

Suppose that G is a non-empty, connected, finite embedded planar graph. Then

$$V(G) - E(G) + F(G) = 2.$$

Proof. We induct on $|E(G)|$, which is the number of edges of G .

Base Case:

(State and prove the Base Case)

Inductive Step: Assume that there exists $k \geq 0$, such that whenever G' is a non-empty, connected, finite, embedded planar graph having $0 \leq |E(G')| \leq k$, then $|V(G')| - |E(G')| + |F(G')| = 2$. We will prove that if G is a non-empty, connected, finite, embedded planar graph having $|E(G)| = k+1$, then $|V(G)| - |E(G)| + |F(G)| = 2$.

Since $k+1 \geq 1$, the graph G has an edge e . Let Γ be the graph $G \setminus e$. Since the vertices of Γ are the same as the vertices of G , Γ is non-empty. Also Γ has either 1 or 2 connected components, since a path between vertices of G either contains the endpoints of e as adjacent vertices or it does not. (We proved this, assuming an unproved fact, in Theorem 8.4.7.) Observe that $|V(\Gamma)| = |V(G)|$ and $|E(\Gamma)| = |E(G)| - 1$.

Case 1: Γ has one connected component.

In this case, let $G' = \Gamma$. The graph G' is a non-empty, connected, embedded

planar graph. It has $|V(G')| = |V(G)|$ and $|E(G')| = |E(G)| - 1$. Upon removing the edge e from G to form G' two faces of G merge together to form a face of G' . Thus, $|F(G')| = |F(G)| - 1$. Thus, by the inductive hypothesis,

$$\begin{aligned} 2 &= |V(G')| - |E(G')| + |F(G')| \\ &= |V(G)| - (|E(G)| - 1) + (|F(G)| - 1) \\ &= |V(G)| - |E(G)| + |F(G)|. \end{aligned}$$

Case 2: Γ has two connected components.

Let G_1 and G_2 be the two connected components of Γ .

(Finish this step.)

Thus, by complete induction, we are done. \square

9.2.11 Exercise

Go through your proof of Euler's theorem and note places where there are unsubstantiated claims. For each of them, how far can you get towards giving a proof? What would you need to do in order to prove each of them?

Proving this final theorem gives you a chance to adapt the proof of Euler's theorem. If you were to assume that every finite tree is planar (a true fact!) then there is a short proof of this *using* Euler's theorem. Proving it from scratch, however, gives you practice using complete induction.

9.2.12 Theorem

Let T be a finite tree with $|V(T)|$ vertices and $|E(T)|$ edges. Then $|V(T)| - |E(T)| = 1$.

Our final example concerns permutations. Suppose that X is a set with exactly $n \in \mathbb{N}$ elements. A **cycle** is a bijection $\sigma: X \rightarrow X$ with the property that the elements of X can be numbered x_1, \dots, x_n so that for all $i \in \{1, \dots, n-1\}$, $\sigma(x_i) = x_{i+1}$ and $\sigma(x_{n-1}) = x_1$. Figure 9.7 shows an example where $n = 5$.

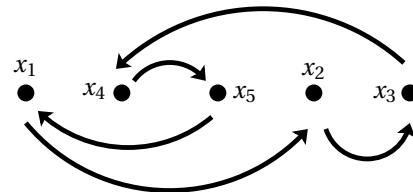


Figure 9.7: An example of a permutation cycle of 5 elements

9.2.13

Exercise

Suppose that X is a set with exactly $n \in \mathbb{N}$ elements and that $f: X \rightarrow X$ is a permutation. Form a graph $\Gamma(f)$ by letting X be the vertex set of $\Gamma(f)$ and declaring there to be an edge between $v, w \in X$ if and only if either $f(v) = w$ or $f(w) = v$. Prove that $\Gamma(f)$ has the property that every vertex has valence 2. Also prove that f is a cycle if and only if $\Gamma(f)$ is connected.

9.2.14

Exercise 9.2.13 explains the use of the word “cycle”. A permutation of a finite set is a cycle if and only if the graph $\Gamma(f)$ contains a cycle traversing every edge. The next theorem shows that every permutation of a finite set can be “broken up” into cycles.

9.2.15

Theorem

Suppose that X is a set with exactly $n \in \mathbb{N}$ elements. Let $f: X \rightarrow X$ be a permutation of X . Then there exists a partition P of X such that for all $A \in P$, the following hold:

- For all $a \in A$, $f(a) \in A$.
- The restriction $f|_A: A \rightarrow A$ is a permutation of A and is a cycle (possibly the identity).

9.3 Well-Ordering Principle

“In the end, I kept going. I learned that it doesn’t matter whether an understanding of difficult material comes naturally to me or not. What matters is that I know how to respond when things get hard. This frame of mind allowed me to recover when the proof of the main theorem in my thesis fell apart and I had to totally abandon the whole project.” -Allison Henrich¹

There is yet another form of induction, called the Well-Ordering Principle. It looks different from the other forms of induction.

9.3.1

Theorem ▶ Well-Ordering Principle

Suppose that $S \subset \mathbb{N}^*$ is non-empty. Then there exists a unique $n \in S$ such that for all $m \in S$, $n \leq m$.

That is, non-empty subsets of the natural numbers have a least element. The corresponding statement for the real numbers is not true. For example, the interval $(0, 1) \subset \mathbb{R}$ has no least element.

¹Allison Henrich is a mathematician known for her creative work with undergraduate researchers. She is an editor of *Living Proof: Stories of Resilience Along the Mathematical Journey* [68], from which this quote is taken.

Proof. We prove the contrapositive: “If $S \subset \mathbb{N}^*$ does not have a least element, then for all $n \in \mathbb{N}^*$, $n \notin S$.” We prove this by induction on n .

Base Case: $n = 0$.

Since $n = 0$ is the least element of \mathbb{N}^* , for all $x \in S$, $n \leq x$. By hypothesis, S does not have a least element. Consequently, $0 \notin S$.

Inductive Step: \langle proof left to reader \rangle .

By induction, for all $n \in \mathbb{N}^*$, $n \notin S$. Hence, $S = \emptyset$.

Finally, we show uniqueness. If n and n' are both least elements of a non-empty subset $S \subset \mathbb{N}^*$, then by the definition of least element, $n \leq n'$ and $n' \leq n$ and so $n = n'$. Thus, every non-empty subset of \mathbb{N}^* has a unique least element. \square

The Well-ordering Principle is used throughout mathematics, often without comment. It shows up in so many different places that it is difficult to give a general outline for how it is used. Here is one common structure, however.

PROOF USING THE WELL-ORDERING PRINCIPLE

To show: There exists $a \in \mathbb{N}^*$ such that properties $P(a)$ and $Q(a)$ hold for a .

Structure of Proof: Let $S = \{n \in \mathbb{N}^* : P(n) \text{ is true}\}$.

\langle Prove that $S \neq \emptyset$. \rangle

Since $S \neq \emptyset$, by the Well-Ordering Principle, S has a least element a .

\langle Prove that $Q(a)$ is true using the fact that a is the least element of S . \rangle

\square

Here are two important applications of the Well-Ordering Principle. The first is the division algorithm. We proved it back in Theorem 9.1.6 using induction. Here is a proof using the Well-Ordering Principle, that is more algorithmic in nature.

9.3.2

Theorem ▶ Division Algorithm

Suppose that $a, b \in \mathbb{N}$. Then there exist unique elements $q, r \in \mathbb{N}^*$ such that $b = qa + r$ and $r < 0$.

The number r in the statement is called the **remainder** upon dividing b by a . To understand the idea behind the statement and proof the theorem, it helps to consider an example.

9.3.3

Example

Let $b = 234589$ and let $a = 168$. Consider how we might divide b by a .

We note that $1000a = 168000 < b$, so we subtract:

$$\begin{array}{r} 234589 \\ - 168000 \\ \hline = 66589 \end{array}$$

Since $66589 \geq a$, we realize that we can take more copies of a out of b .

Before we do that however, notice that we can rewrite this as:

$$b = 1000a + 66589.$$

Taking another copy of a out of b produces the equation:

$$\begin{aligned} b &= 1001a + (66589 - a) \\ &= 1001a + 66421 \end{aligned}$$

Since $66421 \geq a$ we can continue this process.

When will the process stop? When we have an equation of the form:

$$b = qa + r$$

where $q, r \in \mathbb{N}^*$ and $r < a$.

From this example we suspect that the remainder r is the *smallest* non-negative integer such that

$$b = qa + r$$

for some q . This appeal to the *smallest* possibility indicates that we can prove the Division Algorithm using the Well-Ordering Principle.

Proof. We first prove the existence of q, r using the Well-Ordering Principle.

Consider the set of possible remainders:

$$S = \{r' \in \mathbb{N}^* : \exists q' \in \mathbb{N}^* \text{ s.t. } b = aq' + r'\}.$$

Notice that $b = a \cdot 0 + b$, so $b \in S$. Thus $S \neq \emptyset$.

Since $S \subset \mathbb{N}^*$ and $S \neq \emptyset$, S has a least element r . Every element $r' \in S$ has an associated $q' \in \mathbb{N}^*$ such that $b = aq' + r'$. Thus, for our particular r , there exists an $q \in \mathbb{N}^*$ so that $b = aq + r$. Also, by the definition of S , $r \geq 0$. We need only show that $r < a$.

Suppose, for a contradiction, that $r \geq a$. Then $r = a + \rho$ for some $\rho \in \mathbb{N}^*$. Since r, a, ρ are all non-negative, $\rho < r$. Observe that

$$\begin{aligned} b &= aq + r \\ &= aq + a + \rho \\ &= a(q+1) + \rho. \end{aligned}$$

Thus, $\rho \in S$. However, $\rho < r$ and so we have contradicted the choice of r to be the least element of S . Thus, we must have, $r < a$. Hence, there exist q, r satisfying the requirements of the theorem.

We now prove that q, r are unique. Suppose that $q, r, q', r' \in \mathbb{N}^*$, that $r, r' < a$ and that

$$\begin{aligned} b &= aq + r, \text{ and} \\ b &= aq' + r' \end{aligned}$$

Without loss of generality, we may also assume that $q' \leq q$.

Substituting, we arrive at:

$$r' = a(q - q') + r$$

Since $r \geq 0$, we have $r' \geq a(q - q')$. Since $q - q' \geq 0$ and since $r' < a$, we must have $q = q'$. Consequently, arithmetic also shows that $r = r'$, as desired. \square

Here is another example of a proof using the Well-Ordering Principle. Given $x, y \in \mathbb{Z}$, a **linear combination** of x and y is any number c such that there exist $p, q \in \mathbb{Z}$ with $c = px + qy$. The next theorem relates linear combinations to common divisors.

9.3.4

Theorem

Suppose that $x, y \in \mathbb{N}$. There exists a natural number d which is a linear combination of x and y such that whenever c is a linear combination of x and y , then c is a multiple of d .

In fact, it turns out that d is the greatest common divisor of x and y . In our proof, we will construct it as the smallest possible positive linear combination of x and y . Our proof is based on [63, Theorem 23], which is in turn based on a proof in Euclid's *Elements*.

Proof. Let S be the set of *positive* integers which are linear combinations of x and y . Since both $x = x + 0 \cdot y$ and $y = 0 \cdot x + y$ lie in S , the set S is non-empty. By the Well-Ordering Principle, S has a minimal element $d \in S$. We will begin by showing that both x and y are multiples of d . If such is the case, then *every* linear combination of x and y is a multiple of d .

\langle Why? \rangle

By the definition of S , there exist $p, q \in \mathbb{Z}$ such that

$$d = px + qy.$$

Since $x \in S$, $x \geq d$. By the Division Algorithm, there exist $s, r \in \mathbb{N}^*$ such that $x = ds + r$ with $0 \leq r < d$. Then

$$\begin{aligned} r &= x - ds \\ &= x - (px + qy)s \\ &= (1 - ps)x + (-qs)y \end{aligned}$$

Observe that this means that r is a linear combination of x and y . Since $0 \leq r < d = \min S$, we must have $r = 0$. Thus, x is a multiple of d .

(Show that y is also a multiple of d).

□

Theorem 9.3.4 has the following nice corollary.

9.3.5

Corollary

Suppose that $x, y \in \mathbb{N}$ are natural numbers that have no common factor except ± 1 . Then for every $n \in \mathbb{N}$, there exist $a, b \in \mathbb{N}^*$ such that

$$n = ax + by.$$

Proof. Suppose that $x, y \in \mathbb{N}$ have no common factor except ± 1 . Let $n \in \mathbb{N}$.

By Theorem 9.3.4 there exists $d \in \mathbb{N}$ such that there exist $p, q \in \mathbb{N}^*$ with

$$d = px + qy$$

and with the property that every linear combination of x and y is a multiple of d .

Since $x = x + 0 \cdot y$ and $y = 0 \cdot x + y$, both x and y must be multiples of d . Since x and y have no common factor except ± 1 , we must have $d = 1$. Thus,

$$n = (pn)x + (qn)y.$$

Letting $a = pn$ and $b = qn$, we are done. □

9.3.6

The famous psychologist Sigmund Freud was, for a time, obsessed with the numbers 28 and 23. He believed, for example, that he would die at age 51, since $51 = 28 + 23$. Corollary 9.3.5 shows, however, that *every* natural number is some combination of 28 and 23. [51, Chapter 12]

The next theorem provides another opportunity to use the Well-Ordering Principle. Think carefully about what set you want to find the minimal element of. We used this result back in the proof of Theorem 4.3.2.

9.3.7

Theorem ▶ Reduced Fractions

Suppose that $r \in \mathbb{Q}$ and that $r > 0$. Then there exist $a \in \mathbb{Z}$ and $b \in \mathbb{N}$ such that $r = a/b$ and a and b have no common factors other than 1 and -1 .

A proof by contradiction and the Well-Ordering Principle together give rise to another method of proof, sometimes called a “proof by minimal counter-example”. Here is an example, the statement of which is likely well-known to you. For our purposes you should concentrate on the part of the proof where we assume that a certain set is non-empty and show how the Well-Ordering Principle is used to derive a contradiction.

9.3.8

Theorem ▶ Uniqueness of Prime Factorizations

Suppose that p_1, p_2, \dots, p_n and q_1, q_2, \dots, q_m are prime numbers such that

$$p_1 \leq p_2 \leq \cdots \leq p_n,$$

and

$$q_1 \leq q_2 \leq \cdots \leq q_m.$$

If the products are equal, that is, if

$$p_1 p_2 p_3 \cdots p_n = q_1 q_2 \cdots q_m$$

then $n = m$ and for all $i \in \{1, \dots, n\}$, we have $p_i = q_i$.

Our proof is based on [63, Section 2.11].

Proof. Recall that by Theorem 9.2.3 every natural number at least 2 has a prime factorization. Call a number $N \in \mathbb{N}$ with $N \geq 2$ **strange** if there exist distinct finite sequences of primes p_1, \dots, p_n and q_1, \dots, q_m as in the statement of the theorem with

$$N = p_1 p_2 p_3 \cdots p_n = q_1 q_2 \cdots q_m.$$

If there are no strange numbers, then the theorem is true.

Suppose, therefore, that there exists at least one strange number. By the Well-Ordering Principle, there exists a smallest one N . Let p_1, \dots, p_n and q_1, \dots, q_m be the distinct, non-decreasing, sequences of primes whose product is N . If $p_1 = q_1$, then

$$p_2 p_3 \cdots p_n = q_2 \cdots q_m$$

is a strange number strictly smaller than N . Thus, $p_1 \neq q_1$. Without loss of generality, we may assume that $p_1 < q_1$. (Otherwise, switch the labels of p and q .)

(Adapt the previous argument to show that there exists no $j \in \{1, \dots, n\}$ such that $q_1 = p_j$.)

Notice that by the definition of prime number, we must have $n, m \geq 2$. Hence, $q_2 \geq q_1$. Consequently,

$$q_2 \cdots q_m \geq q_1 > p_1.$$

Thus,

$$N - p_1 q_1 = (q_2 q_3 \cdots q_m - p_1) q_1 > 0.$$

The number N is a multiple of both primes p_1 and q_1 , so $N - p_1 q_1$ is as well. In particular, $N \geq 2$. Since $N - p_1 q_1 < N$ it is not strange. Thus, it has a unique factorization into primes, implying that p_1 and q_1 both appear in a single prime factorization for $N - p_1 q_1$. Let r_1, \dots, r_ℓ be the other primes in the prime factorization. Thus,

$$N - p_1 q_1 = p_1 q_1 r_1 r_2 \cdots r_\ell.$$

Hence,

$$N = p_1 q_1 (r_1 r_2 \cdots r_\ell + 1)$$

However,

$$q_1 (r_1 r_2 \cdots r_\ell + 1) = p_2 p_3 \cdots p_n < N.$$

Thus, p_2, p_3, \dots, p_n are the primes in the unique prime factorization of $M = p_2 p_3 \cdots p_n$. The prime q_1 combined with a prime factorization of $r_1 r_2 \cdots r_\ell + 1$ also give a prime factorization of M . Thus, there exists $j \in \{1, \dots, n\}$ such that $q_1 = p_j$. This contradicts our earlier observation.

Thus, there are no strange numbers. \square

Here is the general outline:

PROOF BY MINIMAL COUNTEREXAMPLE

To show: A statement $P(s)$ is true for all elements s of some set S .

Structure of Proof: Assume that the theorem is false. That is, assume that there exists some $s \in S$ so that $P(s)$ is false. We will show that we encounter a contradiction.

(Define some function $c: S \rightarrow \mathbb{N}$ that measures the complexity of the elements of S)

Out of all elements of S which are counter-examples to the theorem, choose one s_0 for which $c(s_0)$ is as small as possible.

(Find a contradiction by either showing how to create a counter-example with strictly small complexity or by using the fact that if $s \in S$ has $c(s) < c(s_0)$ then s is not a counter-example.)

Thus, we encounter a contradiction and so $P(n)$ is true for all $n \in \mathbb{N}$. \square

9.3.9

Exercise

Give a proof of Theorem 9.3.7 using a proof by minimal counter-example.

As a final application of the well-ordering principle, prove the following theorem which was our unproved “fact” when we discussed paths in graphs in Section 8.4.

9.3.10

Theorem

If G is a graph and there is a path in G from a vertex a to a vertex b , then there is such a path α such that if β is any path in G from a to b , then the length of α is less than or equal to the length of β .

9.4 Constructing sequences recursively

“For a hundred years, men beat every possible path – and every path in vain. How was one to locate the idolized secret hexagon that sheltered Him? Someone proposed searching by regression: To locate book A, first consult book B, which tells where book A can be found; to locate book B, first consult book C, and so on, to infinity It is in ventures such as these that I have squandered and spent my years.”

–Jorge Luis Borges, *The Tower of Babel* [21]

We may use a strategy which is very similar to a proof by induction to construct sequences. When we use it we say we have defined a sequence **recursively**. We begin with two examples.

9.4.1 Example

Choose some $\theta \in \mathbb{R}$. Let $x_0 \in S^1$ be the point $(1, 0)$. Assume we have defined $x_n \in S^1$ for some $n \in \mathbb{N}^*$. Let x_{n+1} be the result of rotating x_n counter-clockwise by an angle of θ radians. By induction (but see 9.4.9.4.4 below) we have a sequence (x_n) in S^1 .

9.4.2 Example

Let $x_1 = 1$. Assume that we have defined x_k for every $k \in \{1, 2, \dots, n\}$. Define x_{n+1} as follows

$$x_{n+1} = x_1^2 - x_2^2 + x_3^2 - \dots \pm x_n^2 = \sum_{k=1}^n (-1)^{k-1} x_k^2.$$

By induction, we have a sequence (x_n) in \mathbb{Z} .

9.4.3 Example

Let $f_1 = f_2 = 1$. For $n \geq 3$, let $f_n = f_{n-2} + f_{n-1}$. By induction, we have a sequence (f_n) in \mathbb{N} . It is called the **Fibonacci sequence**.

In the previous examples, we say that each sequence was **constructed recursively**. Before discussing the general principle, we examine this example in some more detail. First of all, observe that we begin with a “base case” where we define the initial term or terms of the sequence. We then assume an inductive hypothesis: The (finite) sequence x_1, \dots, x_k has been defined. Next we define x_{k+1} in terms of the previous values x_1, \dots, x_k . For an arbitrary $n \in \mathbb{N}$, we can then compute x_n by computing all the previous terms of the sequence.

Here is the general method:

DEFINING A SEQUENCE RECURSIVELY

To define: a sequence (x_n) in a non-empty set X so that $x_1 \in X$ and so that (x_n) has a property P .

Structure of Proof: We define (x_n) recursively. Choose some $x_1 \in X$. Assume that we have defined $x_k \in X$ for all $k \in \{1, \dots, n\}$ in such a way that we haven't yet contradicted the possibility of the final sequence having property P . We now define x_{n+1} .

⟨Define $x_{n+1} \in X$ in terms of x_1, \dots, x_n .⟩

By induction (but see the remark below) we have a sequence (x_n) in X .

⟨Verify that f satisfies P .⟩

9.4.4

The astute reader will have noticed that in the previous example (and in the proof structure), we have misapplied induction. Induction is a method of proving (certain kinds of) theorems to be true, but here we have used it to make a definition. In fact, rather than appealing to induction we should appeal to what is known as the “recursion principle”. We defer to [73, Chapter 3] for a statement and proof.

Here is an example of how to use recursive definitions in a proof. Note the use of induction. A version of this theorem was first remarked by Galileo (see [50, pp 40–41].) The Theorem is illustrated in Figure 9.9. Recall that to say a sequence is injective means it has no repeated terms. That is, (x_n) is injective if whenever $x_n = x_m$, we have $n = m$.

9.4.5

Theorem

Suppose that A is a set and that $B \subsetneq A$ is a proper subset. Suppose also that there is an injective function $g: A \rightarrow B$. Then there exists an injective sequence (x_n) in A .

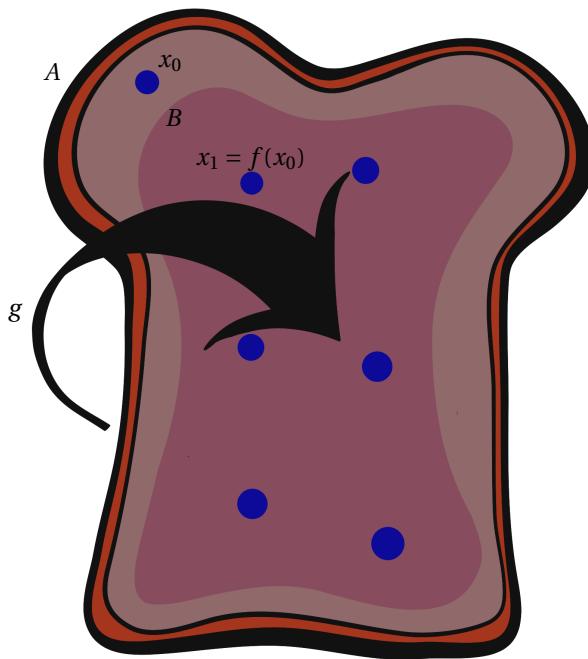


Figure 9.8: An illustration of Theorem 9.4.5. We assume, as on the left, that there is an injection from A to a proper subset $B \subset A$. We need to use that injection to construct a sequence in A having no repetitions.

Before beginning the proof, you may like to try the following exercise:

9.4.6 Exercise

Give an example of a set A and a proper subset $B \subsetneq A$ and an injection $g: A \rightarrow B$. Can you find an example with A being a finite set? Why or why not?

Proof. Let $g: A \rightarrow B$ be an injective function. Since sequences in A are, by definition, functions $\mathbb{N} \rightarrow A$, it suffices to show that there is a sequence (x_n) in A such that for all $n \neq m$, we have $x_n \neq x_m$.

Since $B \subsetneq A$, $A \setminus B \neq \emptyset$. Let $x_0 \in A \setminus B$. Define $x_1 = g(x_0)$. Assume that we have defined x_k for $k \in \{1, \dots, n\}$ so that if $k \geq 2$, then $x_k = g(x_{k-1})$. Define $x_{n+1} = g(x_n)$. By the recursion principle, we have a sequence (x_n) in A such that for all $n \in \mathbb{N}$, we have $x_n = g(x_{n-1})$.

We now show that the sequence (x_n) is injective, using a proof by induction.

Claim: For all $n \in \mathbb{N}^*$ and for all $m \in \mathbb{N}$ such that $m \neq n$, we have $x_n \neq x_m$.

We induct on n , using complete induction.

Base Case: $n = 0$.

Let $m \in \mathbb{N}$. Since $x_m = g(x_{m-1})$, we conclude that $x_m \in B$. We chose $x_0 \in A \setminus B$

and so $x_0 \neq x_m$ as desired.

Inductive Step: Assume that for some $n \in \mathbb{N}^*$ it is the case that for all $k \leq n$ and for all $m \in \mathbb{N}$ with $m \neq k$, we have $x_m \neq x_k$. We will show that for all $m' \in \mathbb{N}$ with $m' \neq n+1$, we have $x_{n+1} \neq x_{m'}$.

Observe that $n+1 \geq 1$. Let $m' \in \mathbb{N}$ with $m' \neq n+1$. Then either $m' < n+1$ or $m' > n+1$. If $m' < n+1$, then $m' \leq n$ and $x_{m'} \neq x_{n+1}$ by the inductive hypothesis (with $k = m'$ and $m = n+1$). Assume, therefore, that $n+1 < m'$. By definition, we have

$$\begin{aligned} x_{n+1} &= g(x_n) \\ x_{m'} &= g(x_{m'-1}) \end{aligned}$$

Since $n+1 < m'$, we have $n < m' - 1$. By the inductive hypothesis, this implies that $x_n \neq x_{m'-1}$. The function g is injective, and so $g(x_n) \neq g(x_{m'-1})$, as desired. By induction we are done. \square

In the proof of the next theorem, you should also construct a sequence recursively. Its statement and proof are more involved than the previous one. The basic idea is that we start with some sequence (a_n) in X , possibly having repetitions, as in Figure 9.9. We want to define a new sequence (x_n) that has all the same terms as (a_n) but without the repetitions. We do this by moving through the sequence (a_n) and skipping any repetitions. We can do this so long as wherever we are in the sequence (a_n) , say at the N th term a_N , there is some term x_m farther down the sequence that we haven't already encountered.

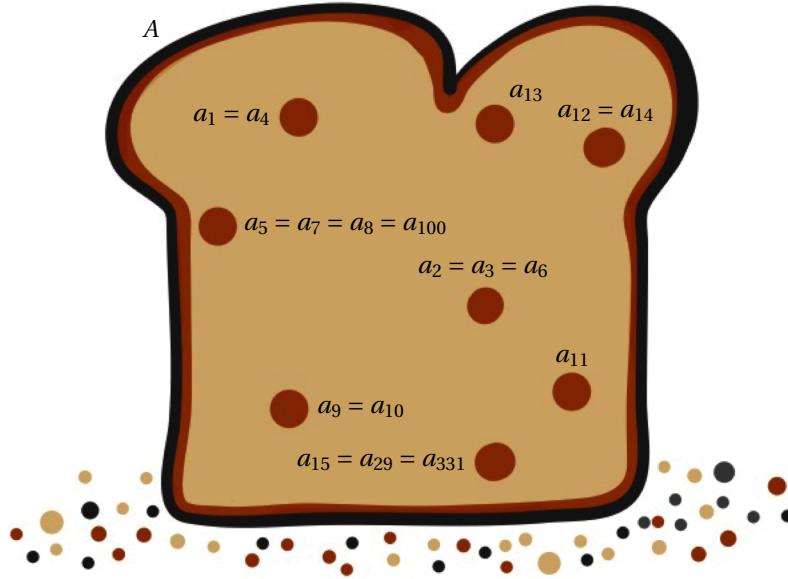


Figure 9.9: An illustration of Theorem 9.4.7. We are given a sequence with repetitions and want to construct a sequence having the same terms, but without repetitions. Only the first terms of the sequence are shown.

9.4.7

Theorem

Suppose that X is a set such that there is a sequence (a_n) in X with the property that for all $N \in \mathbb{N}$, there exists $m > N$ such that $a_m \notin \{a_1, \dots, a_N\}$. Then X contains an injective sequence (x_n) such that for every $n \in \mathbb{N}$ there exists $r \in \mathbb{N}$ such that $x_r = a_n$. (That is, the sequence (x_n) is both injective and has the same range as (a_n) .)

9.5 Other induction methods

“I have heard strange report of thy knowledge in the black art ... This, therefore, is my request, that thou let me see some proof of thy skill
 ... ”

– Christopher Marlowe¹, *The Tragical History of Doctor Faustus*

Is it possible to induct over sets other than the integers? What about the real numbers? Sometimes the answer is “yes,” and sometimes it is “no.”

Induction over the Reals

Here is a version of Mathematical Induction for intervals of real numbers. We closely follow the excellent exposition given by Pete Clark [29].

9.5.1

Definition

Suppose $a < b$. A subset S of the closed interval $[a, b]$ is **inductive** if the following hold:

- (Base Fact) $a \in S$
- (Extending Fact) If $p \in S \cap [a, b]$, then $[a, q] \subset S$ for some $q \in (p, b]$.
- (Closing Fact) For all $p \in [a, b]$, if $[a, p] \subset S$, then $[a, p] \subset S$.

The proof of the next theorem relies on the existence of infima and suprema of real numbers and the completeness of \mathbb{R} . We define and explore those concepts in Chapter 11. Consequently, we omit the proof. However after you have studied those concepts you might like to try to construct your own proof of this theorem (or consult [29]).

9.5.2

Theorem ▶ Principle of Real Induction

If $S \subset [a, b]$ is inductive, then $S = [a, b]$.

¹Christopher Marlowe (1564-1593) was a playwright contemporary to William Shakespeare. In the play, Faustus sells his soul to the devil in return for illicit magical knowledge. The induction methods of this section are the black arts of mathematical magic. Use them with care.

| Proof. Proof omitted. □

As an application, we can prove the Intermediate Value Theorem (IVT). Recall the definition of continuous function (Definition 8.7.33). For real-valued functions defined on a subset $X \subset \mathbb{R}$, we can rephrase it by saying that that a function $f: X \rightarrow \mathbb{R}$ is continuous if and only if for every $p \in X$ and every $\epsilon > 0$, there exists $\delta > 0$ such that $\text{range}(f|_{(p-\delta, p+\delta)}) \subset (f(p)-\epsilon, f(p)+\epsilon)$. Our proof is based on that in [29].

9.5.3

Theorem ▶ Intermediate Value Theorem

Suppose that $f: [a, b] \rightarrow \mathbb{R}$ is continuous and that y is between $f(a)$ and $f(b)$. Then there exists $x \in [a, b]$ such that $f(x) = y$.

Proof. We prove the following claim and then show that it implies the IVT.

Claim: If $f: [a, b] \rightarrow \mathbb{R}$ is continuous and $\text{range}(f) \subset \{-1, 1\}$ and $f(a) = -1$, then $\text{range}(f) = \{-1\}$.

Suppose that $f: [a, b] \rightarrow \mathbb{R}$ is continuous and that $\text{range}(f) \subset \{-1, 1\}$ and that $f(a) = -1$. We will show $f(x) = -1$ for all $x \in [a, b]$. Let $S \subset [a, b]$ be the subset such that $x \in S$ if and only if $f(x) = -1$. By hypothesis, the Base Fact holds. Assume that $p \in S \cap [a, b]$. Let $\epsilon = 1$. Since f is continuous, there exists $\delta > 0$, such that for all $x \in (p - \delta, p + \delta) \cap [a, b]$ we have

$$f(x) \in (f(p) - \epsilon, f(p) + \epsilon) = (-2, 0).$$

(Explain why there exists $q \in (p, b]$ such that $f(q) = -1$ and why this implies that the Extending Fact holds)

(Explain why the Closing Fact holds.)

Thus, by the Principle of Real Induction, the Claim holds.

Finally, we show that the Claim implies the IVT. Let $f: [a, b] \rightarrow \mathbb{R}$ be any continuous function and assume that $f(a) \leq y \leq f(b)$ or that $f(b) \leq y \leq f(a)$. We desire to show that there exists $x \in [a, b]$ such that $f(x) = y$. Suppose, to the contrary that no such x exists. Define $g: [a, b] \rightarrow \mathbb{R}$ by

$$g(x) = \frac{f(x) - y}{|f(x) - y|}$$

for all $x \in [a, b]$. Since g is the quotient of two continuous functions and the denominator is never 0, g is continuous. Observe that $\text{range}(g) \subset \{-1, 1\}$ and that $g(a) = -1$. By the Claim, $\text{range}(g) = \{-1\}$.

(Explain why this is a contradiction to our assumptions)

(Prove the IVT in the case when $f(b) \leq y \leq f(a)$.) □

To point out that there is subtlety involved in the Principle of Real Induction, consider the following examples.

9.5.4

Exercise ▶ (IVT fails over \mathbb{Q})

Let $X = \mathbb{Q} \cap [0, 2]$. For every $x \in X$, define

$$f(x) = \frac{x^2 - 2}{|x^2 - 2|}.$$

Explain why f is continuous on X , but why the IVT fails for this function. Also explain why this shows that we cannot apply the Principle of Real Induction to functions that are defined and continuous only on the rationals.

9.5.5

Exercise

Explain why the following argument shows that we need the Closing Fact in addition to the Extending Fact when using Real Induction. Let $S = [0, 1)$. If $S = [0, 1]$, then we would have $1 < 1$, a contradiction, so Real Induction does not work in this case. Clearly, $0 \in S$ so the Base Fact holds. Show that the Extending Fact also holds, but that the Closing Fact does not.

9.5.6

Exercise

Construct an example to show that when using Real Induction we need the Extending Fact in addition to the Closing Fact.

Clark gives a complete proof of the following classical theorem, but see if you can construct one yourself.

9.5.7

Theorem ▶ Real valued continuous functions on closed, bounded intervals are bounded

Suppose that $f: [a, b] \rightarrow \mathbb{R}$ is continuous. Then there exist $\ell, L \in \mathbb{R}$ such that $\text{range}(f) \subset [\ell, L]$.

Hint: Use real induction. Define

$$S = \left\{ x \in [a, b] : \text{there exist } \ell_x, L_x \in \mathbb{R} \text{ with } \text{range}(f|_{[a, x]}) \subset [\ell_x, L_x] \right\}.$$

Well-orderings and transfinite induction

In Section 9.3, we saw how induction over the natural numbers can be reinterpreted using the well-ordering principle: Every nonempty subset of \mathbb{N} has a least element. It turns out that a similar result holds for any set, as long as we change our definition of “least!”

9.5.8

Example

The subsets $\{x \in \mathbb{Z} : x \leq 0\} \subset \mathbb{Z}$, $(0, 5) \subset \mathbb{R}$, and $(0, 5) \cap \mathbb{Q} \subset \mathbb{Q}$ have no least element, so unless we change our definitions the Well-Ordering Principle does not apply to \mathbb{Z} , \mathbb{R} , or \mathbb{Q} .

Here is the context in which our generalization of the Well-Ordering Principle holds. Recall that a relation on a set X is a predicate in two variables. That is, if \leq is a relation on X , then for any two elements $x, y \in X$ then $x \leq y$ is either true or false.

9.5.9

Definition ► Well-Ordered Set

Suppose that X is a set and that \leq is a relation on X such that the following hold:

1. (Each pair is comparable) For each pair $x, y \in X$, either $x \leq y$ or $y \leq x$,
2. (Antisymmetric) If $x \leq y$ and $y \leq x$ then $x = y$
3. (Reflexive) For every $x \in X$, $x \leq x$
4. (Transitive) For every choice of $x, y, z \in X$, if $x \leq y$ and $y \leq z$, then $x \leq z$.

Then we say that \leq is a **total order** on X and (X, \leq) is a **totally ordered set**. If $A \subset X$, then an element $m \in A$ is the **minimal element** of A if $m \leq a$ for every $a \in A$. An element $M \in A$ is the **maximal element** of A if $a \leq M$ for every $a \in A$. An A totally ordered set (X, \leq) is a **well-ordered set** (and \leq is a **well-ordering**) if every nonempty subset has a minimal element.

9.5.10

Example

The usual \leq (less-than-or-equal-to) relation on any subset $X \subset \mathbb{R}$ is a total order on X . If $X \subset \mathbb{N}$, then (X, \leq) is a well-ordered set. The relation \leq is not a well-ordering on \mathbb{R} , \mathbb{Q} , or \mathbb{Z} .

9.5.11

Exercise

For $n \in \mathbb{N}$, let $S(n) = \{n - \frac{1}{k+1} : k \in \mathbb{N} \text{ and } k \geq 2\}$. Note that the usual ordering \leq on $S(n)$ is a well-ordering (proof?). The ordering \leq is also a well-ordering of the set $S = \bigcup_{n \in \mathbb{N}} S(n)$. Sketch a picture of this set. This is often the picture people have in mind when they discuss an arbitrary well-ordered set.

9.5.12

Example

Let X be any set with at least three elements. Define \leq on $\mathcal{P}(X)$ by $A \leq B$ if and only if $A \subset B$. Then \leq is not a well-ordering on $\mathcal{P}(X)$. Which

conditions from the definition do hold?

9.5.13 **Exercise**

Find a well-ordering on the set $\{x \in \mathbb{Z} : x \leq 0\}$.

9.5.14 **Example**

Let $X = \mathbb{N} \times \mathbb{N}$. Define $(a, b) \leq (c, d)$ if and only if either $a < c$ or if $a = c$ and $b \leq d$. Then (X, \leq) is a well-ordered set.

9.5.15 **Example**

Let $X = \mathbb{N} \times \mathbb{N}$. Define $(a, b) \leq (c, d)$ if and only if either $a < c$ or if $a = c$ and $b \leq d$. Then (X, \leq) is a well-ordered set.

9.5.16 **Example**

Let S be the set of all finite non-decreasing sequences in \mathbb{N} . So for example $(10, 8, 6, 4)$ and $(25, 25, 3, 3, 3, 3)$ are elements of S . Suppose that $\alpha = (a_1, a_2, \dots, a_n)$ and $\beta = (b_1, b_2, \dots, b_m)$ are two elements of S . Define $\alpha \leq \beta$ if and only if one of the following holds:

- $\alpha = \beta$
- there exists $k \in \{1, \dots, n-1\}$ such that $k < m$, $a_i \leq b_i$ for all $i \leq k$, and $a_{k+1} < b_{k+1}$.

Then \leq is a well-ordering on S .

Suppose \leq is a well-ordering on a nonempty set X , we let $\mathbf{0}$ denote the minimal element of X . Also, if $a \leq x$ and $a \neq x$, we write $a < x$. We define

$$\llbracket \mathbf{0}, a \rrbracket = \{x \in X : x < a\}$$

9.5.17

Theorem ▶ Induction for Well-Ordered Sets

Suppose that (X, \leq) is a nonempty well-ordered set and that $A \subset X$ has the properties:

- (Base Fact:) $\mathbf{0} \in A$
- (Inductive Fact:) For every $a \in X$, if $\llbracket \mathbf{0}, a \rrbracket \subset A$ then $a \in A$.

Then $A = X$.

Thus, for any set X such that there exists a well-ordering \leq on X , we can use induction to prove facts about X . So what sets X have a well-ordering? It turns out that they all do!¹ A proof of the next theorem uses only material covered in

¹This statement is logically equivalent to the Axiom of Choice (Section 6).

this text, but it is rather challenging, so it is relegated to Section 9.10.

9.5.18 **Theorem ▶ The Well-Ordering Theorem**

For every set X , there exists a well-ordering \leq on X .

9.5.19 **Theorem**

Suppose that X and Y are sets. Then either there exists an injection $X \rightarrow Y$ or there exists an injection $Y \rightarrow X$.

Proof. If $X = \emptyset$, then the “empty function” is an injection $X \rightarrow Y$ and if $Y = \emptyset$, it is an injection $Y \rightarrow X$. Assume, therefore, that neither X nor Y are empty. A **partial injection** $f: (X, A) \rightarrow Y$ is an injective function $f: A \rightarrow X$ where $A \subset X$. If $A = X$, then a partial injection $f: (X, A) \rightarrow Y$ is an injection $X \rightarrow Y$.

By the Well-Ordering Theorem, there exists a well-ordering \leq on X . Let $\mathbf{0}_X$ be the minimal element of X with respect to this ordering. Let $\mathbf{0}_Y \in Y$. Define $f(\mathbf{0}_X) = f(\mathbf{0}_Y)$. Observe that $f: (X, \{\mathbf{0}_X\}) \rightarrow Y$ is a partial injection.

Let $\llbracket \mathbf{0}_X, \kappa \rrbracket$ denote the set of all $x \in X$ such that $x < \kappa$ and $\llbracket \mathbf{0}_X, \kappa \rrbracket$ the set of all $x \in X$ such that $x \leq \kappa$.

Suppose that there exists $\kappa \in X$ such that for all $\lambda \leq \kappa$, we have a partial injection

$$f_\lambda: (X, \llbracket \mathbf{0}, \lambda \rrbracket) \rightarrow Y$$

A priori, if $\lambda < \lambda' < \kappa$, the partial injections f_λ and $f_{\lambda'}$ have nothing to do with each other. Make the additional assumption, therefore, that for each such λ, λ' , the function $f_\lambda: \llbracket \mathbf{0}, \lambda \rrbracket \rightarrow Y$ is the restriction of the function $f_{\lambda'}$ to $\llbracket \mathbf{0}, \lambda \rrbracket$.

Define a function $g: \llbracket \mathbf{0}_X, \kappa \rrbracket \rightarrow Y$ by declaring $g(\lambda) = f_\lambda(\lambda)$ for all $\lambda < \kappa$.

⟨ Explain why g is an injection ⟩

If g is a surjection, let $f: Y \rightarrow X$ be defined so that $f(y)$ is that element of X such that $g(f(y)) = y$. (That is, f is the “right inverse” to g .) Since g was injective, f is a function and since g was a function f is an injection. Since we were looking for either an injection $X \rightarrow Y$ or an injection $Y \rightarrow X$, we found what we were looking for.

If we still haven’t found what we are looking for, then g is not a surjection. Thus, there exists $y \in Y$ such that $y \notin \text{range}(g)$. Define

$$f_\kappa(x) = \begin{cases} g(\lambda) & \text{if } \lambda < \kappa \\ y & \text{if } \lambda = \kappa. \end{cases}$$

Then $f_\kappa: (X, \llbracket \mathbf{0}_X, \kappa \rrbracket) \rightarrow Y$ is a partial injection.

⟨ Verify this! Also notice that if $\lambda < \kappa$ then f_λ is the restriction of f_κ ⟩

Suppose that there is no injection $Y \rightarrow X$. Then by Transfinite Induction, for each $\kappa \in X$, we have the partial injection f_κ constructed above. Define

$f(\kappa) = f_k(\kappa)$. Then¹ $f: X \rightarrow Y$ is a function. It is also injective.

\langle What properties of our definitions ensure that f is well-defined? \rangle

\langle What properties of our definitions ensure that f is an injection? \rangle \square

¹If we insist on a formal set-theoretic definition of function, as in Chapter 6, we need the version of the Recursion Principle associated to Transfinite Induction to make this statement valid. We do not discuss this in this book, but more advanced books on set theory do.

9.6 Application: Probability

“Using the factorial symbol always makes us look excited, and for good reason: the number $52!$ turns out to be about 10^{68} , a mind-bogglingly large number of different ways to order a deck of cards! This is way more than either stars in the universe or seconds since the big bang.”

–Francis Su [120]

The number of ways to choose k objects out of a collection of $n \geq k$ objects is denoted $\binom{n}{k}$. This is equal to the number of k -element subsets of an n element set. The factorial is defined recursively for $n \in \mathbb{N}^*$ by declaring $0! = 1$ and $(n+1)! = (n+1)n!$ for all $n \in \mathbb{N}^*$.

9.6.1

Theorem

The number of ways to choose k objects out of a collection of n objects is

$$\binom{n}{k} = \frac{n!}{(n-k)!k!}.$$

The number $\binom{n}{k}$ is read as “ n choose k ”. It is ubiquitous throughout mathematics and statistics.

Proof. Let $n \in \mathbb{N}$. We prove the theorem by induction on k . Let S be a set with n elements.

Base Case: $k = 0$

By definition, $0! = 1$, so $\frac{n!}{k!(n-k)!} = \frac{n!}{0!(n-0)!} = 1$. On the other hand, if a set has 0 elements, it is the empty set and so there is a unique subset of S having $k = 0$ elements. Thus,

$$\binom{n}{0} = 1.$$

Inductive Step: Assume that there exists $k \in \mathbb{N}^*$ with $k < n$ such that

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Let $X \subset S$ be a set with $k+1$ elements. Then there are exactly $k+1$ partitions of X of the form $\{\{x\}, \{x\}^c\}$ where $x \in X$. Furthermore, for a given $x \in X$, the

set $Y = \{x\}^C$ has exactly k elements. Thus, when we count the number of $(k+1)$ -element subsets $X \subset S$, we see that

$$\begin{aligned} (k+1) \cdot \binom{n}{k+1} &= (\text{number of } k \text{ element subsets } Y \text{ of } S) \cdot (\text{number of elements of } Y^c) \\ &= \binom{n}{k} \cdot (n-k) \\ &\stackrel{(IH)}{=} \frac{n!}{k!(n-k)!} \cdot (n-k) \\ &= \frac{n!}{k!(n-k-1)!}. \end{aligned}$$

Hence, algebra shows that

$$\binom{n}{k+1} = \frac{1}{(k+1)} \frac{n!}{k!(n-k-1)!} = \frac{n!}{(k+1)!(n-k-1)!}.$$

By induction, we are done. □

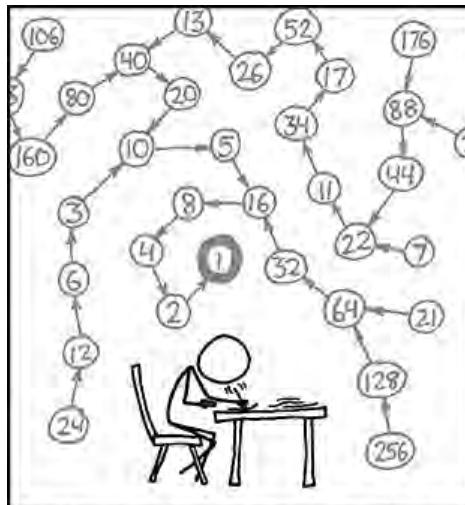
Suppose now that we have a fair coin, which we are going to flip $n \geq 1$ times. There are 2^n possible outcomes of the flips. What is the probability that exactly k of the n flips are Heads? (The other $n-k$ must be tails.)

Consider the set X of the 2^n possible outcomes of the n flips. We let $\mathcal{E} = \mathcal{P}(X)$ be thought of as an event space. Since the coin is fair, for $A \subset X$, we define

$$P(A) = \frac{|A|}{|X|}$$

where $|A|$ and $|X|$ denote the number of elements in A and X respectively. We are interested in the probability that an event contains exactly k Heads. Let $A \in \mathcal{P}(X)$ be the set whose elements are precisely the subsets of X containing exactly k Heads. Since any event which is not a “heads” is a “tail”, this is equal to the number of subsets of an n element set which contain exactly k elements (that is, out of the n flips, there are k which are heads.) Thus,

$$P(\text{exactly } k \text{ of the } n \text{ flips are heads}) = P(A)/|X| = \binom{n}{k}/2^n.$$



THE COLLATZ CONJECTURE STATES THAT IF YOU PICK A NUMBER, AND IF IT'S EVEN DIVIDE IT BY TWO AND IF IT'S ODD MULTIPLY IT BY THREE AND ADD ONE, AND YOU REPEAT THIS PROCEDURE LONG ENOUGH, EVENTUALLY YOUR FRIENDS WILL STOP CALLING TO SEE IF YOU WANT TO HANG OUT.

Figure 9.10: Comic from [xkcd](#).

9.7 Application: Iterated Function Systems

“It’s how you look at population changes in biology. Goldfish in a pond, say. This year there are x goldfish. Next year there will be y goldfish. Some get born, some get eaten by herons, whatever. Nature manipulates the x and turns it into y . Then y goldfish is your starting population for the following year. Just like Thomasina. Your value for y becomes your next value for x . The question is: what is being done to x ?”

– Tom Stoppard, *Arcadia* [118]

One of the most common methods of creating a sequence in a set X is to iterate a function $f: X \rightarrow X$. Given f , we pick some initial element $x_0 \in X$ and then define a sequence (x_n) recursively by letting $x_n = f(x_{n-1})$ for all $n \in \mathbb{N}$. Such a sequence is called an **iterated function sequence**. We saw an example of an iterated function sequence in the proof of Theorem 9.4.5. The sequence in the example of Section can also be interpreted as an iterated function sequence. Iterated function sequences arise in a variety of mathematical and scientific contexts.

9.7.1 Example

Let $r \in \mathbb{R}$ be fixed. A **discrete logistic sequence** is defined by choosing $x_0 \in \mathbb{R}$ and recursively defining, for all $n \in \mathbb{N}$,

$$x_{n+1} = r x_n (1 - x_n).$$

9.7.1

The discrete logistic equation is used as a simple model of population growth. The number x_n is the ratio of the population in year n to the total possible population. The number r is a scaling factor that takes reproduction and death rates into account.

9.7.2

Example ▶ (Collatz Conjecture)

Let $x_0 \in \mathbb{N}$. We define a sequence (x_k) in \mathbb{N} as follows. Assume that x_0, \dots, x_k have been defined and let

$$x_{k+1} = \begin{cases} x_k/2 & \text{if } x_k \text{ is even.} \\ 3x_k + 1 & \text{if } x_k \text{ is odd.} \end{cases}$$

Observe that we have a different sequence for each starting value $x_0 \in \mathbb{N}$. Suppose that there is a $k \in \mathbb{N}$ such that $x_k = 1$. What can you say about the terms of the sequence following x_k ?

The **Collatz Conjecture** says that for all $x_0 \in \mathbb{N}$, the sequence defined in Example 9.7.2 will have 1 as a term of the sequence. It is currently open. The mathematician Paul Erdős (1913 - 1996) thought that perhaps mathematics wasn't yet ready for such a conjecture!

9.7.3

Exercise

Give a formal definition of the directed graph appearing in the xkcd comic in Figure 9.10.

To explain the next two examples, recall that the set \mathbb{C} of complex numbers is simply \mathbb{R}^2 where we write $x + iy$ instead of (x, y) . Multiplication of complex numbers is defined by letting $i^2 = -1$ and using the distributive property so that:

$$(x + iy)(a + ib) = (xa - yb) + i(ya + xb).$$

The **norm** of a complex number $x + iy$ is defined to be:

$$|x + iy| = \sqrt{x^2 + y^2}.$$

Choose $c \in \mathbb{C}$ and let $f_c(z) = z^2 + c$ for all $z \in \mathbb{C}$. Let $z_0 = 0 = 0 + i0$ and, for $k \geq 0$, define $z_{k+1} = f(z_k)$. Then (z_k) is an iterated function sequence for each choice of c . The **Mandlebrot set**¹ is the set of all $c \in \mathbb{C}$ such that the iterated function sequence (z_k) starting at $z_0 = 0$ is bounded. That is, an complex number c is an element of the Mandlebrot set if and only if there exists $M \in \mathbb{N}$ such that $|z_k| \leq M$ for all k . For those values of $c \in \mathbb{C}$ where the iterated function sequence does not remain bounded, we may color the point $c \in \mathbb{C} = \mathbb{R}^2$ according to how many terms of the iterated function sequence are needed before the norm is larger than a pre-chosen threshold.

¹Named after Benoit Mandelbrot (1924-2010)

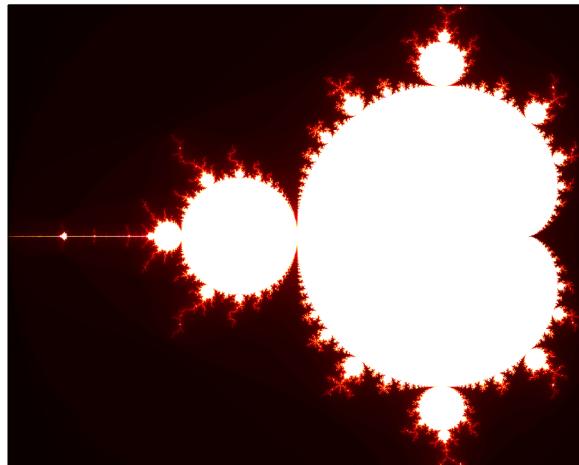
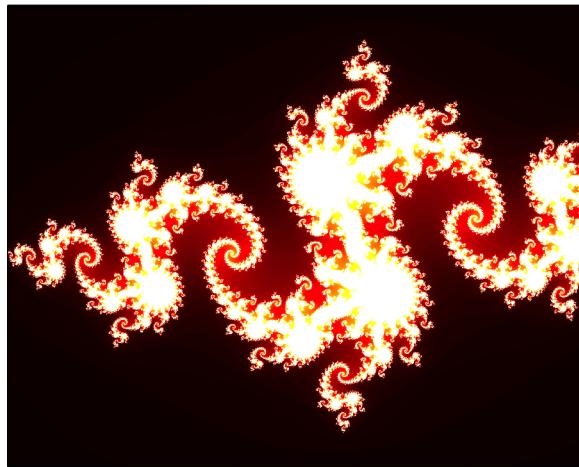


Figure 9.11: The Mandelbrot set

Now, consider c as fixed and think about varying the the initial z_0 values for the iterated function sequence. For $z_0 \in \mathbb{C}$, let (z_k) be the iterated function sequence. If the sequence (z_k) is bounded, then z_0 is an element of the (closed) **Julia set** for f_c . As with the Mandlebrot set, we color the point $z_0 \in \mathbb{C} = \mathbb{R}^2$ according to how many terms of the sequence are needed for the norm to be larger than the pre-chosen threshold. See Figure 9.12 for a picture.

Figure 9.12: The closed Julia set for $c = -0.8 + 0.156i$.

In the Mandlebrot and Julia sets, the points near the edges have the property that if they are perturbed slightly (i.e. moved a little bit in some direction) the behaviour of the iterated function sequence can change dramatically (for instance from being bounded to being unbounded.) This is called “sensitivity to initial conditions” and is one component of the definition of a chaotic system.

An important example of sensitivity to initial conditions occurs in Newton's Method. Frequently in applications, it is necessary to find the places (the *roots*) where a certain function $f: \mathbb{R} \rightarrow \mathbb{R}$ is zero. For instance, to find the maximum and minimum values of a differentiable function F , we solve the equation $f(t) =$

$F'(t) = 0$ for t . For most functions (including most polynomials) it is impossible to algebraically find their roots. Newton's method is a popular method for approximating roots. A full description can be found in most Calculus texts, here we content ourselves with observing how the approximation process is an iterated function sequence. In order to generate a pretty picture, we work with complex numbers rather than real numbers, though much of the same behaviour can occur with reals.

Let $f: \mathbb{C} \rightarrow \mathbb{C}$ be a differentiable function with the property that $f'(z) \neq 0$ for all $z \in \mathbb{C}$. Define $N: \mathbb{C} \rightarrow \mathbb{C}$ by

$$N(z) = z - \frac{f(z)}{f'(z)}$$

Choose $z_0 \in \mathbb{R}$ and let (z_n) to be the iterated function sequence defined by $z_{n+1} = N(z_n)$. If all goes well, the sequence (z_n) will converge to a root of f . However, Newton's method is sensitive to initial conditions. Figure 9.13 depicts the convergence properties of (z_n) for different initial conditions x_0 for the function $f(x) = (x + 2)(x^2 + 1)$.

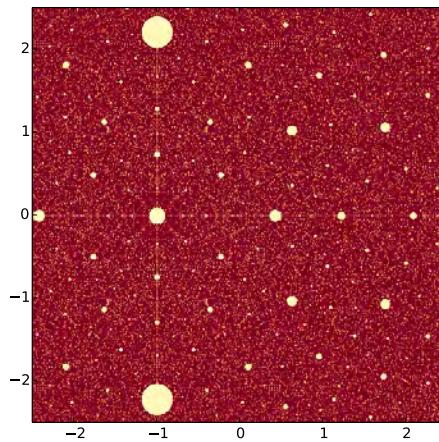


Figure 9.13: Letting $f(z) = (z + 2)(z^2 + 1)$, each point $x + iy \in \mathbb{C}$ with $-2.5 \leq x, y \leq 2.5$ is colored corresponding to how rapidly Newton's method converges when the iterated function sequence has initial term $x + iy$. The more red the color, the longer it takes to converge.

9.8 Application: Paths in Graphs

Thomasina: “Each week I plot your equations dot for dot, x s against y s in all manner of algebraical relation, and every week they draw themselves as commonplace geometry, as if the world of forms were nothing but arcs and angles. God’s truth, Septimus, if there is an equation for a curve like a bell, there must be an equation for one like a bluebell, and if a bluebell, why not a rose? Do we believe nature is written in numbers?”

Septimus: “We do.”

Thomasina: Then why do your equations only describe the shapes of manufacture? ... Armed thus, God could only make a cabinet!”

– Tom Stoppard, *Arcadia* [118]

Recall (from Section) that a path in a graph G is a finite sequence of vertices such that every two adjacent vertices in the sequence are the endpoints of an edge. We say that such an edge is **traversed** by the path. In this section, we consider a classical problem which is the origin of the mathematical subjects of graph theory and topology and then discuss its relevance to the problem of analyzing DNA.

Eulerian Paths and Circuits

In 1736, the residents of Königsberg, Prussia enjoyed long walks around their town. One of the beautiful features of Königsberg at that time, features subsequently destroyed by bombing during World War II and construction afterwards, was the presence of 7 bridges connecting the different parts of the town. On their leisurely walks, the residents wondered, “Is it possible to walk across the 7 bridges of Königsberg without walking across any of them twice?” The famed mathematician Leonhard Euler (1707-1783) answered the question and, in so doing, prefigured the creation of graph theory and topology as mathematical disciplines. Figure 9.14 shows an image of the bridges of Königsberg from Euler’s paper [45]. How might we turn the Königsberg bridge problem into a mathematical problem?

We can construct a graph (called the “Königsberg bridge graph”) by taking a vertex for every landmass and an edge for every bridge. Join two vertices by an edge if and only if one of the vertices is a land mass and the other is a vertex corresponding to a bridge adjacent to the landmass. The graph G is shown in Figure 9.15.

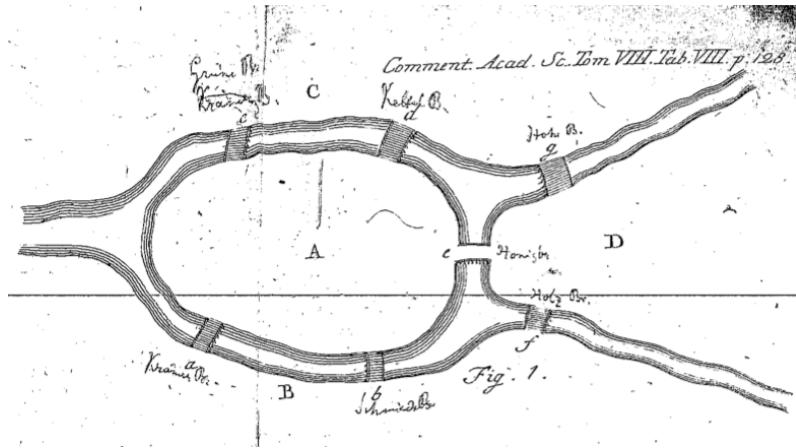
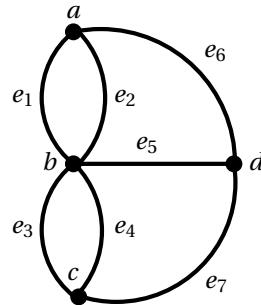


Figure 9.14: The 7 bridges of Königsberg from Euler's paper

Figure 9.15: The Königsberg Graph G .

Observe that our Königsberg bridge graph has multiple edges with the same endpoints. According to our prior definitions, a path in a graph is a list of vertices where each pair of adjacent vertices in the graph are the endpoints of an edge. When there are multiple edges with the same endpoints, this creates a troubling ambiguity. We can rectify this by putting the name of each edge in between its endpoints. For instance, using the notation from Figure 9.15,

$$a, e_6, d, e_7, c, e_4, b, e_2, a$$

is a path starting and ending at a .

9.8.2

Theorem ▶ The Königsberg Bridge Problem

There is no path through G which traverses each edge exactly once.

Proof. Suppose, for a contradiction, that there is a path

$$\alpha = v_0, \dots, v_n$$

which traverses each edge exactly once.

Consider $k \in \{0, \dots, n\}$. Since α traverses each edge of G exactly once, the path enters v_k along a different edge than the edge by which it leaves v_k . No edge of G is a loop. Thus, for each vertex p of G , the vertex p is adjacent to an even number of edges unless $v_0 \neq v_n$ in which case the vertices v_0 and v_n each are

adjacent to an odd number of edges and all other vertices of G are adjacent to an even number of vertices.

However, there is a vertex of G (actually every vertex of the Königsberg bridge graph) which is adjacent to an odd number of vertices. Thus, it is not possible for α to traverse every edge of G exactly once. \square

A path in a graph G is **Eulerian** if it traverses each edge exactly once. A closed Eulerian path is an **Eulerian circuit**. The proof that there is no walk through Königsberg that traverses each edge exactly once actually proves the following stronger result. The condition that G have no loops is not a serious one has adding or removing a loop from a graph does not affect the presence of Eulerian paths or circuits.

If v is a vertex of a graph G , the **valence** (or **degree**) of v is the number of edges that are not loops for which v is an endpoint plus twice the number of loops adjacent to v .

9.8.3

Theorem ▶ Constructing Eulerian Circuits

Suppose that G is a nonempty finite connected graph such that every vertex has even valence. Then G contains an Eulerian circuit.

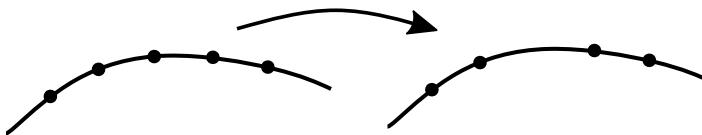


Figure 9.16: Removing a valence 2 vertex in the proof of Theorem 9.8.3.

Proof. We first examine two special cases. The first is when G consists of a single vertex and no edges. In this case, the constant path where we just sit at the vertex is an Eulerian circuit. The second special case is when every vertex of G has valence equal to 2. We tackle this situation by minimal counterexample.

Assume that G is a nonempty finite connected graph such that every vertex has valence 2. Assume, for a contradiction, that G does not contain an Eulerian circuit. Out of all such counter-examples, we may assume that we selected G to minimize the number of vertices. Since G is non-empty, it has a vertex v . If v is the only vertex, then G has a single edge, which must be a loop based at v . Traversing the loop is then an Eulerian circuit, contradicting the assumption that G does not have such a circuit. Thus, we may assume that G has at least two vertices. Let v be one of them. It is incident to edges e_- and e_+ . Let G' be the graph obtained from G by merging e_- and e_+ into a single edge e and removing v as a vertex, as in Figure 9.16. G' is still nonempty and connected (do you see why?). Each vertex still has valence equal to 2. It also has one less vertex than G . Thus, G' cannot be a counterexample and so has an Eulerian circuit. At some point, as we traverse the circuit, we cross the edge e . Insert the vertex v back into e , splitting it back into e_- and e_+ . Traversing e , then amounts to traversing e_- and then e_+ or vice versa. Our Eulerian circuit

for G' is then turned into an Eulerian circuit for G , contradicting our assumption that G was a counterexample. Thus, no counterexample has vertices all of valence 2.

We now prove the remaining cases by induction on the number of vertices v that have valence greater than 2. Let $N(G)$ be the number of the vertices of G that have valence at least 4. (Recall that all vertices have even valence).

(State the base case and explain why it holds.)

Let v be a vertex of G having valence at least 4. Let G' be the graph obtained by splitting G open along v , pairing off the edges incident to v , and inserting vertices of valence 2, as in Figure 9.17. It may be the case that G' is disconnected.

(Explain why each component of G' has an Eulerian circuit.)

(Prove that G has an Eulerian circuit.) □

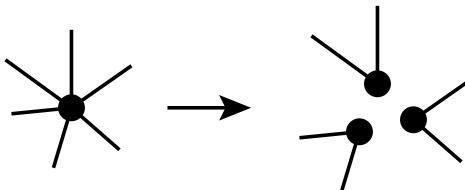


Figure 9.17: Splitting G open at v to obtain G' .

Although there is a trick which allows you to derive the proof in the next exercise from the statement of Theorem 9.8.3, you are encouraged instead to construct a full proof modelled on the proof of Theorem 9.8.3. Doing so will give you practice in writing proofs by minimal counter-example.

9.8.4

Exercise

Suppose that G is a finite, connected graph having vertices v_- and v_+ such that v_- and v_+ both have odd valence and all other vertices of G have even valence. Prove that there is an Eulerian path in G from v_- to v_+ . You may first want to prove that there is no graph such that exactly one vertex has odd valence.

DNA sequencing

DNA molecules are essential to life as we know it. Roughly speaking, DNA consists of two strands winding around each other to form a double helix. Each strand contains a sequence of sub-molecules called *bases*. On (most) DNA there are four kinds of bases, abbreviated C, G, A, and T. The strands are joined together by chemical bonds between the bases. Knowing the DNA sequence, i.e. the finite sequence of Cs, Gs, As, and Ts, tells biologists a great deal about the DNA. Since A always pairs with T and C always pairs with G, it is enough to know the sequence of bases along just a single strand of the DNA. For example, human

DNA contains the sequence ¹

*TTTGTTCCTCCACTTGCTTCTGAGGAACCC
AAGCTAAGACACTGTATGTTATTCTAATT*

Since DNA is naturally incredibly long and the machines that detect the base sequence require short strands of DNA, biologists “cut” the DNA into pieces, analyze the pieces to learn the sequence on each piece, and then reassemble these small sequences to obtain the entire DNA sequence. The “cutting” is performed either randomly or non-randomly by particular enzymes, each of which recognizes a particular short sequence of bases and cuts the DNA after that sequence. After cutting, the fragments of DNA are read and then reassembled into the complete string. Unfortunately, the process of cutting the DNA, analyzing the strands, and reporting the sequences, cannot preserve the order of the sequences on the original strand. The basic steps for determining a long DNA sequence are “cut, analyze, reassemble.” The reassembly stage is the most difficult, as biologists must figure out what the correct order for the pieces.

The basic strategy in reassembly is to make copies of the DNA sequence before cutting and then cut the copies in different ways. For example, suppose that one copy of the strand above is randomly cut into the fragments²:

$$\Delta = \left\{ \begin{array}{l} TTTGTT \\ CCCACTTGCTTCTGA \\ GGAACC \\ CAAGCTAAGACACT \\ GTATGTTATTCTAATT \end{array} \right\}.$$

A different copy of the DNA strand is then randomly cut into different fragments:

$$\blacktriangle = \left\{ \begin{array}{l} TTTGTTCCTC, \\ ACTTGCTTTC, \\ TGAGGAACCC, \\ AAGCTAAGA, \\ CACTGTATGT, \\ TTATTCTAATT \end{array} \right\}.$$

The two sets Δ and \blacktriangle are then compared to each other. The set Δ contains the sequence *GGAACC*. In \blacktriangle , we see that sequence contained in the sequence *TGAGGAACCC*. That is the only sequence in $S(\blacktriangle)$ which contains *GGAACC*, and so we can conclude that in the original strand, *GGAACC* was preceded by *TGA* and itself precedes *C*. In Δ , there is one sequence ending in *TGA*, namely

CCCACTTGCTTCTGA.

¹This sequence was obtained from WolframAlpha

²This is a somewhat misleading way to put it. The machines that do the analyzing cannot analyze the entire length of a fragment, so typically an analysis of a fragment returns some sequence of definitive bases and then a considerable number of unknown bases.

There are, however, two sequences in Δ beginning with C:

$\textcolor{red}{C}AAGCTAAGACACT$ and $\textcolor{red}{CCCACTTGTGCTTCTGA}$.

We already know, however, that the latter strand comes after $GGAACC$, and so the original strand of DNA must contain the sequence

$CCCACTTGTGCTTCTGAGGAACCCAAGCTAAGACACT$

(as we already knew.) Continuing on in this way, we can reconstruct the entire original sequence.

There are two challenges to this process. The first is that there can be errors in both the cutting process and the analyzing process. These are relatively easily dealt with by making many, many copies of the original sequence and using statistical methods to eliminate errors up to a certain allowable probability. The second challenge is more serious: DNA sequences typically contain many repeated patterns of bases (called **repeats**). In the very simplified example above, we saw how the multiple occurrences of C at the beginning of a strand made it somewhat more difficult to reassemble the fragments correctly. In long strands of DNA, the many repeats mean that many comparisons must be made to figure out how to correctly reassemble the fragments. This means that the assembly stage is very slow; it seems that each sequence in Δ must be compared with each sequence in \blacktriangle . Since thousands of DNA strands must have their sequences reassembled this time constraint is a serious obstacle.

Progress can be made by reinterpreting the assembly step as a problem in graph theory. To do this, we create a graph with a vertex for each sequence in Δ . We join two vertices v and w by a directed edge if there is a sequence (let's call it Q) in \blacktriangle such that the sequence Q contains the end of the sequence corresponding to v followed by the beginning of the sequence corresponding to w . Call the resulting graph G . Reconstructing the original sequence then amounts to the problem of finding a path in G which passes through every vertex exactly once. The desired path is called a **Hamiltonian path**¹. The challenge of finding a Hamiltonian path is called the **Travelling Salesman Problem** for G .

Unfortunately, the Travelling Salesman Problem is, in general, extremely difficult to solve. In particular, all known methods for finding a Hamiltonian path take an extremely long time when the graph has a large number of vertices. In 2001, however, significant progress was made by Pevzner, Tang, and Waterman [100]. They found a way of transforming the assembly problem into the problem of finding Euler circuit in a different (but related) graph associated to the DNA sequences. Finding an Euler path (in a graph that has one) is straightforward and there are algorithms for it whose running time only grows linearly with respect to the number of vertices.

¹Named after William Rowan Hamilton (1805-1865).

9.9 Additional Exercises

“Proving things is a matter of finding good arguments, and when you’ve seen a lot of good arguments you have a much better sense of what a good argument smells like.”

– Amie Wilkinson¹ [64]

- Let $r \neq 1$ be a real number. Prove, using regular old induction, that for all $n \in \mathbb{N}^*$

$$\sum_{k=0}^n r^k = \frac{1 - r^{n+1}}{1 - r}.$$

- Suppose that (X, d) is a metric space and that $x_1, \dots, x_n \in X$. Prove that

$$d(x_1, x_n) \leq \sum_{i=1}^{n-1} d(x_i, x_{i+1})$$

- Prove the following following characterization of prime numbers:

9.9.1

Theorem ▶ Characterization of prime numbers

For $p \in \mathbb{N}$, the following are equivalent:

- p is a prime number
- If $a, b \in \mathbb{N}$ and ab is a multiple of p then a is a multiple of p or b is a multiple of p .

- Let X be a set with $n \geq 1$ elements. Prove that there are $n! = n(n-1)\cdots 3 \cdot 2 \cdot 1$ permutations of X .
- Let X and Y be sets with n and m elements, respectively. Prove that if $X \cap Y = \emptyset$, then $X \cup Y$ has $n + m$ elements. What can you say about the situation when $X \cap Y \neq \emptyset$?
- Suppose that X is a finite set and that $\{U_\lambda \subset X : \lambda \in \Lambda\}$ is a partition of X . Suppose that, for each $\lambda \in \Lambda$, U_λ has n_λ elements. Prove that the number of elements of X is

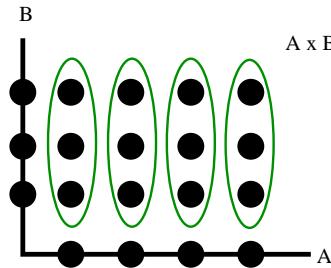
$$\sum_{\lambda \in \Lambda} n_\lambda.$$

(Hint: Induct on the number of elements of Λ .)

- Let X and Y be sets with n and m elements, respectively. Prove that $X \times Y$ has nm elements.

Hint: Observe that $\{\{a\} \times B : a \in A\}$ is a partition of $A \times B$, as in the image below.

¹Amie Wilkinson is a mathematician who studies dynamical systems.



8. A **tree** T is a connected graph with the property that for every edge e in T , the graph $T \setminus e$ obtained by removing e (but leaving its endpoints) is disconnected. A **leaf** is a vertex of a tree which is an endpoint of exactly one edge of the tree. It is a fact (see Theorem 9.2.8) that every tree with at least one edge has at least two leaves. Suppose that T is a tree with vertex set $V(T)$ and edge set $E(T)$. Let $\mathcal{F}(V(T))$ denote the set of functions $f: V(T) \rightarrow \mathbb{R}$ and $\mathcal{F}(E(T))$ the set of functions $g: E(T) \rightarrow \mathbb{R}$. See the discussion in Section and Exercise 18 in Section 8.12.

Assign an orientation to every edge of T , so that for each edge e , one endpoint of e is the **head** (denoted $\partial_+ e$) and the other endpoint is the **tail** (denoted $\partial_- e$). Define $\nabla: \mathcal{F}(V(T)) \rightarrow \mathcal{F}(E(T))$ as follows. Given a function $f \in \mathcal{F}(V(T))$, we will have a function $\nabla f \in \mathcal{F}(E(T))$. The function ∇f is defined by declaring

$$\nabla f(e) = f(\partial_+ e) - f(\partial_- e)$$

for every edge $e \in E(T)$.

Prove that, for a finite tree T with at least one edge, the function $\nabla: \mathcal{F}(V(T)) \rightarrow \mathcal{F}(E(T))$ is surjective.

(Hint: Use regular old induction on the number of edges of T . To apply the inductive hypothesis, use the fact that every tree with at least one edge has a leaf and remove an edge having a leaf as an endpoint.)

9. Suppose that A is a non-empty subset of \mathbb{N} such that there exists $M \in \mathbb{N}$ so that for all $a \in A$, $a \leq M$. (That is, M has an upper bound.) Use the Well-Ordering Principle to prove that there exists a unique $M' \in A$ such that for all $a \in A$, $a \leq M'$. (That is, show that A contains a unique maximal element.)
10. Explain why the d in Theorem 9.3.4 is the greatest common divisor of x and y .

9.10 Appendix: The Well-Ordering Theorem

“We will settle with your father about the money afterwards; but the things should be ordered immediately.”

– Jane Austen, *Pride and Prejudice*

In this section we prove the Well-Ordering Theorem, following the exposition given in [136]. The proof relies heavily on the persistence of certain structures under intersections as in Chapter 2. We also make use of injective functions and power sets. All-in-all a heady mix! The Well-Ordering Theorem is actually logically equivalent to the Axiom of Choice. Of all the statements logically equivalent (in the presence of the other set theory axioms) to the Axiom of Choice, it is the most counter-intuitive. The Well-Ordering Theorem was first formulated by Cantor, and the Axiom of Choice was introduced by Zermelo in order to make it more palatable [13].

9.10.1

Theorem ▶ The Well-Ordering Theorem

For every set X , there exists a well-ordering on X .

Proof. We actually define a total ordering \preccurlyeq on X such that for each nonempty $A \subset X$, there exists a maximal element in A . Once we have defined such a total ordering, we define another total ordering \leq on X by declaring $x \leq y$ if and only if $y \preccurlyeq x$.

(Show that in such a situation \leq is a well-ordering on X .).

It turns out that it is better to work with certain subsets of X , rather than X itself. Let $\mathcal{P}^*(X) = \{A \subset X : A \neq \emptyset\}$. For each $A \in \mathcal{P}^*(X)$, choose a particular element $F(A) \in A$. If you studied Chapter 6, you will know that the Axiom of Choice guarantees it is possible to do this in such a way that

$$\{x \in X : \exists A \in \mathcal{P}^*(X), x = F(A)\}$$

is a set. Consequently, $F: \mathcal{P}^*(X) \rightarrow X$ is a function. If you didn't study Chapter 6, you will need to trust me on that.

Say that a set $\mathcal{F} \subset \mathcal{P}^*(X)$ of nonempty subsets of X is **distinguished** if:

1. $X \in \mathcal{F}$
2. For all $A \in \mathcal{F}$, either $A \setminus \{F(A)\} \in \mathcal{F}$ or it is empty
3. For all $\mathcal{A} \subset \mathcal{F}$, either $\bigcap_{A \in \mathcal{A}} A \in \mathcal{F}$ or it is empty.

(Prove that the intersection of distinguished sets is distinguished)

Therefore, the intersection of all distinguished sets is distinguished. Let \mathcal{F} be that distinguished set.

(Explain why if \mathcal{F}' is some other distinguished set, then $\mathcal{F} \subset \mathcal{F}'$. That is, \mathcal{F} is the smallest distinguished set.)

We will attempt to construct a well-ordering on \mathcal{F} using the subset relation \subset . Recall that a well-ordering is a total ordering such that every nonempty set has a minimum. We will show that as a relation on \mathcal{F} , the relation \subset is a total order such that every nonempty set has a maximum.

(Remind yourself that \subset is reflexive, antisymmetric, and transitive.)

To be a total order on \mathcal{F} , we need to be able to compare any two elements of \mathcal{F} . That is we need to know that if $A, B \in \mathcal{F}$ then $A \subset B$ or $B \subset A$. Rather than proving this directly (which is very difficult), we take a more abstract approach, wherein we collect all incomparable sets together and show we can do without them. Unless there are no incomparable sets, this will contradict our choice of \mathcal{F} to be the *smallest* distinguished set.

Say that a set $I \in \mathcal{F}$ is **incomparable** if there exists $Z \in \mathcal{F}$ such that $I \not\subset Z$ and $Z \not\subset I$. Notice that such a Z is also incomparable. Let \mathcal{F}' be the set of all $S \in \mathcal{F}$ such that every incomparable $I \subset S$.

(Show that \mathcal{F}' satisfies the first and third criteria for being distinguished.)

We now show, using a somewhat more involved argument, that \mathcal{F}' also satisfies the second criterion for being distinguished.

(Explain why each $S \in \mathcal{F}'$ is not incomparable, using the fact that if Z is incomparable then $Z \subset S$ by the definition of \mathcal{F}' .)

Suppose that $S \in \mathcal{F}'$. Let $S' = S \setminus \{F(S)\}$; assume it is nonempty. If $S' \not\subset \mathcal{F}'$, there exists an incomparable set I such that $I \subset S$ but $I \not\subset S'$. Thus, there is an element $s \in I$ such that $s \in S$ but $s \notin S'$. That element must be $F(S)$.

(Explain why.)

Consequently, $I = S$, implying S is incomparable, a contradiction. Thus, $S' \in \mathcal{F}'$, as desired. We conclude that \mathcal{F}' is distinguished.

(Explain why this implies that $\mathcal{F} = \mathcal{F}'$.)

No incomparable set I is an element of \mathcal{F}' , so \mathcal{F} contains no incomparable sets. Thus, the subset relation \subset is a total order on \mathcal{F} .

We now show that for each nonempty $\mathcal{A} \subset \mathcal{F}$, \mathcal{A} contains a maximal element. Let $\mathcal{A} \subset \mathcal{F}$ be nonempty. Define

$$\mathcal{M} = \{Z \in \mathcal{F} : \text{for every } A \in \mathcal{A}, A \subset Z\}$$

to be the set of all sets in \mathcal{F} containing all elements of \mathcal{A} .

Clearly, $X \in \mathcal{M}$, so \mathcal{M} is nonempty. Let $M = \bigcap_{Z \in \mathcal{M}} Z$.

(Explain why $A \subset M$ for every $A \in \mathcal{A}$)

Thus, since \mathcal{A} is nonempty and no $A \in \mathcal{A}$ is the empty set, the set M is nonempty. Since \mathcal{F} is distinguished, $M \in \mathcal{F}$.

(Explain why $M \in \mathcal{M}$ and why if $Z \in \mathcal{M}$, then $M \subset Z$.)

Let $M' = M \setminus \{F(M)\}$. Since $M' \subsetneq M$, $M' \not\subset \mathcal{M}$. Thus, there exists $A \in \mathcal{A}$ such

that $A \not\subset M'$.

(Prove that $A = M$.)

Thus, $M \in \mathcal{A}$. Since $A \subset M$ for every $A \in \mathcal{A}$ and since $M \in \mathcal{A}$, we see that M is the maximal element of \mathcal{A} .

It remains to convert the total order \subset on \mathcal{F} into a well-ordering on X . To do this we construct an injection $I: X \rightarrow \mathcal{F}$.

For $x \in X$ consider the set $I(x)$ which is the intersection of all sets $Z \in \mathcal{F}$ such that $x \in Z$. Since X is such a set, the intersection is defined.

(Explain why $x \in I(x)$ and why $I(x) \in \mathcal{F}$.)

Thus, we have an injection $I: X \rightarrow \mathcal{F}$. We now show it is injective.

(Explain why if $Z \in \mathcal{F}$ and $x \in Z$, then $I(x) \subset Z$.)

Let $I' = I(x) \setminus \{F(I(x))\}$. Recall that if $I' \neq \emptyset$, then $I' \in \mathcal{F}$. Since $I \not\subset I'$, it must be the case that $x \notin I'$.

(Show that this implies that $x = F(I(x))$.)

Now suppose that $x, y \in X$ and $I(x) = I(y)$. Since F is a function, $F(I(x)) = F(I(y))$. Thus, $x = y$. Consequently, $I: X \rightarrow \mathcal{F}$ is an injective function.

Define $x \preccurlyeq y$ if and only if $I(x) \subset I(y)$.

(Use the fact that \subset is a total order on \mathcal{F} to show that \preccurlyeq is a total order on X .)

Let $A \subset X$ be nonempty; we show that A contains a maximal element. Let $\mathcal{A} = \text{range } I|_A$. By our previous remarks, there exists a set $M \in \mathcal{A}$ such that $S \subset M$ for all $S \in \mathcal{A}$. By the definition of \mathcal{A} , there exists $m \in A$ such that $M = I(m)$. Thus, for all $x \in A$, $I(x) \subset I(m)$. That is, for all $x \in A$, $x \preccurlyeq m$. Thus, A has a maximal element.

Consequently, the order \preceq defined at the start of this proof in terms of \preccurlyeq is a well-ordering on X . \square

10 | The sizes of sets

Key Terms

- cardinality of a finite set
- $\text{card } X = \text{card } Y$.
- $\text{card } X \leq \text{card } Y$.
- A set X is countable.

“Everything was magical. And it seemed to go on forever. None of the pathways ended”
–Erin Morgenstern, *Night Circus*

10.1 Finite Sets

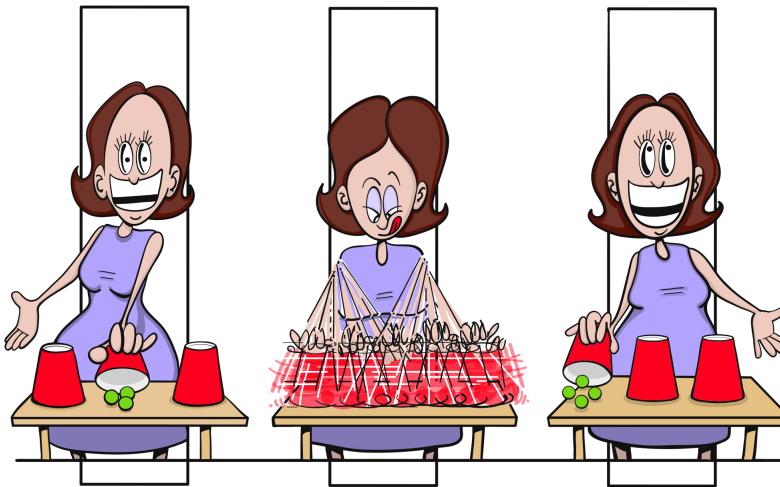
“Mathematical ideas that may seem obvious to us – such as the fact that you can count a set of objects, move them around, and then count them again and you get the same number – are fascinating to young children.”

- Jo Boaler, *What's Math Got to Do With It?* [15]

The number of elements of a finite set is a crucial attribute of the set. What *exactly* do we mean by this number? Informally, we certainly have an idea of what we mean: we can count the elements of the set, beginning with 1 and not skipping any elements, until we run out of elements. Whatever number we end with is the “number of elements of the set.” Considering things more carefully, however, we might begin to worry.

We've likely all had the experience of counting the number of elements in some collection and coming to a different number than the number a friend has obtained. We usually put this down to one of us having made a mistake. What if, however, it wasn't that we made a mistake but that the number of elements of the

set changed? or wasn't well-defined to begin with? Furthermore, we only have first-hand experience of sets with a relatively small number of elements. What if the size of a set, when the set is very large, doesn't make sense? After all, for very large finite sets we couldn't list the elements in our lifetime! What exactly do we mean by a "finite set" when we can't physically or mentally count all of its elements?



As is often the case, careful definitions can bring clarity. Our definition is inspired by the fact that we "should" be able to count the elements of a finite set until at some point we run out of elements. Since counting involves naming each element in the set with an element of \mathbb{N} , we model the process of counting with bijections.

10.1.1

Definition ▶ Finite and Infinite

The empty set \emptyset is **finite**. Its **cardinality** is 0 and we write $|\emptyset| = 0$ or $\text{card}(\emptyset) = 0$. A nonempty set X is **finite** if there exists $n \in \mathbb{N}$ such that there is a bijection

$$f: \{1, \dots, n\} \rightarrow X.$$

In this case, we say that the **cardinality** of X is n and we write $|X| = n$ or $\text{card}(X) = n$. A set is **infinite** if it is not finite.

Our first theorem confirms our intuition that two finite sets have the same cardinality if and only if we can form a one-to-one matching between their elements. Its proof is a straightforward application of the definition of cardinality.

10.1.2

Theorem

Suppose that X and Y are finite sets. Then $|X| = |Y|$ if and only if there is a bijection $f: X \rightarrow Y$.

But is it possible that $|X|$ is not well-defined? That is, is it possible for there to be

some finite set X and distinct $n, m \in \mathbb{N}$ such that there is a bijection $\{1, \dots, n\} \rightarrow X$ and also a bijection $\{1, \dots, m\} \rightarrow X$? Although the answer may seem like an obvious “No!”, that is only because we have grown accustomed to the idea that the number of elements of a finite set is a well-defined concept. When we remember that what we consider obvious was formed by our long experience with finite sets having relatively few elements, we may question whether or not the same results hold for sets with many, many more elements than we can possibly imagine. Thus, we need a proof. We begin by considering the situation when $X = \{1, \dots, m\}$.

10.1.3 **Theorem**

For each $n, m \in \mathbb{N}$, if there is a bijection $f: \{1, \dots, m\} \rightarrow \{1, \dots, n\}$, then $m = n$.

For convenience, we begin with an important exercise.

10.1.4 **Exercise**

Let $m \in \mathbb{N}$ and suppose that $q \in \{1, \dots, m\}$. Construct a bijection

$$\phi: \{1, \dots, m-1\} \rightarrow \{1, \dots, m\} \setminus \{q\}.$$

The challenges in the proof of Theorem 10.1.3 are mostly of the bookkeeping variety. We will induct on n . When $n = 1$, we can use the fact that $\{1\}$ has a unique element and the definition of bijection to conclude that $\{1, \dots, m\}$ does as well. For the inductive step, we consider a bijection $f: \{1, \dots, m\} \rightarrow \{1, \dots, k+1\}$. We then create a bijection $f': \{1, \dots, m-1\} \rightarrow \{1, \dots, k\}$ from f as follows. We remove $k+1$ from $\{1, \dots, k+1\}$ and also remove whatever number $q \in \{1, \dots, m\}$ is sent to $k+1$ from $\{1, \dots, m\}$. We obtain $A = \{1, \dots, q-1\} \cup \{q+1, \dots, m\}$. By restricting the domain and codomain of f , we create a bijection

$$f|_A: \{1, \dots, m\} \setminus \{q\} \rightarrow \{1, \dots, k\}.$$

We renumber the domain of $f|_A$ using the bijection ϕ constructed in Exercise 10.1.4. The composition $f' = f|_A \circ \phi$ is then the bijection we are looking for. Applying the induction hypothesis, we conclude that $m-1 = k$ and, hence that $m = k+1$, as desired.

Proof. Let $P(n)$ be the statement:

“for all $m \in \mathbb{N}$, if there is a bijection $f: \{1, \dots, m\} \rightarrow \{1, \dots, n\}$ then $m = n$.”

We prove that $P(n)$ is true for all $n \in \mathbb{N}$ by induction.

Base Case: We prove that for all $m \in \mathbb{N}$, if there is a bijection $f: \{1, \dots, m\} \rightarrow \{1\}$ then $m = 1$.

Let $m \in \mathbb{N}$ and assume that there is a bijection $f: \{1, \dots, m\} \rightarrow \{1\}$. If $a \in \{1, \dots, m\}$, then $f(a) = 1$, since 1 is the unique element of $\{1\}$. Since f is injective, the set $\{1, \dots, m\}$ is empty or has a unique element. Since $m \geq 1$, $1 \in \{1, \dots, m\}$, and so $\{1, \dots, m\} \neq \emptyset$. Thus, $\{1, \dots, m\} = \{1\}$. Hence, $m = 1$.

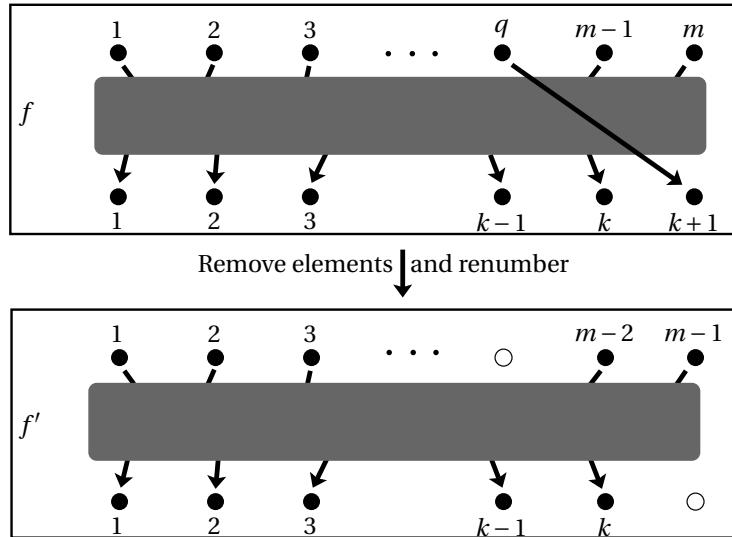


Figure 10.1: The inductive step of the proof of Theorem 10.1.3. The dark box means that we don't know exactly how the bijection matches elements, except that $f(q) = k + 1$.

Inductive Step: Assume that there exists $k \in \mathbb{N}$ such that for all $m' \in \mathbb{N}$, if there is a bijection $f': \{1, \dots, m'\} \rightarrow \{1, \dots, k\}$ then $m' = k$. We will show that for all $m \in \mathbb{N}$ if there is a bijection $f: \{1, \dots, m\} \rightarrow \{1, \dots, k+1\}$, then $m = k+1$. Figure 10.1 gives the essential idea for how we can apply the inductive hypothesis.

Let $m \in \mathbb{N}$ and suppose that $f: \{1, \dots, m\} \rightarrow \{1, \dots, k+1\}$ is a bijection. Recall that $k+1 \geq 2$, so $k, k+1 \in \{1, \dots, k+1\}$. By the definition of bijection, there is a unique element $q \in \{1, \dots, m\}$ such that $f(q) = k+1$. Let $A = \{1, \dots, m\} \setminus \{q\}$. Define $f|_A: A \rightarrow \{1, \dots, k\}$ by

$$f|_A(x) = f(x)$$

for all $x \in A$.

(Verify that $f|_A$ is a bijection).

By Exercise 10.1.4 there is a bijection

$$\phi: \{1, \dots, m-1\} \rightarrow \{1, \dots, m\} \setminus \{q\}.$$

Define $f': \{1, \dots, m-1\} \rightarrow \{1, \dots, k\}$ by letting $f' = f|_A \circ \phi$.

(Explain why f' is a bijection).

By our inductive hypothesis, applied with $m' = m-1$, we must have $m-1 = k$. Hence, $m = k+1$, as desired.

Thus, by induction for all $m, n \in \mathbb{N}$, if there is a bijection from $\{1, \dots, m\}$ to $\{1, \dots, n\}$, then $m = n$. □

The next theorem is the result we are after. Construct a short proof using Theorem 10.1.3.

10.1.5

Theorem

If X is a finite set and there is a bijection $\{1, \dots, n\} \rightarrow X$ and a bijection $\{1, \dots, m\} \rightarrow X$, then $n = m$.

The cardinality of a finite set is an example of what is called an “invariant,” namely a number (in this case) which does not change for sets that are “equivalent” from a certain point of view – in this case two sets are “equivalent” if there is a bijection between them. In other settings, different notions of equivalence may be used and in those situations an “invariant” would be a number (or some other mathematical object) assigned to the sets in such a way that equivalent sets get the same number (or other mathematical object).

10.1.6

Exercise

Adapt the proof of Theorem 10.1.3 to show that, for all $m, n \in \mathbb{N}$, if there exists an injection $f: \{1, \dots, m\} \rightarrow \{1, \dots, n\}$ then $m \leq n$. Extend this result to show that if X and Y are finite sets and if there is an injection $f: X \rightarrow Y$, then $|X| \leq |Y|$.

10.1.7

Exercise ▶ (Subsets of finite sets are finite)

Adapt the proof of Theorem 10.1.3 to show that, for all $n \in \mathbb{N}$, if $Y \subset \{1, \dots, n\}$, then Y is finite and $|Y| \leq n$. Remember that this means you need to show that either $Y = \emptyset$ or there is a $p \in \mathbb{N}$ such that $p \leq n$ and a bijection $f: \{1, \dots, p\} \rightarrow Y$. Then extend this result to show that a subset of a finite set is always finite.

10.1.8

Exercise

Suppose that X is a finite set and that $x \in X$. Prove that $|X \setminus \{x\}| = |X| - 1$. Note that this means you must show that if there is a bijection $f: \{1, \dots, n\} \rightarrow X$, then there is a bijection $g: \{1, \dots, n-1\} \rightarrow X \setminus \{x\}$.

10.1.9

Exercise

Let $n \in \mathbb{N}$. Suppose that $Y \subset \{1, \dots, n\}$. Prove that $|Y| + |Y^C| = n$.

10.1.10

Exercise

Let X be a finite set and suppose that $P \subset \mathcal{P}(X)$ is a partition of X . Prove that

$$\sum_{A \in P} |A| = |X|.$$

(Remember to use Definition 10.1.1 when working with $|A|$ and $|X|$!)

Although we are used to comparing sizes of finite sets by counting the number of

elements in each, we can also just match the elements up directly. The following is a useful encapsulation. Parts of the theorem were either previously proved or follow directly from our previous work.

10.1.11 **Theorem ▶ Cardinalities of Finite Sets**

Suppose that X and Y are finite sets. Then

1. $|X| = |Y|$ if and only if there exists a bijection $f: X \rightarrow Y$.
2. $|X| \leq |Y|$ if and only if there exists an injection $f: X \rightarrow Y$.
3. $|X| \geq |Y|$ if and only if there exists a surjection $f: X \rightarrow Y$.
4. For all $n \leq |X|$, there exists a finite set $A \subset X$ such that $|A| = n$.
5. If $|X| \leq |Y|$ and $|Y| \leq |X|$, then $|X| = |Y|$.
6. Either $|X| \leq |Y|$ or $|Y| \leq |X|$.

We also need the following very useful result.

10.1.12 **Theorem**

Suppose that X and Y are finite sets such that $|X| = |Y|$. Then a function $f: X \rightarrow Y$ is an injection if and only if it is a surjection. Thus, every injection and every surjection is also a bijection.

10.2 Infinite Sets

“These are some of those difficulties that derive from reasoning about infinities with our finite understanding, giving to them those attributes that we give to finite and bounded things.” – Galileo [50]

In Theorem 10.1.5, we saw that two finite sets with a bijection between them had the same number of elements. For sets with an infinite number of elements, however, we do not (yet!) have a way of measuring their size. For the remainder of this chapter, we explore the rather surprising consequences of using the notion of “bijection” to govern how we think about the size of infinite sets. We begin by showing the unsurprising result that infinite sets contain finite sets of all sizes. You can prove it by induction or by doing a proof by minimal counterexample.

10.2.1 **Theorem**

X is infinite if and only if for all $n \in \mathbb{N}^*$, there exists $A \subset X$ such that $|A| = n$.

Theorem 10.2.1 gives a characterization of infinite sets (they have subsets of all finite cardinalities). The next theorem provides many more such characterizations. Previous results in this text will be very helpful in proving it.

10.2.2

Theorem ▶ Characterization of Infinite Sets

Suppose that X a set. Then the following are equivalent:

1. X is infinite.
2. There exists an injective sequence in X . (That is, an injective function $\mathbb{N} \rightarrow X$.)
3. If A is a finite set, then there is an injection $A \rightarrow X$.
4. If A is a finite set, then there is no injection $X \rightarrow A$.
5. There exists a surjection $X \rightarrow \mathbb{N}$.
6. For all finite subsets $A \subset X$, there exists a bijection $f: X \rightarrow X \setminus A$.

The cardinality $|A|$ of a finite set A is an extremely useful invariant of the finite set. (After all, we count all sorts of things!) Might there be a similarly useful invariant for infinite sets? We won't define such an invariant directly. Rather we'll define a way of comparing two infinite sets. As in Figure 10.2, we will say two sets have the same cardinality if we can pair up the elements using a bijection.

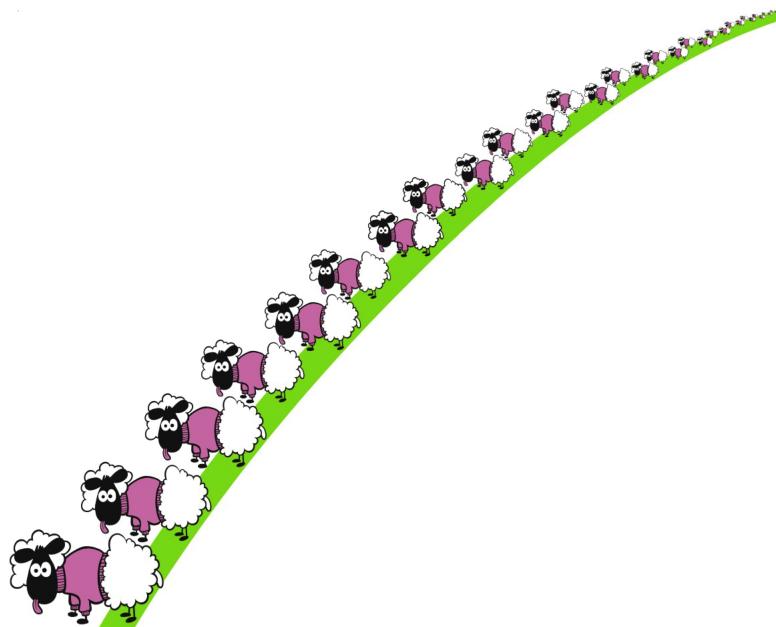


Figure 10.2: There are the same number of sheep as there are sweaters since the act of wearing a sweater determines a bijection from the set of sheep to the set of sweaters.

10.2.3

Definition ▶ Cardinality Relations

Suppose that X and Y are sets. We say that they have **the same cardinality** and write:

$$\text{card } X = \text{card } Y$$

if there is a bijection $X \rightarrow Y$. If there is an injection $X \hookrightarrow Y$, we say that **the cardinality of X is at most the cardinality of Y** and write

$$\text{card } X \leq \text{card } Y.$$

If there is a surjection $X \twoheadrightarrow Y$, we say that **the cardinality of X is at least the cardinality of Y** and write

$$\text{card } X \geq \text{card } Y.$$

10.2.4

Warning

In Definition 10.2.3 we have not actually defined $\text{card } X$, although we have previously defined it (and denoted it by $|X|$) in the case when X is a finite set. Definition 10.2.3 should be thought of as setting forth the phrase “ $\text{card } X = \text{card } Y$ ” to be a short hand for the phrase “there is a bijection from X to Y ”. Similarly, “ $\text{card } X \leq \text{card } Y$ ” is short hand for “there is an injection from X to Y .”

10.2.5

Exercise

Prove the following (perhaps by appealing to previous results):

1. $\text{card } \mathbb{N} = \text{card } 2\mathbb{N}$ (where $2\mathbb{N}$ is the set of even natural numbers)
2. $\text{card } \mathbb{N} = \text{card } \mathbb{Z}$
3. $\text{card } \mathbb{R} = \text{card } (0, 1)$ (where $(0, 1)$ is the open interval in \mathbb{R})
4. If X is infinite, then $\text{card } \mathbb{N} \leq \text{card } X$.
5. $\text{card } \mathbb{N} \leq \text{card } \mathbb{R}$
6. If $A \subset X$, then $\text{card } A \leq \text{card } X$.
7. For any set X , $\text{card } X \leq \text{card } \mathcal{P}(X)$.

Prove the next result by appealing to facts about bijections.

10.2.6

Theorem

The notion “having the same cardinality” is an equivalence relation on sets. That is:

1. (Reflexive) For all sets X , $\text{card } X = \text{card } X$.
2. (Symmetric) For all sets X and Y , if $\text{card } X = \text{card } Y$, then $\text{card } Y = \text{card } X$.
3. (Transitive) For all sets X , Y , and Z , if $\text{card } X = \text{card } Y$ and $\text{card } Y = \text{card } Z$, then $\text{card } X = \text{card } Z$.

Theorem 10.2.6 shows that, with regard to the symbol “=”, the cardinalities of infinite sets behave exactly like the cardinalities of finite sets. What about with regard to the symbols \leq and \geq ? Here the situation is more complicated. We start with a warm-up exercise and then proceed to the important Theorem 10.2.8. Aspects of its proof are relatively straightforward and aspects are very difficult. Theorem 10.1.11 covers the case when X and Y are finite.

10.2.7

Exercise

For each of the statements in the following theorem, come up with a slogan that captures the essence of the theorem. For instance, the first one might be summarized as “When it comes to comparing cardinalities, surjections are nearly as good as injections.”

10.2.8

Theorem ▶ Comparing Cardinalities

The following hold for all sets X and Y :

1. If X is nonempty, then $\text{card}(X) \leq \text{card}(Y)$ if and only if $\text{card}(Y) \geq \text{card}(X)$.
2. If $\text{card}(X) \leq \text{card}(Y)$ and $\text{card}(Y) \leq \text{card}(Z)$, then $\text{card}(X) \leq \text{card}(Z)$.
3. If $\text{card}(X) \leq \text{card}(Y)$, then there exists $A \subset Y$ such that $\text{card}(X) = \text{card}(A)$.
4. If $\text{card}(X) \leq \text{card}(Y)$ and $\text{card}(Y) \leq \text{card}(X)$, then $\text{card}(X) = \text{card}(Y)$.
5. Either $\text{card}(X) \leq \text{card}(Y)$ or $\text{card}(Y) \leq \text{card}(X)$.

Proof. ⟨ Prove the first statement; perhaps by appealing to a previously proved theorem. ⟩

⟨ Prove the second statement; perhaps by appealing to a previously proved theorem. ⟩

⟨ Prove the third statement. ⟩

The fourth statement is called the Cantor-Bernstein Theorem. We state it separately as Theorem 10.6.1 and prove it below.

The fifth statement is equivalent to the Axiom of Choice (which we discussed in Chapter 6.) It follows immediately from the definition of $\text{card}(X) \leq \text{card}(Y)$ and Theorem 9.5.19. □

We conclude with an exercise which will be useful in the next section.

10.2.9

Exercise

Suppose that $\text{card } X = \text{card } A$ and $\text{card } Y = \text{card } B$. Prove that $\text{card } X \times Y = \text{card } A \times B$.

10.3 Countable Sets

“Only professional mathematicians learn anything from proofs. Other people learn from explanations.” - Ralph Boas¹

The importance of the set of natural numbers suggests that it might be useful to give names to sets having the same cardinality as \mathbb{N} .

10.3.1

Definition ► Countability and the Continuum

A set X which is either finite or for which $\text{card } X = \text{card } \mathbb{N}$ is called **countable**. If a set is not countable, it is **uncountable**. If $\text{card } X = \text{card } \mathbb{N}$ we say that $\text{card } X = \aleph_0$.

The letter \aleph (pronounced “aleph”) is the first letter of the Hebrew alphabet. Aleph with a subscript is traditionally used to denote certain types of cardinalities.

The reason the term “countable” is used is because a bijection $f: \{1, \dots, n\} \rightarrow X$ or $f: \mathbb{N} \rightarrow X$ is just a way of counting the elements of X . Such a bijection produces a list x_1, x_2, \dots of the elements of X . The list is either finite or infinite, but in either case every element from X appears in the list and no element appears twice. The following theorem is very useful for showing that certain sets are countable. It is a rephrasing of theorems you have already encountered. You will especially want to make use of Theorem 9.4.7 and recall that a sequence is just a function whose domain is \mathbb{N} .

¹Ralph Boas (1912-1992) is best known for his excellent mathematical exposition. The quote is from [16].

10.3.2

Theorem ▶ Characterization of Countable Sets

Suppose that $X \neq \emptyset$. Then the following are equivalent:

1. X is countable
2. $\text{card } X \leq \text{card } \mathbb{N}$
3. If A is an infinite countable set, then there exists an injection $X \rightarrow A$.
4. There exists an infinite countable set A such that there exists a surjection $A \rightarrow X$.
5. There is a countable set A such that $X \subset A$.

The cardinalities of infinite sets behave somewhat strangely when compared to the cardinalities of finite sets. We exhibit this with a collection of important examples.

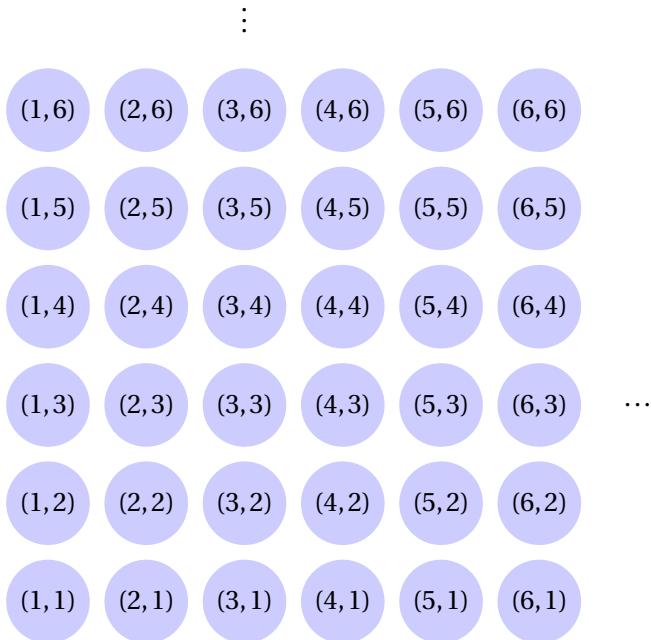
10.3.3

Theorem ▶ Cantor Snake

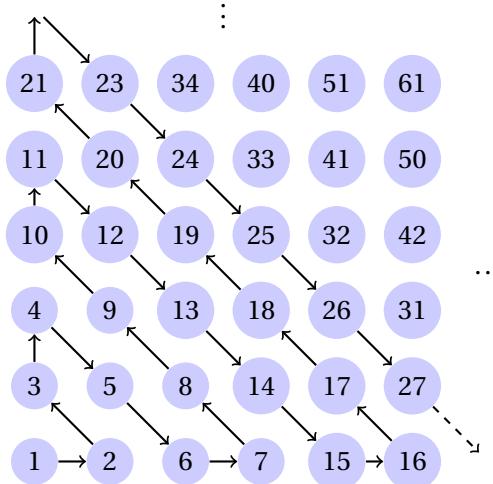
$$\text{card}(\mathbb{N} \times \mathbb{N}) = \text{card}(\mathbb{N}).$$

We give two proofs. The first one lacks sufficient detail for some tastes, but is well-known. The second uses the fact that natural numbers (other than 1) have unique prime factorizations (Theorem 9.3.8.)

Proof of Theorem 10.3.3 (version 1: The Cantor Snake). We will exhibit a bijection $CS: \mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$. To define CS , arrange the elements of $\mathbb{N} \times \mathbb{N}$ in a grid:



We define $CS: \mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$ by weaving, snake-like, diagonally back and forth through the grid, letting $CS(k)$ be the k th point of $\mathbb{N} \times \mathbb{N}$ we encounter, as in the diagram below:



It is clear from the picture that CS is a bijection, and so $\text{card } \mathbb{N} = \text{card } \mathbb{N} \times \mathbb{N}$. □

10.3.4 Exercise

What makes the Cantor Snake proof less than satisfactory? Can you rewrite it so as to remedy the flaws? Can you give a precise (perhaps recursive) definition of CS ?

Proof of Theorem 10.3.3 (version 2). We begin by constructing a bijection $f: \mathbb{N} \times \mathbb{N} \rightarrow A \subset \mathbb{N}$ where $A \subset \mathbb{N}$. Define $f(n, m) = 2^n 3^m$. If $f(n, m) = f(x, y)$, we have $2^n 3^m = 2^x 3^y$. By the uniqueness of prime factorizations (Theorem 9.3.8), $n = x$ and $m = y$. Thus, $f: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ is an injection. By Theorem 10.3.2, $\mathbb{N} \times \mathbb{N}$ is countable. Since it is also infinite, by the definition of “countable,” $\text{card } \mathbb{N} \times \mathbb{N} = \text{card } \mathbb{N}$. □

10.3.5 Exercise

Does the Cantor Snake proof have any advantages over the proof using prime factorizations?

The countability of $\mathbb{N} \times \mathbb{N}$ can then be used to prove that the following important theorem.

10.3.6

Theorem

The following sets are all countable:

1. $\mathbb{Z} \times \mathbb{Z}$
2. \mathbb{Q}
3. $\underbrace{A \times A \times \cdots \times A}_{n \text{ times}}$ where A is any countable set and $n \in \mathbb{N}$.

We conclude with another very useful theorem.

10.3.7

Theorem ▶ The countable union of countable sets is countable

Suppose that \mathcal{A} is a countable set such that for all $A \in \mathcal{A}$, A is a countable set. Then $\bigcup_{A \in \mathcal{A}} A$ is countable.

It is worth trying to construct a proof of this theorem using the Cantor Snake: list the sets in \mathcal{A} horizontally and above each make a vertical list of its elements. We could then attempt to create a bijection as we did using the Cantor Snake. The main challenge is that some of our sets may have only finitely many elements and it may not be clear how to adapt the snake to that situation. Additionally, some of the sets may have nonempty intersection, and so the Cantor Snake may be only a surjection rather than an injection. Furthermore, rather than repeating the same proof that we have already created, it might be better to find a way to simply quote the previous result. Our proof¹ will do that.

Proof. **Special Case:** $\mathcal{A} \neq \emptyset$ and, for all $A \in \mathcal{A}$, $A \neq \emptyset$.

Since \mathcal{A} is countable, by Theorem 10.3.2, there is a surjection $\mathbb{N} \rightarrow \mathcal{A}$. This means that we can list the elements of \mathcal{A} (possibly with repetition) as:

$$A_1, A_2, A_3, \dots$$

For each $i \in \mathbb{N}$, the set A_i is countable, so we can also list its elements (possibly with repetition) as:

$$a_{i,1}, a_{i,2}, a_{i,3}, \dots$$

Thus, $a_{i,j}$ is the j th element of the i th set A_i . Now let $f: \mathbb{N} \times \mathbb{N} \rightarrow \bigcup_{A \in \mathcal{A}} A$ be the function defined by

$$f(i, j) = a_{i,j}$$

for all $(i, j) \in \mathbb{N} \times \mathbb{N}$.

>Show that f is surjective

¹Incidentally, according to [93, Chapter 1.1], Theorem 10.3.7 cannot be proven without some version of the Axiom of Choice. Can you find the place where the Axiom of Choice is used implicitly?

Since $\bigcup_{A \in \mathcal{A}} A$ is the surjective image of a countable set, by Theorem 10.3.2 it is countable.

Finally, we consider the other cases.

If $\mathcal{A} = \emptyset$, then, by definition $\bigcup_{A \in \mathcal{A}} A = \emptyset$. The empty set is countable, so $\bigcup_{A \in \mathcal{A}} A$ is countable. Similarly, if $\emptyset \in \mathcal{A}$, then $\mathcal{A}' = \mathcal{A} \setminus \{\emptyset\}$ is still countable and $\bigcup_{A \in \mathcal{A}} A = \bigcup_{A \in \mathcal{A}'} A$. By our previous work, $\bigcup_{A \in \mathcal{A}} A$ is countable. \square

10.4 Uncountable Sets

“Galileo Galilei
Comes to knock and knock again
At a small secluded doorway
In the ordinary brain.”
– William Jay Smith, *Galileo Galilei* [115]

From the preceding section, it may seem as though every infinite set is countable. This is not so:

10.4.1

Theorem ▶ (0, 1) is uncountable

The interval $(0, 1) \subset \mathbb{R}$ is uncountable. In fact, $\text{card } \mathbb{N} < \text{card } (0, 1)$.

To prove that a non-empty set is uncountable, we must prove that there is no bijection from the set to a finite set or to \mathbb{N} . Not surprisingly, we do this with a proof by contradiction. The argument in the following proof is known as the **Cantor Diagonalization Argument**.

Proof. Suppose, for a contradiction, that the interval $(0, 1)$ is countable. It is clearly infinite, and so we assume that there is a bijection $f: \mathbb{N} \rightarrow (0, 1)$. We will produce a contradiction by showing that f cannot be surjective.

Since for each $k \in \mathbb{N}$, the number $f(k) \in (0, 1)$ has a decimal expansion we may write it with an infinite decimal expansion:

$$f(k) = .a_{k1}a_{k2}a_{k3}a_{k4}a_{k5}a_{k6}\dots$$

If there is not a unique such decimal expansion for $f(k)$ we choose the decimal expansion which ends in repeating 9s rather than in repeating 0s.

We now produce a number $b \in (0, 1)$ such that $b \notin \text{range } f$. We do so by specifying its decimal representation.

For each $n \in \mathbb{N}$, define b_n by:

$$b_n = \begin{cases} 6 & \text{if } a_{nn} = 5 \\ 5 & \text{if } a_{nn} \neq 5 \end{cases}$$

Observe that for all $n \in \mathbb{N}$, $b_n \in \{5, 6\}$. Define

$$b = .b_1b_2b_3b_4\dots$$

Informally, the number b is constructed by “toggling” the diagonal entries of the table of decimal representations of the elements in the range of f :

.	a_{11}	a_{12}	a_{13}	a_{14}	a_{15}	
.	a_{21}	a_{22}	a_{23}	a_{24}	a_{25}	
.	a_{31}	a_{32}	a_{33}	a_{34}	a_{35}	...
.	a_{41}	a_{42}	a_{43}	a_{44}	a_{45}	
.	a_{51}	a_{52}	a_{53}	a_{54}	a_{55}	
						⋮

Since $0 < b_1 < 9$, the number b is an element of $(0, 1)$. Also since the decimal representation of b does not end in repeating 9s or 0s it is the unique decimal representation for b . Since f is surjective, there exists $k \in \mathbb{N}$ such that

$$\cdot a_{k1} a_{k2} a_{k3} a_{k4} a_{k5} a_{k6} \dots = f(k) = b = .b_1 b_2 b_3 b_4 \dots$$

Since the decimal representation of b is unique, for each n we have $a_{kn} = b_n$. In particular, $a_{nn} = b_n$. However, b_n , by definition, differs from a_{nn} . We have, therefore, encountered our contradiction. Hence, f is not surjective and is, therefore, not a bijection. \square

10.4.2 Exercise

Can you rewrite the proof of Theorem 10.4.1 so that it is not a proof by contradiction? (Hint: Show that no injection $f: \mathbb{N} \rightarrow (0, 1)$ can be a surjection.)

10.4.3 Exercise

Prove that the following sets are uncountable:

1. Any interval $[a, b]$, $[a, b)$, $(a, b]$, (a, b) with $a < b$.
2. \mathbb{R}
3. The set of irrational numbers $\mathbb{Q}^C \subset \mathbb{R}$.
4. The set of irrational numbers contained in any open interval in \mathbb{R} .

As another consequence of Theorem 10.4.1 we can answer a question raised in our discussion of circle rotations in Section 8.4.

10.4.4 Theorem

There is no surjective sequence in the unit circle S^1 . In particular, no iterated function sequence arising from a function which is the rotation of the circle by some fixed angle will ever have the property that every point of S^1 appears as some element of the sequence.

As we did with finite sets, infinite sets, and countable sets we can find multiple

characterizations of uncountable sets. The proof of the next theorem is mostly a matter of putting together things you already know.

10.4.5

Theorem ▶ Characterization of Uncountable Sets

Suppose that $X \neq \emptyset$ is a set. Then the following are equivalent.

1. X is uncountable
2. No function $X \rightarrow \mathbb{N}$ is injective
3. No function $\mathbb{N} \rightarrow X$ is surjective
4. If $A \subset X$ is countable, then there exists a bijection $X \rightarrow X \setminus A$.

We conclude with some more examples of uncountable sets. Adapt the Cantor Diagonal argument to prove the next theorem.

10.4.6

Theorem

Let \mathcal{S} be the set of infinite sequences in $\{0, 1\}$. Then \mathcal{S} is uncountable.

10.4.7

Corollary

Suppose that X is an infinite set and that Y is a set with at least two elements. Then the set $\mathcal{F}(X, Y) = \{f: X \rightarrow Y\}$ is uncountable.

10.4.8

Exercise

Give an example of an uncountable set X such that X is the union of countable sets.

10.5 Producing Larger Cardinalities

“Some infinities are bigger than other infinities... There are days, many of them, when I resent the size of my unbounded set. I want more numbers than I’m likely to get, and God, I want more numbers for Augustus Waters than he got. But, Gus, my love, I cannot tell you how thankful I am for our little infinity.”

—John Green, *The Fault in our Stars*

A set X for which $\text{card } X = \text{card } \mathbb{R}$ is said to have **the cardinality of the continuum** and we write $\text{card } X = \mathfrak{c}$. The letter \mathfrak{c} is just “c” written in the Fraktur font - an old German script. It stands for “continuum,” an old name for the set of real numbers. So far, we have not seen sets having cardinality larger than \mathfrak{c} . That is about to change....

10.5.1

Theorem

Suppose that X is a set. Then $\text{card } X < \text{card } \mathcal{P}(X)$.

The proof of this result is reminiscent of Russell's Paradox.

Proof. By Exercise 10.2.5, we know that $\text{card } X \leq \text{card } \mathcal{P}(X)$. It remains to show that $\text{card } X \neq \text{card } \mathcal{P}(X)$; that is, there is no bijection $X \rightarrow \mathcal{P}(X)$.

Suppose, for a contradiction, that there is such a bijection $f: X \rightarrow \mathcal{P}(X)$. Then for each $x \in X$, the set $f(x)$ is a subset of X so we may inquire if $x \in f(x)$ or if $x \notin f(x)$.

Let $R = \{x \in X : x \notin f(x)\}$. Since f is a bijection, there exists $r \in X$ such that $f(r) = R$. We consider two possibilities: either $r \in R$ or $r \notin R$.

(Show that both possibilities lead to contradictions.)

Hence, $\text{card } X < \text{card } \mathcal{P}(X)$. □

10.5.2

Exercise

Back in Section 3.7 and in Theorem 6.1.23 we gave two different proofs that there does not exist a set U such that $A \in U$ if and only if A is a set (i.e. Russell's Paradox). Provide a new proof of that theorem using Theorem 10.5.1.

We now have a way of generating larger and larger cardinalities:

$$\text{card } \mathbb{N} < \text{card } \mathcal{P}(\mathbb{N}) < \text{card } \mathcal{P}\mathcal{P}(\mathbb{N}) < \dots$$

For convenience, let $\mathcal{P}^k(\mathbb{N}) = \underbrace{\mathcal{P}\mathcal{P}\mathcal{P}\dots\mathcal{P}}_{k \text{ times}}(\mathbb{N})$.

This raises some natural questions:

1. Is there a k such that $\mathfrak{c} = \mathcal{P}^k(\mathbb{N})$?
2. Is there a set A such that $\text{card } \mathbb{N} < \text{card } A < \text{card } \mathcal{P}(\mathbb{N})$?
3. For every infinite set X , does there exist some $k \in \mathbb{N}$ such that $\text{card } X = \text{card } \mathcal{P}^k(\mathbb{N})$?

In Section 10.6, we show that $\mathfrak{c} = \text{card } \mathcal{P}(\mathbb{N})$. This means that (examining the second question), if there is a set A such that $\text{card } \mathbb{N} < \text{card } A < \text{card } \mathcal{P}(\mathbb{N})$ then there exists a subset $A \subset \mathbb{R}$ which is uncountable, but whose cardinality is strictly less than the cardinality of \mathbb{R} . Does there exist such a set? The answer to this question, in particular, upended the way people conceived of the relationship between mathematics and truth. We take this up again in Section 10.9.

We conclude this section with some more results on uncountable sets.

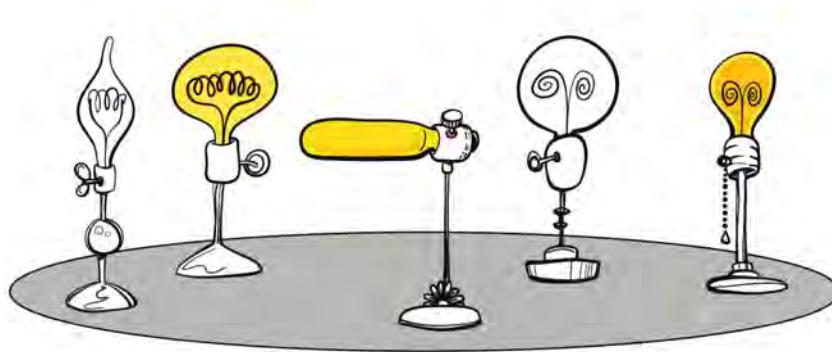


Figure 10.3: A characteristic function determines whether each point in a set is “on” or “off.”

To begin, consider each point of a set X as a lightbulb (see Section 8.2) that can be switched on or off as in Figure 10.3. Choosing a setting for each lightbulb, determines a function $f: X \rightarrow \{0, 1\}$, where $f(x) = 0$ if the bulb at point x is “off” and $f(x) = 1$ if the bulb at point x is “on.” For instance, if $A \subset X$ is a particular collection of lightbulbs, we could decide to turn each of the bulbs in that set “on” and all other bulbs off. This function is called the **characteristic function** of A . More formally, for a subset $A \subset X$, the **characteristic function** of A is the function $\chi_A: X \rightarrow \{0, 1\}$ defined by:

$$\chi_A(x) = \begin{cases} 1 & x \in A \\ 0 & x \notin A \end{cases}.$$

Consider a given function $f: X \rightarrow \{0, 1\}$. It tells us which lightbulbs are on and which are off. If we let $A = \{x \in X : f(x) = 1\}$ be the set of points where the bulbs are on, we see that $f = \chi_A$. (In particular, f and χ_A have the same domain and range and take the same value on each $x \in X$.) For a set X , we let $\chi(X)$ denote the set of characteristic functions of subsets of X :

$$\chi(X) = \{\chi_A : A \subset X\}.$$

Observe that $\chi(X)$ is exactly the set of functions from X to the set $\{0, 1\}$.

10.5.3

Theorem

$$\text{card } \mathcal{P}(X) = \text{card } \chi(X).$$

Proof. Define $h: \mathcal{P}(X) \rightarrow \chi(X)$ by $h(A) = \chi_A$ for all subsets $A \subset X$. We claim that h is a bijection.

(Complete the proof or appeal to a previous result)

□

Finally, here is a variant (taken from [84, Corollary 7.13]) of Theorem 10.5.1.

10.5.4

Theorem

Suppose that Y is a set such that there is a function $\tau: Y \rightarrow Y$ with the property that for all $y \in Y$, $\tau(y) \neq y$. If X is any set, let $\mathcal{F}(X, Y)$ denote the set of functions with domain X and codomain Y . Then, for every function $\Phi: X \rightarrow \mathcal{F}(X, Y)$, Φ is not surjective.

If Y satisfies the hypothesis of Theorem 10.5.4 we say that Y **admits a self-map without fixed points**. It follows from Theorem 10.5.1 and Theorem 10.5.3 that the cardinality of the set of characteristic functions on a set X is not equal to the cardinality of X (for any set X .) Since the set $\{0, 1\}$ admits a self-map without fixed points (namely the transposition interchanging 0 and 1) Theorem 10.5.4 gives another proof of that fact.

10.6 The Cantor-Bernstein Theorem

“The hope of pleasure in the work itself: how strange that hope must seem to some of my readers – to most of them! ... [A person] at work, making something which he feels will exist because he is working at it and wills it, is exercising the energies of his mind and soul as well as of his body. Memory and imagination help her as she works. Not only her own thoughts, but the thoughts of the people of past ages guide her hands; and, as a part of the human race she creates.”

– William Morris¹

In Section 10.2, we asked whether it is true that if $\text{card } X \leq \text{card } Y$ and $\text{card } Y \leq \text{card } X$, then $\text{card } X = \text{card } Y$. If the answer is “yes,” then this is more evidence that our notion of cardinality is a good mental model for the “size” of a set.

10.6.1

Theorem ▶ Cantor-Bernstein

Suppose that X and Y are sets such that $\text{card } X \leq \text{card } Y$ and $\text{card } Y \leq \text{card } X$. Then $\text{card } X = \text{card } Y$.

The proof we give is due, in essence, to Julius König and can be found in [4]. Before beginning, recall that if $f: A \rightarrow A$ is function, then for $k \in \mathbb{N}^*$, the notation f^k indicates the function obtained by composing f with itself k times. The function f^0 is the identity function.

Proof. If necessary, by replacing X and Y with $X \times \{0\}$ and $Y \times \{1\}$, we may assume that $X \cap Y = \emptyset$.

⟨ Explain why this replacement doesn't affect the truth value of the theorem. ⟩

¹William Morris (1834 - 1896) is best known as the founder of the Arts and Crafts movement. This is from a talk, reprinted in [95], devoted to articulating a vision for work which is life-giving to all members of society. I have changed some of the pronouns to broaden its relevance.

Since $\text{card } X \leq \text{card } Y$, there is an injection $f: X \hookrightarrow Y$. Similarly, since $\text{card } Y \leq \text{card } X$ there is an injection $g: Y \hookrightarrow X$. We must construct a bijection $X \rightarrow Y$. We begin by creating a certain partition of $X \cup Y$.

Let $z, z' \in X \cup Y$. Define $z \sim z'$ if and only if there exists

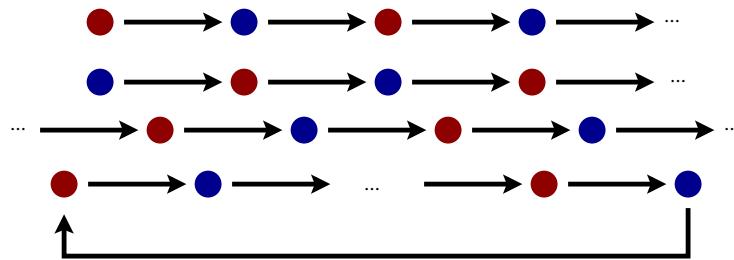
$$h \in \{f \circ (g \circ f)^k, (g \circ f)^k, g \circ (f \circ g)^k, (f \circ g)^k : k \in \mathbb{N}^*\}$$

so that one of the following holds:

- $h(z) = z'$
- $h(z') = z$.

(Prove that \sim is an equivalence relation on $X \cup Y$.)

Recall that the set of equivalence classes are a partition of $X \cup Y$. The equivalence class of an element $z \in X \cup Y$ can be categorized based on what happens when we repeatedly apply f and g . There are essentially four types of sets, indicated in the diagram below. The red dots represent elements of X and the blue dots represent elements of Y and the arrows represent the functions f and g (with f taking red dots to blue and g taking blue dots to red.)



We say that an equivalence class $[z]$ (for some $z \in X \cup Y$) **begins** at $y \in Y$, if $y \in [z]$ and $y \notin \text{range } f$. Define $h: X \rightarrow Y$ by defining $h(x)$, for $x \in X$, as follows:

$$h(x) = \begin{cases} f(x) & \text{if } [x] \text{ does not begin at any } y \in Y \\ y & \text{if there exists } y_0 \in [x] \text{ s.t. } [x] \text{ begins at } y_0 \text{ and } g(y) = x. \end{cases}$$

We claim that h is well-defined and that it is a bijection.

(Prove it!).

□

10.6.2

Exercise

Where in the proof of the Cantor-Bernstein Theorem do we use the fact that f and g are injections? Where do we use our assumption that $X \cap Y = \emptyset$?

We now turn to some of the consequences of the Cantor-Bernstein Theorem.

10.6.3

Theorem ▶ $\text{card } \mathbb{R} = \text{card } \mathcal{P}(\mathbb{N})$

$$\text{card } \mathbb{R} = \text{card } \mathcal{P}(\mathbb{N})$$

For simplicity, we will use the fact that every real number $r \in (0, 1)$ has a binary decimal representation:

$$b = ._2 b_1 b_2 b_3 b_4 \dots = \sum_{i=1}^{\infty} \frac{b_i}{2^i}$$

with $b_i \in \{0, 1\}$ for each $i \in \mathbb{N}$. Furthermore, the binary decimal representation is unique unless it terminates in repeating 0s or 1s.

Proof. Recall that $\text{card}(0, 1) = \text{card } \mathbb{R}$, so it suffices to show that $\text{card}(0, 1) = \text{card } \mathcal{P}(\mathbb{N})$. By the Cantor-Bernstein Theorem, we need only show that $\text{card}(0, 1) \leq \text{card } \mathcal{P}(\mathbb{N})$ and $\text{card } \mathcal{P}(\mathbb{N}) \leq \text{card}(0, 1)$.

$\text{card}(0, 1) \leq \text{card } \mathcal{P}(\mathbb{N})$: We construct an injection $f: (0, 1) \hookrightarrow \mathcal{P}(\mathbb{N})$ as follows. For $b \in (0, 1)$, let

$$b = ._2 b_1 b_2 b_3 b_4 \dots$$

be its binary decimal representation. If there is more than one such, choose the one which terminates in repeating 1s. Let $f(b) = \{i \in \mathbb{N} : b_i = 1\}$.

We claim that f is injective.

(Show that f is injective)

Consequently, $\text{card}(0, 1) \leq \text{card } \mathcal{P}(\mathbb{N})$.

$\text{card } \mathcal{P}(\mathbb{N}) \leq \text{card}(0, 1)$: We construct an injection $g: \mathcal{P}(\mathbb{N}) \hookrightarrow (0, 1)$. Let $A \subset \mathbb{N}$.

Let $b_i = \begin{cases} 3 & i \notin A \\ 4 & i \in A \end{cases}$. Then define

$$g(A) = \sum_{n \in A} \frac{b_i}{10^n}.$$

(The sum over the empty set is 0). Since for all $A \subset \mathbb{N}$, the number $g(A)$ has a decimal representation with only 3s and 4s, it has a unique decimal representation. Thus, $g(A) = g(B)$ if and only if $A = B$. Hence, g is injective. \square

10.6.4

Exercise

Let $(0, 1) \subset \mathbb{R}$. Then $\text{card}(0, 1) \times (0, 1) = \text{card } \mathbb{R} \times \mathbb{R}$.

Here is another result (originally due to Cantor) whose proof we again adapt from [4].

10.6.5

Theorem

$$\text{card } \mathbb{R} \times \mathbb{R} = \text{card } \mathbb{R}.$$

Proof. Once again we use the Cantor-Bernstein Theorem. Clearly, $\text{card } \mathbb{R} \leq \text{card } \mathbb{R} \times \mathbb{R}$ since $x \mapsto (x, 0)$ gives an injection. To finish the proof, we show $\text{card } \mathbb{R} \times \mathbb{R} \leq \text{card } \mathbb{R}$. By the previous exercise, it suffices to show that $\text{card } (0, 1) \times (0, 1) \leq \text{card } (0, 1)$.

For a numbers $a, b \in (0, 1)$, let

$$\begin{aligned} a &= .a_1 a_2 a_3 \dots \\ b &= .b_1 b_2 b_3 \dots \end{aligned}$$

Define $f(a, b) = .a_1 b_1 7 a_2 b_2 7 a_3 b_3 7 \dots$ (in decimal, not binary decimal, notation). Since the decimal expression for $f(a, b)$ does not terminate in all 0s or 9s, $f(a, b)$ has a unique decimal representation for all $(a, b) \in (0, 1) \times (0, 1)$. In particular, $0 < f(a, b) < 1$ and so $f: (0, 1) \times (0, 1) \rightarrow (0, 1)$ is a function.

We claim that f is an injection. To see this, suppose that $f(a, b) = f(a', b')$. Then:

$$.a_1 b_1 7 a_2 b_2 7 a_3 b_3 7 \dots = a'_1 b'_1 7 a'_2 b'_2 7 a'_3 b'_3 7 \dots$$

Since such decimal representations are unique, it is easy enough to match up terms to conclude that $a = a'$ and $b = b'$. Hence, f is an injection and $\text{card } \mathbb{R} \times \mathbb{R} \leq \text{card } \mathbb{R}$. \square

10.7 Application: Transcendental Numbers

“She had caught a glimpse of something majestic. Hiding between all the ordinary numbers was an infinity of transcendental numbers whose presence you would never have guessed unless you looked deeply into mathematics. Every now and then one of them, like π , would pop up unexpectedly in everyday life. But most of them – an infinite number of them, she reminded herself – were hiding, minding their own business, almost certainly unglimped by the irritable Mr. Weisbrod.” - Carl Sagan¹, *Contact*

We can use the fact that \mathbb{R} is uncountable to prove the existence of certain types of numbers, called *transcendental numbers*. These existence proofs are non-constructive: they do not allow us to know that any specific number is transcendental. We warm up by considering the irrationals.

¹Carl Sagan (1934-1996) was an astronomer, skeptic, and well-known science communicator. *Contact* is a science fiction novel that was later turned into a movie.

10.7.1

Theorem ▶ Irrationals are uncountable

The set \mathbb{Q}^c of irrational real numbers is uncountable. In fact, for every open interval $(a, b) \subset \mathbb{R}$, $\mathbb{Q}^c \cap (a, b)$ is uncountable.

(Hint: Do a proof by contradiction and use the fact that the union of countable sets is countable.)

Back in Chapter 1, we proved that $\sqrt{2}$ was irrational, so the existence of irrational numbers is nothing new. However, Theorem 10.7.1 which says that the irrationals are uncountable, does produce the rather counter-intuitive consequence: there are “more” irrationals than rationals. To get a sense for why this is counter-intuitive, note the following:

Claim 1: Whenever $a < b$ are rational, there exists an irrational s between them. That is, $s \in (a, b)$.

Claim 1 follows immediately from the fact that $(a, b) \cap \mathbb{Q}^c$ is uncountable and, therefore, non-empty.

Claim 2: Whenever $a < b$ are irrational, there exists a rational r between them. That is $r \in (a, b)$.

To see that Claim 2 holds, let $a = .a_1 a_2 \dots$ and $b = .b_1 b_2 \dots$ be their decimal expansions. Suppose that index i is the first place where $a_i \neq b_i$. Since $a < b$, $a_i < b_i$. Let $j > i$ be the first index after i where $a_j \neq b_j$. Such an index exists since a is irrational. The decimal

$$.a_1 a_2 \dots a_i a_{i+1} \dots a_{j-1} 9 0 0 0 \dots$$

is then a rational number between a and b .

As a result of Claims 1 and 2 we know that between any two rationals there is an irrational and between any two rationals there is an irrational. So our intuition tells us that the rationals and irrationals should “alternate” on the number line. However, Theorem 10.7.1 tells us that there are uncountably many irrationals and we already knew there were only countably many rationals. So even though the rationals and irrationals seem to “alternate” there are “more” irrationals than rationals.

The solution to this conundrum is to realize that we only have intuition for *countable sets*. The fact that \mathbb{R} is uncountable means that it simply doesn’t make sense to think about the rationals and irrationals “alternating”. Indeed, notice that for the even and odd integers which do genuinely alternate, there is a function taking each even integer to the next biggest odd integer and another function which takes each odd integer to the next smallest even integer – these functions give bijections between the evens and the odds. For an irrational number s , however, there is no “next biggest” rational and, similarly, for a rational “r” there is no “next smallest” irrational, so the alternating analogy simply doesn’t apply to the rationals and irrationals.

The term “dense” in the next definition captures the relationship between rationals and irrationals better. Claims 1 and 2 show that the irrationals and rationals

are both dense.

10.7.2

Definition ► Dense in \mathbb{R}

A subset $X \subset \mathbb{R}$ is **dense** (in \mathbb{R}) if for every open interval $(a, b) \subset \mathbb{R}$ (with $a < b$) there exists $x \in X \cap (a, b)$.

We can increase the surprise by considering two other complementary sets of real numbers:

10.7.3

Definition ► Algebraic and Transcendental

Suppose that $r \in \mathbb{R}$. Then r is **algebraic** if there exist $a_0, \dots, a_n \in \mathbb{Q}$, not all zero, such that for the polynomial

$$p(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$$

we have $p(r) = 0$. (That is, r is a root of a polynomial with rational coefficients.) A number $r \in \mathbb{R}$ is **transcendental** if it is not algebraic.

10.7.4

Example

The following numbers are all algebraic. Can you find the non-zero polynomials with rational coefficients for which they are a root?

1. a/b where $a, b \in \mathbb{N}$.
2. \sqrt{n} for every $n \in \mathbb{N}$.
3. $\sqrt{5} + \sqrt{3}$.

We will prove that the algebraic numbers are countable and, therefore, that the transcendental numbers are uncountable. We begin with a few lemmas. The first one is a consequence of Theorem 10.3.6.

10.7.5

Lemma

For each $n \in \mathbb{N}$, the n -fold cartesian product $\mathbb{Q}^n = \{(x_1, x_2, \dots, x_n) : x_i \in \mathbb{Q}\}$ is countable.

10.7.6

Lemma

For all $n \in \mathbb{N}$, the set P_n of polynomials of degree¹ at most n having rational coefficients is countable.

(Hint: Construct an injection from P_n to \mathbb{Q}^{n+1})

10.7.7

Lemma

The set of all polynomials P having rational coefficients is countable.

¹Recall that the degree of a polynomial $a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$ is n if $a_n \neq 0$.

We also need the following result; its proof is too involved to go into here.

10.7.8 **Theorem ▶ Polynomials have finitely many roots**

A polynomial $p(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ which is not the zero polynomial has at most n roots.

Proof. ⟨ The proof is beyond the scope of this text. ⟩ □

10.7.9 **Theorem ▶ Algebraic Numbers are Countable**

The set \mathbb{A} of algebraic real numbers is countable.

Proof. Let P be the set of non-zero polynomials having rational coefficients. By Lemma 10.7.7, the set P is countable. For $p \in P$, let R_p be the set of roots of p . By the Fundamental Theorem of Algebra, for each $p \in P$, the set R_p is finite. By the definition of \mathbb{A} ,

$$\mathbb{A} = \bigcup_{p \in P} R_p.$$

Since this is the countable union of countable sets, \mathbb{A} is countable. □

10.7.10 **Corollary ▶ The set of transcendentals is uncountable**

The set \mathbb{A}^c of transcendental numbers is uncountable. Indeed, for every open interval $(a, b) \subset \mathbb{R}$ with $a < b$, the set $\mathbb{A}^c \cap (a, b)$ is uncountable.

Proof. Let $a < b$ and let I be either (a, b) or \mathbb{R} . Suppose that $\mathbb{A}^c \cap I$ is countable. Since subsets of countable sets are countable and since \mathbb{A} is countable, the set $\mathbb{A} \cap I$ is countable. Then $I = (\mathbb{A} \cap I) \cup (\mathbb{A}^c \cap I)$ is the union of two countable sets and is, therefore, countable. But this contradicts the fact that I is uncountable. □

One intriguing consequence of Corollary 10.7.10 is that there exists a transcendental number, even though it doesn't produce a specific example. It turns out that the numbers π , e , $\sin(1)$, $\ln(2)$, etc. are transcendental numbers; however the proofs that they are transcendental are very difficult. There remain many interesting open questions about transcendental numbers.

In many applications of mathematics, there is a need for random numbers. Unfortunately, it is very difficult to generate truly random numbers via a mechanical process (such as on a computer) and so usually *pseudo-random numbers* are used. These are numbers that are chosen in a predictable fashion from a non-predictable sequence. For instance, one might choose a list of pseudo-random numbers to be the digits of π , or some other number. Since rational numbers have predictable decimal expansion (they eventually repeat), it would be a bad idea to use the digits of a rational number to generate pseudo-random numbers. The paper [80] shows that it would also be a bad idea to choose the digits of an algebraic number (or certain kinds of transcendental numbers.)

10.8 Application: Countable Sets and Probability

“All things proceed from the Nothing, and are borne towards the Infinite. Who will follow these marvellous processes? The Author of these wonders understands them. None other can do so.”

-Blaise Pascal¹, *Pensées* 72

If you are asked to pick a “random” real number in the interval $(-10, 10)$, what would you choose? 7? -5? $13/27$? Chances are the number you pick will be rational. (Of course, you might pick π or e , but then that choice wouldn’t be random, now would it?) To make randomness precise, as discussed in Sections 5.7 and 8.10, we need to pick a probability space for the real numbers. As a reminder, a probability space (X, \mathcal{E}, P) consists of a set X , an event space $\mathcal{E} \subset \mathcal{P}(X)$ (satisfying certain axioms), and a function $P: \mathcal{E} \rightarrow [0, 1]$ also satisfying certain axioms. The event space \mathcal{E} must satisfy:

(E1) $\emptyset, X \in \mathcal{E}$

(E2) If $A \in \mathcal{E}$, then $A^c \in \mathcal{E}$

(E3) If Λ is countable and if $A_\lambda \in \mathcal{E}$ for every $\lambda \in \Lambda$, then $\bigcup_{\lambda \in \Lambda} A_\lambda \in \mathcal{E}$.

An element of \mathcal{E} is said to be an **event**. The criterion (E3) can be summarized by saying that the countable union of events is an event. (We phrased this slightly differently in Definition 5.7.20.) The function P is required to have the properties that $P(\emptyset) = 0$, $P(X) = 1$, and $P(\bigcup_{\lambda \in \Lambda} A_\lambda) = \sum_{\lambda \in \Lambda} P(A_\lambda)$ whenever $\{A_\lambda : \lambda \in \Lambda\}$ is a countable collection of pairwise disjoint events.

Henceforth, let $X = (a, b) \subset \mathbb{R}$ with $a < b$.

10.8.1 Exercise

Show that for any number $x_0 \in X$, there exists an event space \mathcal{E} on X and a probability function P such that for all $A \subset X$, $P(A) = 1$ if and only if $x_0 \in A$.

Such probability spaces are clearly biased towards the number x_0 . In order to be as unbiased as possible we will consider “uniform probability spaces” on subsets of \mathbb{R} .

10.8.2 Definition ▶ Open subsets

Suppose that $X \subset \mathbb{R}$. A subset $U \subset X$ is **open** if for every $x \in U$, there is an open interval $(a, b) \subset \mathbb{R}$ such that $x \in (a, b)$ and $(a, b) \cap X \subset U$.

¹Blaise Pascal (1623-1662) was a philosopher, mathematician, scientist, and religious author. He, along with Pierre Fermat, is credited with creating probability theory. In his philosophical work *Pensées* he lays out the controversial argument (now known as Pascal’s wager), which uses rudimentary probability theory and notions of the infinite, for the existence of God.

For example, if $X = (0, 1)$, then the open subsets of X are just the unions of open intervals which are subsets of X . If $X = [0, 2\pi]$ then the interval $[0, 1)$ is also open, since $[0, 1) = (-1, 1) \cap X$. The set $[0, 1) \cup (1, 2\pi]$ is also open in $[0, 2\pi]$.

For a finite length interval $X \subset \mathbb{R}$ then there is a very special event space defined for X :

10.8.3

Definition ▶ Borel Event Space

If $X \subset \mathbb{R}$ be a bounded interval of the form (a, b) , $[a, b)$, $(a, b]$, or $[a, b]$, the **Borel Event Space** is the smallest event space \mathcal{E} on X such that every interval and every open set in X is an event. A probability function P on \mathcal{E} is **uniform** if whenever I is an interval of the form (x, y) , for $a \leq x < y \leq b$ then

$$P((x, y)) = \frac{y - x}{b - a}$$

(that is, $P(I)$ is the proportion of the interval X occupied by I .) We say that (X, \mathcal{E}, P) is a **uniform probability space**.

It is a fact that given such X and its Borel Event Space, there exists a unique uniform probability function defined on X .

10.8.4

Example

Let $X = [0, 2\pi]$ and consider the Borel Event Space on X with the uniform probability function P . Then every interval in X is an event and we can calculate the probability of each interval. For example:

- $P((0, \pi)) = \frac{\pi - 0}{2\pi - 0} = \frac{1}{2}$.
- $P(\{0, 2\pi\}) = 1 - P((0, 2\pi)) = 1 - 1 = 0$. Since $\{0\}$ and $\{2\pi\}$ are subsets of $\{0, 2\pi\}$ we have $P(\{0\}) = P(\{2\pi\}) = 0$.
- For $y > 0$, we have

$$P([0, y]) = P(\{0\} \cup (0, y)) = P(\{0\}) + P((0, y)) = P((0, y)) = y/2\pi.$$

10.8.5

Exercise

Suppose that X is an interval in \mathbb{R} with a uniform probability function P and nonzero length. Prove that for every $x \in X$, the set $\{x\}$ is an event and that $P(\{x\}) = 0$.

We can interpret the previous exercise as saying that if we choose in advance what element of the interval X we are hoping to choose, then the probability that we choose that particular element is equal to 0.

10.8.6

Exercise

Suppose that X is an interval in \mathbb{R} with a uniform probability function P and nonzero length ℓ . Let $[x, y] \subset X$ be an interval with $y \geq x$. Prove that

$$P([x, y]) = \frac{y - x}{\ell}$$

(Hint: The definition of P tells you that this is the correct formula if were to calculate the probability of the *open* interval (x, y) . You are to prove that it is also the correct formula for the closed interval.)

10.8.7

Exercise

Suppose that X is a closed, bounded interval in \mathbb{R} having a Borel event space and uniform probability function P . Suppose that $A \subset B \subset X$ are both Borel sets (not necessarily intervals). Show that $P(A) \leq P(B)$.

The goal of this section is to prove the next theorem.

10.8.8

Theorem

If (X, \mathcal{E}, P) is a uniform probability space, and if $Y \subset X$ is countable, then $Y \in \mathcal{E}$ and $P(Y) = 0$.

One consequence of this result is that if ‘randomness’ is defined using a uniform probability space, then the probability of randomly choosing an algebraic number is 0 while the probability of choosing a transcendental number is 1. Yet, if you ask someone for a random number in the interval $(0, 1)$, they will almost always give you an algebraic number! Before working out the proof, we consider an example which contains all the important features.

10.8.9

Example

Suppose that $X = [0, 2\pi]$ and consider the Borel Event Space on X with the uniform probability function P . Let

$$Y = \{1, 1/2, 1/3, 1/4, 1/5, 1/6, \dots\}.$$

We will first show that Y is an event and then that its probability is 0.

Let $y_n = 1/n$. By Exercise 10.8.5, $\{y_n\}$ is an event with $P(\{y_n\}) = 0$.

\langle Explain why $Y = \bigcup_{n \in \mathbb{N}} \{y_n\}$ is an event. \rangle

\langle Explain why $P(Y) = 0$. \rangle

10.8.10

Exercise

Prove Theorem 10.8.8

10.9 The cardinal numbers

“He added all the numbers he knew,
multiplied them by new-found numbers
and called it a prayer of Numbers.”
– Carl Sandburg, *Number Man*

So far, we have seen how injections can be used to treat the sizes of infinite sets like numbers. For example, for nonempty sets A, B, C , we know that if $\text{card}(X) \leq \text{card}(Y)$ and $\text{card}(Y) \leq \text{card}(X)$, then $\text{card}(X) = \text{card}(Y)$ (The Cantor-Bernstein Theorem). This and our other results, suggest that \leq is a relation on cardinalities much like the corresponding relation \leq on \mathbb{N} . But, we have given no definition of what we mean by $\text{card}(X)$! So we have a relation (of sorts) but it doesn't relate things! In this section, we (partially) rectify that.

As we are learning, (almost) any mathematical idea can be expressed in terms of sets. In Section 6.3, we saw how the extended natural numbers \mathbb{N}^* can be derived from set theory. In that section, we defined the **successor** of a set A to be the set

$$S(A) = A \cup \{A\}.$$

We then defined individual natural numbers, as follows:

- Define $0 = \emptyset$.
- Define $1 = S(0) = \emptyset \cup \{\emptyset\} = \{\emptyset\}$.
- Define $2 = S(1) = 1 \cup \{1\} = \{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\}$.
- Define $3 = S(2) = \{\emptyset, \{\emptyset\}, 2\}$
- etc.

Using this process we can define any particular natural number we wish. To define 1101, for example¹, we would first define the numbers 0 through 1100 and then define $1101 = 1100 \cup \{1100\}$. In Section 6.3, we used the axioms of set theory to construct the *set* of extended natural numbers \mathbb{N}^* and we showed that $(\mathbb{N}^*, 0, S)$ is a natural number system. Notice that with this approach, each natural number is a set and, by our definition of finite cardinalities (Definition 10.1.1), for each $n \in \mathbb{N}^*$, $|n| = n$. When we count a finite set X having n elements, we are establishing a bijection between the set X and the set $n = \{0, 1, \dots, n - 1\}$.

Likewise, when we list the elements of an infinite countable set X , starting with 0, say, we are establishing a bijection between $\mathbb{N}^* = \{0, 1, 2, \dots\}$ and X . Since we are using \mathbb{N} as a method of counting (and not paying attention to any of its arithmetical properties) we use the new symbol \aleph_0 to denote it. That is, define $\aleph_0 = \mathbb{N}$. We previously used the notation

$$\text{card } X = \aleph_0$$

¹When my younger son was 5 he claimed that this number doesn't actually exist. According to him it went extinct with the dinosaurs.

to mean that X was infinite and countable. Since we now have a definition for \aleph_0 , for a countably infinite set X , we *define* $\text{card } X$ to be \aleph_0 . Just as each $n \in \mathbb{N}^*$ is a number, we will consider \aleph_0 to be a number - it is the first infinite cardinal.

In more advanced (and formal) treatments of set theory (for instance [39, 73]) it is possible to choose a collection of sets (called the **cardinal numbers** or **cardinals**) such that for each set A there exists a unique cardinal number \aleph with $\text{card } A = \text{card } \aleph$ (that is, there exists a bijection $A \rightarrow \aleph$). Furthermore, if α_i and \aleph_j are two cardinal numbers, there is a bijection between them if and only if they are equal. As with the finite cardinals (i.e. elements of \mathbb{N}^*), we can order the class of all cardinal numbers by declaring $\aleph_i \leq \aleph_j$ if and only if $\text{card } \aleph_i \leq \text{card } \aleph_j$ (i.e. if and only if there is an injection from \aleph_i to \aleph_j .) The Cantor-Bernstein Theorem assures us that if $\aleph_i \leq \aleph_j$ and $\aleph_j \leq \aleph_i$ then $\aleph_i = \aleph_j$. Theorem 9.5.19 (see Theorem 10.2.8 as well) guarantees that given two cardinals \aleph_i and \aleph_j , either $\aleph_i \leq \aleph_j$ or $\aleph_j \leq \aleph_i$.

As with the elements of \mathbb{N} (the finite cardinals), it is also possible to define the basic arithmetic operations of addition, multiplication, and exponentiation on the cardinals. For example, thinking of $3 = \{0, 1, 2\}$ and $4 = \{0, 1, 2, 3\}$ as cardinals, we define $3 + 4$ to be the cardinal with the same cardinality as the set

$$3 \sqcup 4 = (3 \times \{0\}) \cup (4 \times \{1\}) = \{(0, 0), (1, 0), (2, 0), (0, 1), (1, 1), (2, 1), (3, 1)\}.$$

(i.e. the disjoint union of the set 3 and the set 4.) This cardinal is easily seen to be $7 = \{0, 1, 2, 3, 4, 5, 6\}$ since there is a bijection from $7 = \{0, \dots, 6\}$ to $3 \sqcup 4$.

10.9.1 Exercise

In Section 2.4, for $a, b \in \mathbb{N}^*$ we gave a recursive definition of $a + b$. We defined $a + 0 = a$ and $a + b$ to be the successor of the sum of a with the predecessor of b . Prove that using this definition of $+$ gives the same answer for $a + b$ (with $a, b \in \mathbb{N}^*$) as the cardinal arithmetic definition given above.

Similarly, $\aleph_0 + \aleph_0$ is defined to be the cardinal number with the same cardinality as the set $\mathbb{N} \sqcup \mathbb{N}$. We have seen that this cardinal is just \aleph_0 itself, as the countable union of countable sets is countable. In other words, $\aleph_0 + \aleph_0 = \aleph_0$.

If \aleph_i and \aleph_j are cardinals, then $\aleph_i \cdot \aleph_j$ is defined to be the cardinal number with the same cardinality as the set $\aleph_i \times \aleph_j$.

10.9.2 Exercise

1. Show that, using cardinal arithmetic, $2 \cdot 3 = 6$.
2. Show that, using cardinal arithmetic, $\aleph_0 \cdot \aleph_0 = \aleph_0$.

Finally, if \aleph_i and α_j are cardinals, then the exponentiation $\aleph_i^{\aleph_j}$ is defined to be the cardinal with the same cardinality as the set of functions $\{f: \aleph_j \rightarrow \aleph_i\}$.

10.9.3

Exercise

Prove that, using cardinal arithmetic, $2^3 = 8$.

In Section 10.5, we constructed a sequence of sets

$$\mathbb{N}, \mathcal{P}(\mathbb{N}), \mathcal{P}(\mathcal{P}(\mathbb{N})), \mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N}))), \dots, \mathcal{P}^k(\mathbb{N}), \dots$$

of strictly increasing cardinality. Are there sets whose cardinalities are not equal to any of these?

The next exercise shows that there are!

10.9.4

Exercise

Let $A_0 = \mathbb{N}$. For each $n \in \mathbb{N}$, define A_n recursively to be $\mathcal{P}(A_{n-1})$. Let $A = \bigcup_{n \in \mathbb{N}^*} A_n$. Prove that

$$\text{card } A_n < \text{card } A$$

for all $n \in \mathbb{N}^*$. What other sets can you construct which have a cardinality different from any cardinality you've already encountered?

10.9.5

Exercise

If you studied Chapter 6, use the axioms from that chapter to prove that the set A in Exercise 10.9.4 is actually a set.

In the previous exercise, the set A you constructed has the property that

$$\text{card } \mathcal{P}^k(\mathbb{N}) < \text{card } A$$

for all $k \in \mathbb{N}$. Such a set is so large that it boggles the imagination. Are there any more manageable sets whose cardinalities are not in the list? In particular: Does there exist a set A such that

$$\text{card } \mathbb{N} < \text{card } A < \text{card } \mathcal{P}(\mathbb{N})?$$

Recall that $\text{card } \mathbb{R} = \text{card } \mathcal{P}(\mathbb{N})$ (Theorem 10.6.3) and that if $\text{card } X \leq \text{card } Y$, then there exists a subset of Y with the same cardinality as X (Theorem 10.2.8). We may, therefore, rephrase our question as: Does there exist a subset $A \subset \mathbb{R}$ such that $\text{card } \mathbb{N} < \text{card } A < \text{card } \mathbb{R}$? More assertively, we state:

10.9.6

The Continuum Hypothesis

If $A \subset \mathbb{R}$ is uncountable, then $\text{card } (A) = \text{card } (\mathbb{R})$.

How can we be so certain that there is no set of intermediate cardinality? On the other hand, might we be able to prove such a set exists? We can't! In 1938, Kurt Gödel proved that the Continuum Hypothesis cannot be *disproved* using the standard axioms of set theory. In 1963, things got even stranger when Paul Cohen proved that the Continuum Hypothesis cannot be *proved* on the basis of

the usual axioms of set theory. That is, the Continuum Hypothesis is independent of the usual set theory axioms.

This leads us to a very strange situation. The set of real numbers \mathbb{R} is constructed using the axioms of set theory (see Chapter 11 for the outline of how to do this). Cardinalities are defined simply using the notions of injections and bijections. Yet, the existence of an uncountable subset of \mathbb{R} having cardinality strictly less than \mathbb{R} can be neither proved nor disproved using the axioms of set theory. If we believe that the set \mathbb{R} has some sort of real (though perhaps only internal to our minds) existence, then our question **must** have an answer. This means that the usual axioms of set theory are not simply not strong enough. Gödel and Cohen's work shows that we may add either the Continuum Hypothesis or its negation to our axiom system without introducing any logical contradictions in our mathematics. But which should it be? Logically speaking, we are free to believe it or not as we wish! Of course, if you and I decide differently on the truth of the Continuum Hypothesis, then we will not believe each other's theorems, if their proofs require it.

10.10 Application: Cardinality and Symmetry

“And it was as it dreamed, and the square was,
with all its lines and angles equal.
Fit diagram for any textbook this,
sharp black on white, exact, symmetrical.”
– P.K. Page¹, *The Figures* [99]

In Section 2.5, we saw how the symmetries of an object form a group. For example, given the square on the left in Figure 10.4, there are four bilateral symmetries (depicted on the right) and four rotational symmetries (by 0° , 90° , 180° , and 270°). The 0° rotation is the identity, composing any two of these eight symmetries equals one of the other eight symmetries, and each of the symmetries has an inverse symmetry.

In this section, we see how our explorations of cardinality can be used to prove the most important theorem of finite group theory: Lagrange's Theorem. At the end of the section, we apply Lagrange's Theorem to the study of symmetry. Throughout this section, let $(G, \mathbb{1}, \circ)$ be a group and let $H \subset G$ be a subgroup. That is, H is also a group using the operation \circ inherited from G . For instance, if G is the group of symmetries of the square, then the set of four rotations is a subgroup, as is the set consisting of the identity, the 180° rotation, the vertical reflection, and the horizontal reflection. The group G has 8 elements and both of those subgroups have 4 elements.

¹P.K. Page is a Canadian poet, novelist, and painter.

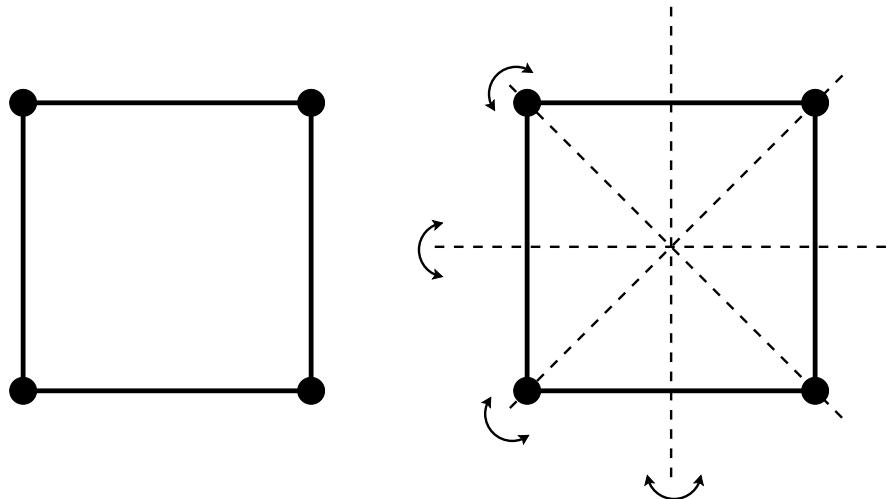


Figure 10.4: The four bilateral symmetries of a square

10.10.1 **Exercise**

Let G be the group of symmetries of the square. Find an example of a subgroup having exactly 2 elements and find another example of a subgroup having exactly 1 element. Is there a subgroup having exactly 3 elements?

In its most elementary form, Lagrange's Theorem says that if G is a group with finitely many elements and if $H \subset G$ is a subgroup, then the number of elements of G is a multiple of the number of elements of H . To get an even more informative statement, we use an equivalence relation.

Define a relation \sim_H on G by

$$(x \sim_H y) \Leftrightarrow (\exists h \in H \text{ s.t. } x = h \circ y).$$

We can rephrase this as saying that $x \sim_H y$ if and only if $x \circ y^{-1} \in H$.

10.10.2 **Lemma**

The relation \sim_H is an equivalence relation.

10.10.3 **Definition**

If $[x] \in G/\sim_H$, we call $[x]$ the **right coset** of H in G containing x . The right coset $[x]$ is often denoted Hx .

We can also define an equivalence relation on G giving rise to “left cosets.” In this text, we have chosen to use right cosets because right cosets show up in our application of group theory to bell-ringing.

10.10.4

Theorem ▶ Lagrange's Theorem

Suppose that $(G, \mathbb{1}, \circ)$ is a group with finitely many elements and that $H \subset G$ is a subgroup. Then the number of elements in G is a multiple of the number of elements in H . In fact,

$$|G| = |G/\sim_H| \cdot |H|,$$

where the vertical bars denote the number of elements in the set.



There are two key elements of the proof, both illustrated by a loaf of sliced bread. We can (in principle) compute the volume of the loaf by first slicing it. We convince ourselves that each slice has the same volume as each other slice, count the slices, and then multiply the volume of each slice times the number of slices. Similarly, we will first appeal to Lemma 10.10.2 to know that the equivalence classes in G using the relation \sim_H are a partition of G . Secondly, we show that each equivalence class has the same number of elements as each other equivalence class. Finally, we multiply the number of equivalence classes times the number of elements in each equivalence class to arrive at $|G|$. The second step is where all of the work is. But how are we to show this, working in the abstract setting that we are? How do we count elements of a set if we don't know precisely what the set is? The key to construct a bijection from H to each equivalence class!

Proof. By Lemma 10.10.2 and Theorem 7.3.10, the sets in G/\sim_H partition G . Thus, it suffices to show that all the sets in G/\sim_H have the same number of elements as H .

Claim: If $[x] \in H \setminus G$, then $|[x]| = |H|$.

We prove the claim by showing that there exists a bijection $f: H \rightarrow [x]$.

Let $h \in H$ and define

$$f(h) = h \circ x$$

By the definition of \sim_H , $f(h) \in [x]$.

⟨Prove that f is a bijection⟩

□

Recall that we thought of the quotient set G/\sim_H as being a “church picnic” where we have all the different families (equivalence classes) $[x]$ gathered. The proof of

Lagrange's theorem shows that if \sim_H is an equivalence relation arising from a subgroup of a group then all of the families at the picnic have exactly the same size.

10.10.5

Corollary

If a finite group G has a prime number of elements then its only subgroups are $\{1\}$ and G itself.

Use Lagrange's theorem to solve the following exercise. Recall that $\mathbb{Z}/p\mathbb{Z}$ is the quotient set of \mathbb{Z} under the equivalence relation where two integers are declared to be equivalent if their difference is a multiple of p . The key to the proof is to recognize that $\mathbb{Z}/p\mathbb{Z}$ is a group with $+$ as the group operation; see Section 7.8 for a refresher. By definition, the function $\phi_{[k]}$ is a homomorphism if

$$\phi_{[k]}([a+b]) = \phi_{[k]}([a]) + \phi_{[k]}([b])$$

for all $[a], [b] \in \mathbb{Z}/p\mathbb{Z}$; so that's what you should show. To use Lagrange's Theorem, show that the range of $\phi_{[k]}$ is a subgroup of $\mathbb{Z}/p\mathbb{Z}$.

10.10.6

Exercise

Suppose that $p \in \mathbb{N}$ is prime. Let $[k] \in \mathbb{Z}/p\mathbb{Z}$ and define $\phi_{[k]}: \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$ by

$$\phi_{[k]}([x]) = [k] \cdot [x]$$

Then $\phi_{[k]}$ is a bijective homomorphism

In Section 2.5, we discussed how if X is a set with some sort of structure, then $\text{SYM}(X)$ is a group. One way of obtaining subgroups of $\text{SYM}(X)$ is to “decorate” X . A decoration of a set X is a choice of $Y \subset X$ (the colored points) and we consider functions $f: X \rightarrow X$ which not only preserve the structure of X , but also have the property that $f(y) \in Y$ for all $y \in Y$. We can formalize this by saying that the decorated object \tilde{X} is the pair (X, Y) and that a symmetry of \tilde{X} is a symmetry of X which preserves the set Y .

For example, suppose that X is a regular hexagon (as on the left of Figure 10.5). If we had 4 red dots to the hexagon (as on the right of Figure 10.5), the new decorated shape \tilde{X} has two of the bilateral symmetries of the X and two of the rotations of X (namely, the rotation by 0 radians and by π radians) as symmetries. The decorated shape \tilde{X} has no other symmetries. Since $\text{SYM}(\tilde{X})$ is a group with function composition as the operation, it is a subgroup of $\text{SYM}(X)$. Since $\text{SYM}(X)$ has 12 elements (6 reflections and 6 rotations) and since $\text{SYM}(\tilde{X})$ has 4 symmetries (2 reflections and 2 rotations), there are 3 distinct left cosets of $\text{SYM}(\tilde{X})$ in $\text{SYM}(X)$, by Lagrange's Theorem.

The collection of symmetries of any given object form a group. For example, the symmetry group of a regular hexagon has 12 symmetries: 6 rotations and 6 reflections. If you decorate the hexagon and require the symmetries to preserve the decoration, the new symmetry group is a subgroup of the old symmetry group.

10.10.7

Exercise

Prove that there is no way to decorate a regular pentagon X so that the decorated pentagon \tilde{X} has exactly 6 symmetries.

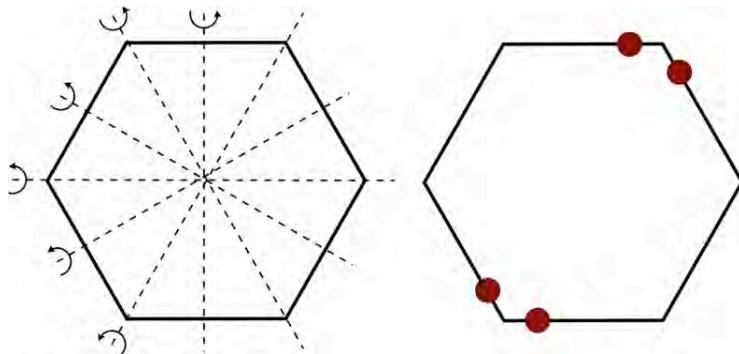


Figure 10.5: On the left we have a regular hexagon with its 6 bilateral symmetries depicted. On the right we have a decorated hexagon.

We conclude with an application to bell ringing. Recall from Section 8.9, that a change is a pattern of ringing bells in one sequence after another where to go from one sequence to the next we switch the positions of some pairs of neighboring bells. One of the basic changes is Plain Bob Minimus. The table shows the change Plain Bob Minimus for four bells, there are versions for more bells.

S	A	T	B
A	S	B	T
A	B	S	T
B	A	T	S
B	T	A	S
T	B	S	A
T	S	B	A
S	T	A	B
S	T	B	A
T	S	A	B
T	A	S	B
A	T	B	S
A	B	T	S
B	A	S	T
B	S	A	T
S	B	T	A
S	B	A	T
B	S	T	A
B	T	S	A
T	B	A	S
T	A	B	S
A	T	S	B
A	S	T	B
S	A	B	T

In Section 8.9, we learned that the plain lead on four bells is the set of all permutations effected by the symmetries in the subgroup

$$H = \{\text{id}, (12)(34), (1342), (14), (14)(23), (13)(24), (1243), (23)\}$$

That subgroup is generated by $\{(12)(34), (23)\}$. Notice that the first section of Plain Bob Minimus is simply the plain lead. In fact, each section of Plain Bob Minimus is the plain lead on four bells, just starting from a different round each time. To get between sections, the symmetry (34) is used. All 24 permutations of 4 bells show up in Plain Bob Minimus. Given our initial round of “S A T B”, each subsequent round is determined by a permutation that gets us from “S A T B” to the new round. For example, the round “T B S A” corresponds to the permutation $(13)(24)$. Here is Plain Bob Minimus written with some permutation labels emphasizing a certain pattern:

$$\begin{array}{rcl}
 & \mathbb{1} & \\
 (12)(34) & = & h_1 \\
 (13)(42) & = & h_2 \\
 (14) & = & h_3 \\
 (14)(23) & = & h_4 \\
 (13)(24) & = & h_5 \\
 (1243) & = & h_6 \\
 (23) & = & h_7 \\
 \hline
 & \mathbb{1} \circ (243) & \\
 h_1 \circ (243) & & \\
 h_2 \circ (243) & & \\
 h_3 \circ (243) & & \\
 h_4 \circ (243) & & \\
 h_5 \circ (243) & & \\
 h_6 \circ (243) & & \\
 h_7 \circ (243) & & \\
 \hline
 & \mathbb{1} \circ (234) & \\
 h_1 \circ (234) & & \\
 h_2 \circ (234) & & \\
 h_3 \circ (234) & & \\
 h_4 \circ (234) & & \\
 h_5 \circ (234) & & \\
 h_6 \circ (234) & & \\
 h_7 \circ (234) & &
 \end{array}$$

Furthermore, we also can see the structure of the sections of Plain Bob Minimus. The first section is just the effect of applying the permutations in H to the initial round “S A T B”. The second section is the effect of applying symmetries which are a combination of (243) and the symmetries of H to “S A T B”. The third section is the effect of applying symmetries which are a combination of (234) and the symmetries of H to “S A T B”. Thus the second section is the coset $H(243)$ and the third section is the coset $H(234)$ in the group S_4 (the group of permutations of 4 objects). We observe Lagrange’s theorem at work: H contains 8 permutations and there are 3 cosets: H , $H(243)$, and $H(234)$. The group S_4 contains $4! = 24 = 3 \cdot 8$ elements.

10.11 Application: dimension and space-filling curves

“Can a surface (say a square including its boundary) be one-to-one correlated to a line (say a straight line including its endpoints) so that to every point of the surface there corresponds a point of the line, and conversely to every point of the line there corresponds a point of the surface?” - G. Cantor (as quoted in [57])

The sets \mathbb{R}^n (for $n \in \mathbb{N}$) play a prominent role in mathematics. The number n is called the **dimension** of \mathbb{R}^n . What dimension space do we live in? Apparently, we have 3-dimensions of physical space and 4-dimensions of space-time¹. If we take other quantities (for instance, color or air pressure) into account we also live in a higher dimensional space. But what exactly do we mean by dimension? Considering only physical directions for a moment: what is the fundamental difference between living in a 2-dimensional space and in a 3-dimensional space?

According to common usage, the number of dimensions should be the number of quantities (i.e. real numbers) needed to describe our situation. Our position on earth is at 2-dimensional, because we can describe it with latitude and longitude. We could, of course, use more quantities to represent a position on earth. For example, we could associate to a point on earth the triple $(\mu, \lambda, 19)$ where μ is the latitude of the point and λ is the longitude. In this case, the third number “19” is superfluous. So really, the number of dimensions should be the *minimum* number of quantities needed to describe our situation.

Space is 3-dimensional because we can describe it with latitude, longitude, and distance from the earth’s surface². Although we can describe our position by a 4-tuple $(\mu, \lambda, r, \mu + \lambda)$ where μ is latitude, λ is longitude, r is the distance from earth’s surface, we don’t need the final coordinate $\mu + \lambda$. When we claim that our physical world is 3-dimensional, we are claiming not only that our position can be described by 3 quantities, but also that it can’t be described by fewer than 3 quantities.

Without begin too precise about how we are modelling our physical location mathematically, earth’s surface is at most 2-dimensional (since we have a way of describing our location with two quantities) and space is 3-dimensional (since we have a way of describing our location with three quantities). But how do we know that there isn’t some clever way of describing our position with even fewer quantities? Might it be possible to describe our position on earth’s surface using only a single quantity?

In fact, there is! We’ll use the unit sphere $S^2 \subset \mathbb{R}^3$ as a model for Earth’s surface. We start by arguing that $\text{card } S^2 = \text{card } [0, 1] \times [0, 1]$. Latitude and longitude (in radians) are each numbers in the interval $[0, 2\pi]$, so specifying a latitude and

¹If recent theories from physics are correct, we may in fact have many more dimensions of space-time.

²We are glossing over a great deal of physical, mathematical, and philosophical complexity. See, for example, Poincaré’s 1906 essay *La Relativité de l’espace*. It is available online in a 1913 English translation *The Relativity of Space* by George Bruce Halsted.

longitude gives a surjection $[0, 2\pi] \times [0, 2\pi] \rightarrow S^2$. Restricting the domain gives an injection from $[0, \pi] \times [0, \pi] \rightarrow S^2$. Since $\text{card } [0, \pi] = \text{card } [0, 2\pi] = \text{card } [0, 1]$, by the Cantor-Bernstein Theorem $\text{card } S^2 = \text{card } [0, 1] \times \text{card } [0, 1]$, as claimed. The proof of Theorem 10.6.5 implies

$$\text{card } [0, 1] = \text{card } [0, 1] \times [0, 1] = \text{card } S^2.$$

That is, there is a bijection $f: S^2 \rightarrow [0, 1]$. Consequently, if we are at position $p \in S^2$, we can represent it uniquely by the number $f(p) \in [0, 1]$. Apparently, the dimension of the earth's surface is not 2, but 1!

Similarly, for each $n \in \mathbb{N}^*$, a point in \mathbb{R}^n can be represented by a single real number. To see this, recall that by Theorem 10.6.5, $\text{card } \mathbb{R}^2 = \text{card } \mathbb{R}$. Thus, for $n \geq 2$, by induction, we have

$$\text{card } \mathbb{R}^n = \text{card } (\mathbb{R}^{n-1} \times \mathbb{R}) = \text{card } (\mathbb{R} \times \mathbb{R}) = \text{card } \mathbb{R}.$$

Thus, there is a bijection between \mathbb{R}^n (for $n \geq 1$) and \mathbb{R} . Positions in n -dimensional space can be represented by a single number!

Does this mean that the notion of “dimension” is a meaningless concept? If all we are concerned with are *sets* and *functions*, then: yes, it is meaningless. Dimension is not a quantity that is preserved by arbitrary functions. However, in the contexts where we are concerned with notions of dimension, we are concerned not with *arbitrary* functions but with functions preserving a certain structure on the set. If you've had linear algebra, this is easy to explain. For $n, m \in \mathbb{N}$, the sets \mathbb{R}^n and \mathbb{R}^m are not just sets they are vector spaces¹. In linear algebra, the “dimension” of a vector space is given a very specific definition. The functions of interest in linear algebra are those functions (namely “linear functions”)² that preserve vector space structure.

In linear algebra, considering the sets \mathbb{R}^n and \mathbb{R}^m (for $n, m \in \mathbb{N}^*$) as vector spaces and considering only *linear* functions $f: \mathbb{R}^m \rightarrow \mathbb{R}^n$, you will learn:

1. $n = m$ if and only if there is a linear bijection $f: \mathbb{R}^n \rightarrow \mathbb{R}^m$;
2. $n < m$ if and only if there is a linear injection $f: \mathbb{R}^n \rightarrow \mathbb{R}^m$ and there is no linear surjection $f: \mathbb{R}^n \rightarrow \mathbb{R}^m$;
3. $n > m$ if and only if there is a linear surjection $f: \mathbb{R}^n \rightarrow \mathbb{R}^m$ and there is no linear injection $f: \mathbb{R}^n \rightarrow \mathbb{R}^m$.

Observe that the dimension n of the vector space \mathbb{R}^n functions a lot like cardinality. Unfortunately, the property of being a vector space is quite restrictive; the surface of the earth³ isn't a vector space. Furthermore, even if we just restrict

¹If you haven't yet taken linear algebra, don't worry – all you need to know is that this is a certain kind of structure on certain kinds of sets.

²Linear functions are functions that preserve vector space structure. That is, a function $f: \mathbb{R}^n \rightarrow \mathbb{R}^m$ is **linear** if for any two vectors \mathbf{v} and \mathbf{w} and real numbers k, ℓ , we have $f(k\mathbf{v} + \ell\mathbf{w}) = kf(\mathbf{v}) + \ell f(\mathbf{w})$.

³or even any reasonable mathematical model of the surface of the earth

ourselves to the Euclidean spaces \mathbb{R}^n we will likely want to consider nonlinear functions. Whatever types of mathematical structures and whatever types of functions we consider, they need to be broad enough to do interesting and useful mathematics but narrow enough to ensure that dimension behaves at least somewhat as expected. We might, for instance consider, differentiable functions $\mathbb{R}^n \rightarrow \mathbb{R}^m$. Do statements (1), (2), and (3) above remain true if we replace “linear” with “differentiable”? Since the derivative of a multivariable function is a matrix, further investigation requires linear algebra outside the scope of this text. Instead, we’ll aim higher and ask if statements (1), (2), and (3) remain true with “linear” replaced by “continuous.”

Let’s assume that whatever the definition of dimension is, that the dimension of \mathbb{R}^n should be n . Somewhat more generally, if $I \subset \mathbb{R}$ is an interval, then the dimension of $\underbrace{I \times \cdots \times I}_{n \text{ times}}$ should be n . For the remainder of this section, we consider only the relationship between dimension 1, dimension 2, and continuous functions.

10.11.1 Exercise

Prove that there is no continuous bijection $f: \mathbb{R}^2 \rightarrow \mathbb{R}$.

Hint: Suppose f is such a bijection. Let $z \in \mathbb{R}^2$ be the (unique!) point such that $f(z) = 0$. Let $h: \mathbb{R}^2 \setminus \{z\} \rightarrow (\mathbb{R} \setminus \{0\})$ be defined by letting

$$h(t) = \frac{f(t)}{|f(t)|}$$

for all $t \in \mathbb{R}^2 \setminus \{z\}$. Explain why the function h is continuous, and that range $h = \{-1, +1\}$. Explain why this contradicts the Intermediate Value Theorem.

We can strengthen Exercise 10.11.1 to show:

10.11.2 Theorem

There is no continuous injection $f: \mathbb{R}^2 \rightarrow \mathbb{R}$.

We simply sketch the proof; you may like to provide the details for yourself.

Proof. We again proceed by contradiction. Suppose that $f: \mathbb{R}^2 \rightarrow \mathbb{R}$ is a continuous injection. Let $p, q, r \in \mathbb{R}^2$ be three distinct points. Since f is an injection, $f(p)$, $f(q)$, and $f(r)$ are all distinct points in \mathbb{R} . We may choose the labelling so that $f(p) < f(q) < f(r)$. Let $\hat{f}: \mathbb{R}^2 \rightarrow \mathbb{R}$ be the function defined by $\hat{f}(x) = f(x) - f(q)$ for all $x \in \mathbb{R}^2$. Observe that \hat{f} is a continuous injection and that 0 is in the range of \hat{f} . Since there exists a point in the range of \hat{f} that is less than 0 and a point in the range of \hat{f} that is bigger than 0, we may apply the technique from Exercise 10.11.1 and construct a contradiction to the Intermediate Value Theorem. \square

More generally, it turns out¹ that if $n > m$, then there is no continuous injection

¹This follows from the famous Invariance of Domain theorem of algebraic topology.

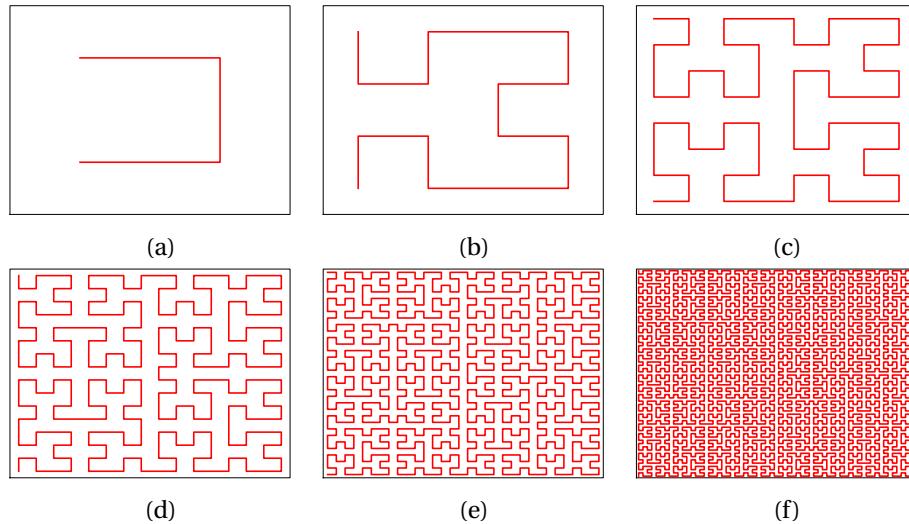


Figure 10.6: The first six approximations to the Hilbert Curve.

$$f: \mathbb{R}^n \rightarrow \mathbb{R}^m.$$

Question: Is there a continuous surjection from a 1-dimensional space to a 2-dimensional space?

In fact, there is! The remainder of this section will consist of constructing one. Rather than working with \mathbb{R} and \mathbb{R}^2 in all their unbounded glory, we will work with the slightly more manageable interval $I = [0, 1]$ and square $S = [0, 1] \times [0, 1]$. A continuous surjection $f: I \rightarrow S$ is called a **space-filling curve**. The first example of a space-filling curve was due to Peano in 1890. Hilbert adapted his example to produce the eponymous **Hilbert Curve**. The Hilbert Curve is explained informally many places online; in our explanation we present a detailed description connecting the informal idea to the formal definitions needed for proofs. We also take the opportunity to discuss connections with other themes (cardinality, graphs) of this text. Our presentation is modelled on that of the excellent and intriguing text [112]. The first chapter of [12] presents a similar perspective on space-filling curves, in the context of their applications in scientific computing. The article [65] is also an excellent starting point.

The Hilbert curve can be defined as a limit of certain other non-space-filling curves f_1, f_2, f_3, \dots , each of which is a continuous injective function from I to S . Figure 10.6 shows the first 6 curves of the pattern whose limit is the Hilbert Curve. In each image, the square S is drawn in black and the range of each f_i for $i \in \{1, 2, 3, 4, 5, 6\}$ is drawn in red. Figure 10.7 shows the first 4 approximating curves, placed on a grid to help clarify the pattern used in construction. We'll use these approximating curves as inspiration for giving a direct definition of the Hilbert Curve.

In what follows, we'll give one solution to the following exercise, but you should try to do it first on your own.

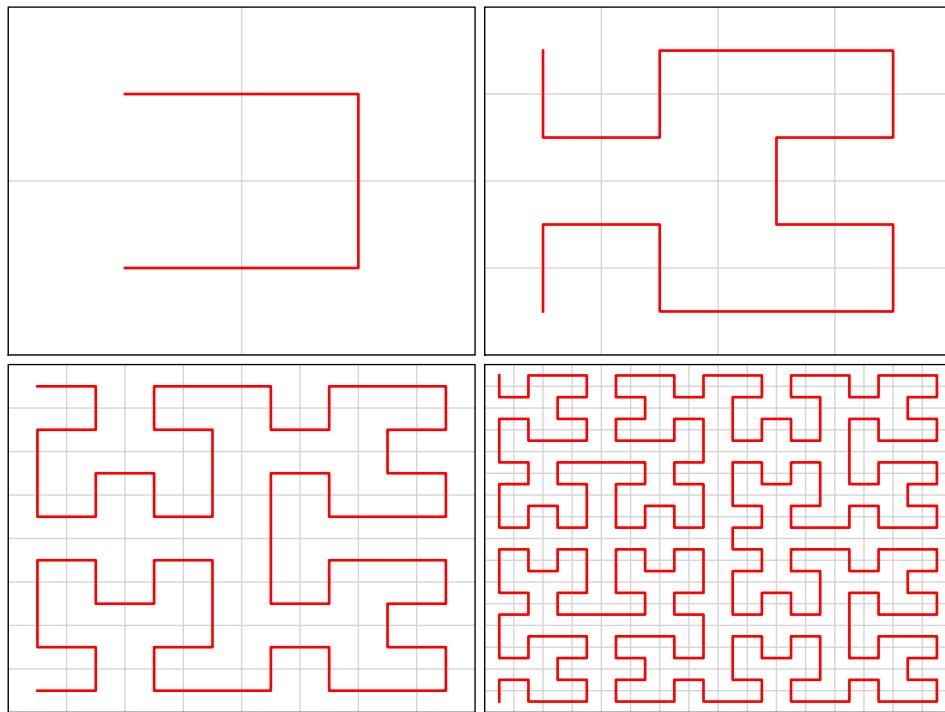


Figure 10.7: The first four approximations to the Hilbert Curve, displayed on a grid.

10.11.3 **Exercise**

Try to precisely articulate what the pattern is in Figure 10.7. What is the 7th curve in the sequence?

Intervals and Trees

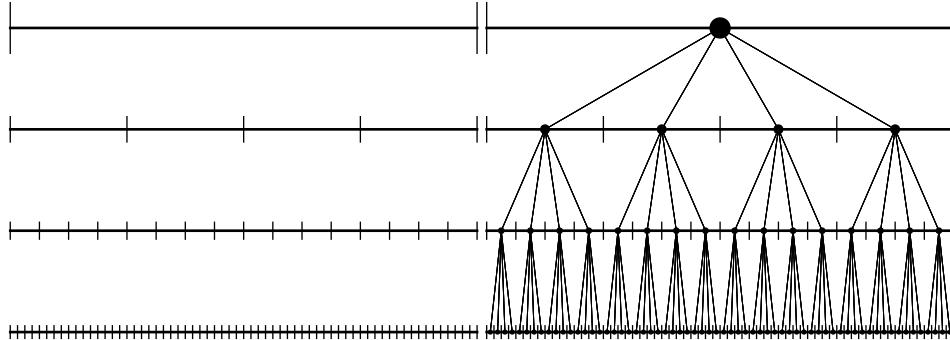


Figure 10.8: At each step we subdivide each subinterval into 4 smaller subintervals. We construct a rooted tree T_I from the sequence of subdivisions.

The range of each approximation f_n is obtained by joining the centers of subsquares of S in a certain order. The domain I of f_n is subdivided into 4^n subintervals and the codomain S is subdivided into 4^n subsubsquares. Each subinterval of I is mapped into S by joining the centers of the subsquares in a certain order. The order the subsquares are joined depends on the value of n . Figure 10.7 shows the process. The left hand side of Figure 10.8, shows the sequential subdivisions of I , beginning with the 0th subdivision, which is just the interval itself. The Hilbert curve will ultimately be defined by matching the subintervals of the subdivisions of I with the subsquares of the subdivisions of Q . We start by investigating the decompositions of I .

We start with the interval $I = [0, 1]$ and proceed to subdivide. It will be helpful to have a list of the subintervals in each subdivision. Let $\mathcal{I}_0 = \{I\}$ and assume we have defined \mathcal{I}_n to be a set of closed subintervals of I . Let \mathcal{I}_{n+1} be the set consisting of all the subintervals obtained by dividing each subinterval in \mathcal{I}_n into four equal sized subintervals. Inductively, we have a sequence $\mathcal{I}_0, \mathcal{I}_1, \dots$. For each $n \in \mathbb{N}^*$, any two distinct subintervals in \mathcal{I}_n are disjoint, except for possibly sharing an endpoint. Also, each subinterval in \mathcal{I}_{n+1} is a subset of precisely one subinterval in \mathcal{I}_n .

We can visually represent these subdivisions with a rooted 4-valent tree T_I , as on the right of Figure 10.7. The **root** of T_I is the interval I itself. Descending from the root, at height $n \in \mathbb{N}^*$ we have a vertex for each element of \mathcal{I}_n . In fact, we might as well take the vertices of T_I to be the subintervals of the subdivisions of I . If $J_n \in \mathcal{I}_n$ and $J_{n+1} \in \mathcal{I}_{n+1}$, we join them by an edge descending from J_n to J_{n+1} if $J_{n+1} \subset J_n$. Notice that for each vertex J in T_I , there is a unique path in T_I from the root I to J that does not backtrack. We call that path the **geodesic** from the root to J .

To help keep track of things, we can label each edge of T_I with a label from the set $\{0, 1, 2, 3\}$, as in Figure 10.9. More precisely, suppose that e is an edge joining $J_n \in \mathcal{I}_n$ to $J_{n+1} \in \mathcal{I}_{n+1}$. We assign e the label 0 if J_{n+1} is the leftmost subinterval of J_n ; the label 1 if J_{n+1} is the subinterval that is second-from-left; the label 2 if J_{n+1} is the subinterval that is second-from-right; and the label 3 if J_{n+1} is the

subinterval of J that is rightmost.

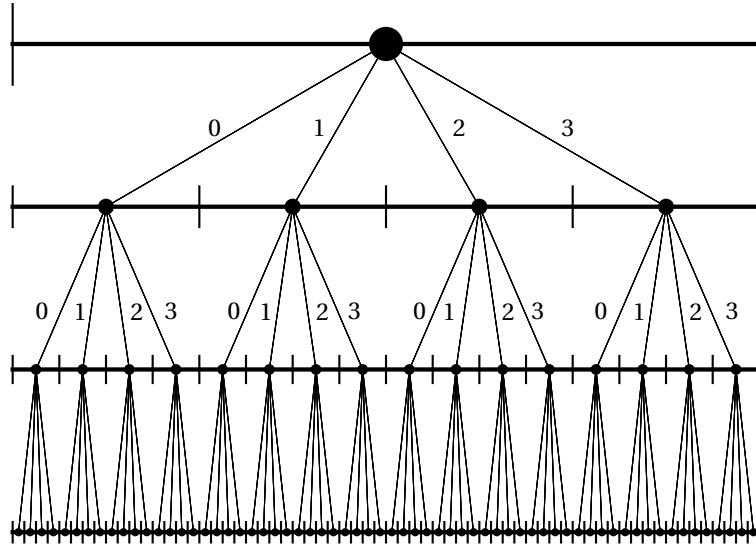


Figure 10.9: We label each edge of the tree according to which subinterval it descends into.

- 10.11.4 As we traverse the geodesic from the root to a vertex $J \in \mathcal{J}_n$, we can read off the labels on these edges. We get a finite sequence (called the **label sequence**) b_1, \dots, b_n in $\{0, 1, 2, 3\}$. Conversely, a finite sequence b_1, \dots, b_n in $\{0, 1, 2, 3\}$ defines a unique geodesic in T_I from the root to an interval J_n in the n th subdivision of I . Thus, we have a bijection between the set of finite sequences in $\{0, 1, 2, 3\}$ and the set of subintervals of the subdivisions of I .

The next theorem is a key part of our construction of the Hilbert Curve.

10.11.5

Theorem

Let $x \in I$ and let $J_n \in \mathcal{J}_n$ be a subinterval such that the geodesic from the root to J_n has label sequence b_1, b_2, \dots, b_n . Then the following are equivalent:

1. $x \in J_n$
2. There is a base 4 representation of x whose first n digits coincide exactly with the label sequence for J_n .

We want to move from considering intervals in I to considering points in I . A **ray** in T_I is an infinite path in T that starts at the root and which never backtracks. Each ray is, therefore, a sequence of intervals J_0, J_1, J_2, \dots such that $J_0 = I$ and, for each $n \in \mathbb{N}^*$, we have $J_n \in \mathcal{J}_n$ and $J_{n+1} \subset J_n$. Let $\text{RAYS}(T_I)$ be the set of rays in T_I .

Our labelling of the edges shows that there is a bijection from the $\text{RAYS}(T_I)$ to the set of infinite sequences in $\{0, 1, 2, 3\}$. For example, the sequence

$$0, 2, 3, 3, 3, 2, 2, 1, 1, \dots$$

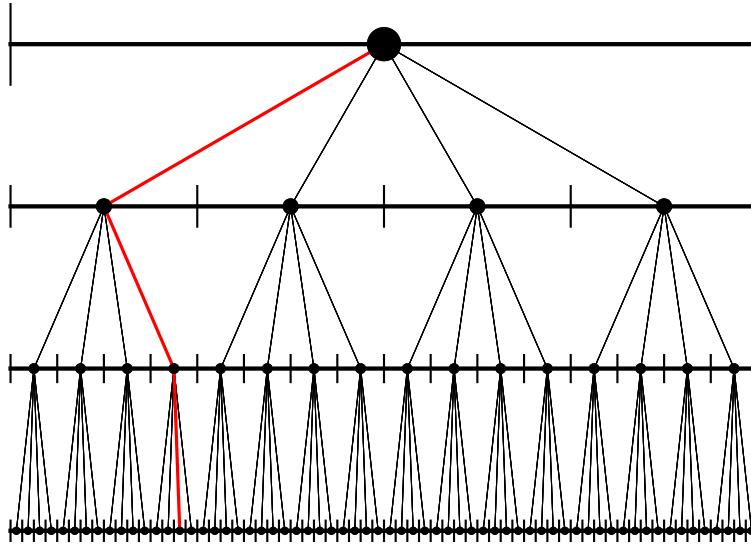


Figure 10.10: A sequence in the set $\{0, 1, 2, 3\}$ corresponds to a ray, that is a path from the root which doesn't backtrack.

corresponds to the ray where we start at the root, then go to the vertex corresponding to the leftmost subinterval of the first subdivision, then to the second-from-right subinterval of the second subdivision, then to the rightmost subinterval of the third subdivision, and so forth, as in Figure 10.10 (which only depicts the first three steps). We say that this sequence is the **label sequence** of the ray.

10.11.6

Theorem

Suppose that $t \in I$ and that (b_i) is an infinite label sequence corresponding to a ray J_0, J_1, \dots in T_I . The following are equivalent:

1. $t = .4b_1b_2b_3\dots$

2. $t \in \bigcap_{n \in \mathbb{N}^*} J_n$

10.11.7

Exercise

Prove that a ray in T corresponds to an endpoint of an interval in one of the subdivisions of I if and only if the associate sequence in $\{0, 1, 2, 3\}$ is eventually constant at 0 or 3. If the corresponding sequence is not eventually constant at 0 or 3, then it is the unique representation of the corresponding $x \in I$.

Say that a ray in T is **eventually left-turning** if the associated sequence is eventually constant at 0; it is **eventually right turning** if it is eventually constant at 3. Let $E(T_I)$ denote the set of rays that are eventually left-turning or eventually right-turning. Let

$$E(I) = \{e \in I : \exists n, j \in \mathbb{N}^* \text{ with } j \leq 4^n \text{ s.t. } e = \frac{j}{4^n}\}.$$

δ	γ	δ	γ
α	β	α	β
δ	γ	δ	γ
α	β	α	β

Figure 10.11: Labelling subsquares

These are the endpoints of subintervals in the subdivisions of I .

10.11.8

Corollary

There is a bijection from $I \setminus E(I)$ to $\text{RAYS}(T_I) \setminus E(T_I)$.

Prove that both $E(I)$ and $E(T_I)$ are countably infinite, and use this fact together with Corollary 10.11.8 to prove the next Corollary. You should be able to prove it without appealing to the Cantor-Bernstein Theorem or previously proved results concerning the cardinality of I .

10.11.9

Corollary

There is a bijection from I to $\mathcal{R}(T_I)$.

Squares and Trees

Now we do for subdivisions of squares what we did for subdivisions of intervals in the previous subsection. When we subdivide a square into four smaller squares, we can label the four smaller squares as $\alpha, \beta, \gamma, \delta$ beginning with the subsquare in the lower left-hand corner and moving counter-clockwise, as in Figure 10.11.

Let $\mathcal{S}_0 = \{S\}$ and, given a set \mathcal{S}_n of subsquares of S , let \mathcal{S}_{n+1} be the set of subsquares obtained by dividing each of the squares in \mathcal{S}_n into four congruent subsquares. As we did with intervals, we form a rooted tree T_S to keep track of our sequence of subdivisions. The vertex set is $\bigcup_{n \in \mathbb{N}^*} \mathcal{S}_n$. If $J_n \in \mathcal{S}_n$ and $J_{n+1} \in \mathcal{S}_{n+1}$ we add an edge between J_n and J_{n+1} . Notice that every vertex other than the root is joined to exactly five other vertices, corresponding to one bigger square and four smaller squares. The root, which is S itself, is just joined to the four smaller squares in \mathcal{S}_1 . A schematic depiction of a portion of T_S is given in Figure 10.12.

Our squashed spider representation of T_S isn't very easy to work with, so we redraw it so that it looks like our representation of T_I . See Figure 10.13.

10.11.10

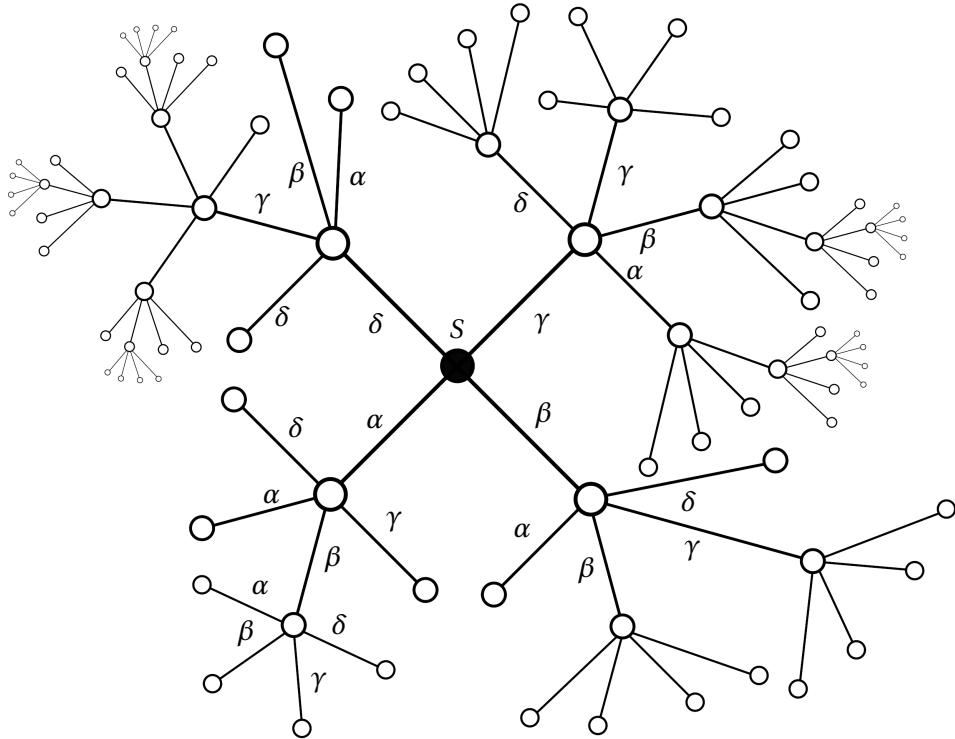


Figure 10.12: A portion of the tree T_S , squashed flat like a spider. We have labelled the vertices to distinguish our subsquares.

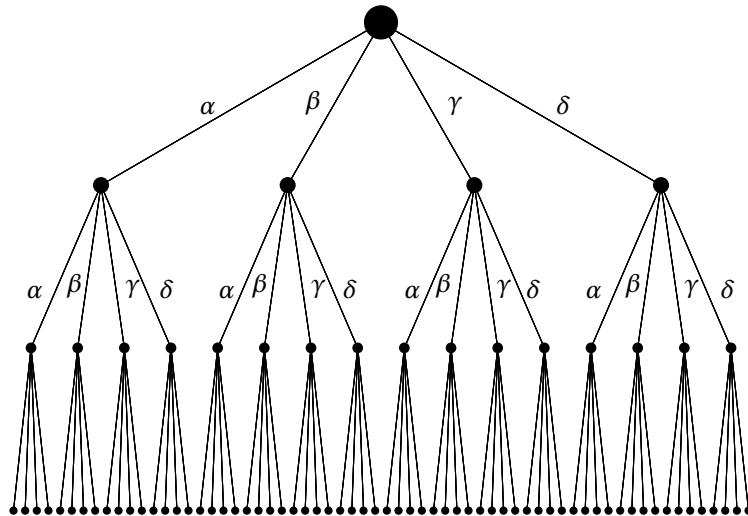


Figure 10.13: The tree T_S drawn so as to match our drawing of T_I . Every edge is labelled according to what subsquare its endpoints represent, but we have only drawn the first two layers.

Next we mimic our work from 10.11.4 but with squares instead of intervals. If $J_n \in \mathcal{S}_n$ is a vertex, there is a path with no backtracking in T_S of length n from the root to J_n . We call this path a **geodesic** from S to J_n . Reading the labels on

these edges gives us a finite sequence (the **label sequence**) $\epsilon_1, \dots, \epsilon_n$ in $\{\alpha, \beta, \gamma, \delta\}$. Conversely, a finite sequence $\epsilon_1, \dots, \epsilon_n$ in $\{\alpha, \beta, \gamma, \delta\}$ defines a unique geodesic from the root to some $J_n \in \mathcal{J}_n$.

We'll use the next exercise later.

10.11.11 Exercise

Suppose that $J_n \in \mathcal{J}_n$ and that it has label sequence $\epsilon_1, \dots, \epsilon_n$ in $\{\alpha, \beta, \gamma, \delta\}$ corresponding to the geodesic from the root to J_n . If $(x, y) \in J$, what can you say about the *binary* representations of x and y ?

A **ray** in T_S is an infinite path without backtracking emanating from the root. More precisely, a ray is a sequence J_0, J_1, J_2, \dots such that $J_0 = S$, and, for all $n \in \mathbb{N}^*$, $J_n \in \mathcal{J}_n$ and $J_{n+1} \subset J_n$. Our labelling of the edges shows that there is a bijection from the set of rays in T_S to the set of infinite sequences in $\{\alpha, \beta, \gamma, \delta\}$. For example, the sequence

$$\alpha, \gamma, \delta, \delta, \delta, \gamma, \gamma, \alpha, \alpha, \dots$$

corresponds to the ray where we start at the root J_0 , then go to the vertex corresponding to the bottom left square J_1 of the first subdivision, then to the top right square J_2 of the subdivision of J_1 , then to the top left square of the subdivision of J_2 and so forth. We say that this sequence is the **label sequence** of the ray. Let $\text{RAYS}(T_S)$ denote the set of rays in T_S . Adapt our work from the previous section to show:

10.11.12 Theorem

If $(x, y) \in S$, then there exists a ray J_0, J_1, J_2, \dots in T_S such that $(x, y) \in \bigcap_{n \in \mathbb{N}^*} J_n$. Furthermore, unless (x, y) is a corner of a subsquare in some subdivision, there is a unique such ray. Conversely, if J_0, J_1, J_2, \dots is a ray in T_S , then there is a unique $(x, y) \in S$ such that $(x, y) \in \bigcap_{n \in \mathbb{N}^*} J_n$.

10.11.13 Exercise

Show that a sequence in $\{\alpha, \beta, \gamma, \delta\}$ is associated to a corner of a subsquare in some subdivision if and only if it is eventually constant. Also show that the set $E(T_S)$ of such sequences is countable.

There is a bijection $\text{RAYS}(T_I) \rightarrow \text{RAYS}(T_S)$, as in Figure 10.14. We can use this bijection to reprove Theorem 10.6.5.

10.11.14 Exercise

Without appealing to either the Cantor-Bernstein theorem or Theorem 10.6.5, prove that $\text{card}(S) = \text{card}(I)$ by constructing an explicit bijection between S and I .

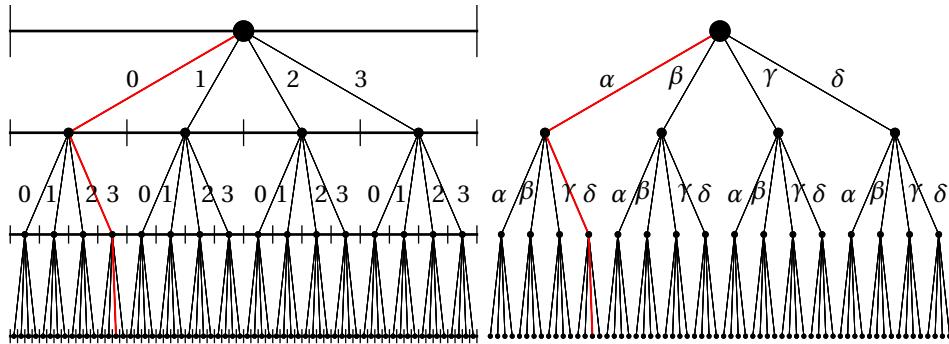


Figure 10.14: A ray in T_I with label sequence beginning 0,3,2 is matched with a ray in T_S with label sequence beginning α, δ, γ .

Constructing the Hilbert Curve

The bijection you constructed in Exercise 10.11.14 is necessarily discontinuous, and yet (depending on how you solved it) it may provide the key idea for defining the Hilbert Curve. Here is the key idea for one possible solution, an idea we'll develop as we define the Hilbert curve.

The most straightforward way to use our setup to define a function $I \rightarrow S$ is as follows. Suppose that $t \in I$. By Theorem 10.11.6, there is a ray $\rho(t) \in \text{RAYS}(T_I)$ such that t is an element of each interval that is a term of $\rho(t)$. In particular, if we write t in base 4 as

$$t = ._4 b_1 b_2 b_3 \dots$$

then the ray $\rho(t)$ has label sequence

$$b_1, b_2, b_3, \dots$$

We then match the ray $\rho(t) \in \text{RAYS}(T_I)$ with a corresponding ray $\rho'(t) \in \text{RAYS}(T_S)$. For now, we do this in the most straightforward way imaginable. Ultimately, however, that won't produce the Hilbert Curve; we'll have to vary the construction. For now, though, match the rays as follows. Replace each 0 in that sequence with α ; each 1 with β ; each 2 with γ ; and each 3 with δ . We get a sequence that is a ray J_0, J_1, J_2, \dots in T_S . By Theorem 10.11.12, there exists a unique $(x, y) \in S$ such that $(x, y) \in \bigcap_{n \in \mathbb{N}^*} J_n$. Let $f(t) = (x, y)$.

10.11.15 Exercise

What keeps f from being well-defined? Why should we be skeptical about its surjectivity?

10.11.16 Example

The real number $t = 1/15$ has base 4 representation $t = ._4 0101\overline{01}$. (To see this, notice that $16t = 1 + t$.) Performing our replacements on the

sequence

$$(b_i) = 0, 1, 0, 1, 0, 1, 0, 1, \dots$$

we obtain

$$(s_i) = \alpha, \beta, \alpha, \beta, \alpha, \beta, \dots$$

Let (x, y) be the coordinates of the point in S associated to this sequence.
Write both x and y in base 2 (i.e. binary) as:

$$\begin{aligned} x &= ._2 d_1 d_2 d_3 \dots \\ y &= ._2 e_1 e_2 e_3 \dots \end{aligned}$$

We use base 2, since each time we subdivide a square, we divide both the sides parallel to the x -axis and the sides parallel to the y -axis in half. The odd numbered subsquares in (s_i) are all the bottom left (i.e. α), so the odd numbered binary digits of both x and y are 0. Similarly, since the even numbered subsquares in (s_i) are all bottom right (i.e. β), the even numbered binary digits of x are 1, while those of y are 0. Thus,

$$\begin{aligned} 10.11.16 \quad x &= ._2 010101\overline{01} = 1/3 \\ y &= ._2 000000\overline{00} = 0 \end{aligned}$$

Therefore, the real number $1/15 \in I$ is matched with the point $(1/3, 0) \in S$ by f .

10.11.17 Exercise

What point in S is matched with the point $18/63 = ._4 102\overline{102}$ in I ?

To get a sense of what this association does, approximate each element of I to the nearest $1/4$ (i.e. one base 4 digit). This means we have taken the interval $I = [0, 1]$ and subdivided it into the intervals

$$[0, 1/4], [1/4, 1/2], [1/2, 3/4], [3/4, 1].$$

Each element of $[0, 1/4]$ is rounded to $.40$. Each element of $[1/4, 1/2]$ is rounded to $.41$ and so forth. We take the square S and subdivide it once, obtaining the squares of \mathcal{S}_1 :

$$\alpha = [0, 1/2] \times [0, 1/2], \beta = [1/2, 1] \times [0, 1/2], \gamma = [1/2, 1] \times [1/2, 1], \delta = [0, 1/2] \times [1/2, 1].$$

Under our association, each element of $[0, 1/4]$ is associated with a point of α ; each element of $(1/4, 1/2)$ is associated with a point of β ; each element of $(1/2, 3/4)$ is associated with a point of γ ; and each element of $(3/4, 1)$ is associated with a point of δ . Since we are just approximating, we might as well choose the center of each of the subsquares as the approximation.

Consider the endpoints of the subintervals. The endpoint $1/4$ can be written in base 4 as either $.40\bar{3}$ or as $.4\bar{1}0$. Using the first representation, our association of rays in T_I with rays in T_S would associate $1/4$ with a point in α , while using the second representation would associate it with a point in β . Similarly, the

endpoint $1/2$ will be associated with a point in either β or γ and $3/4$ will be associated with either a point in γ or δ . This suggests that the first image in Figure 10.7 is a reasonable first approximation to our function $I \rightarrow S$.

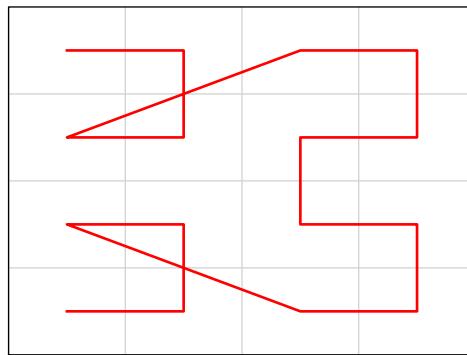
What happens when we go onto the second approximation? In this case, we have the subintervals of I , represented by the paths

$$00, 01, 02, 03, 10, 11, 12, 13, 20, 21, 22, 23, 30, 31, 32, 33$$

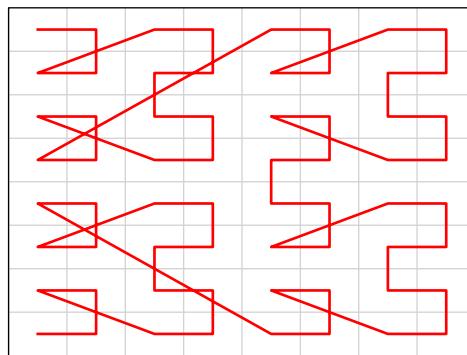
in T_I . These intervals are mapped into the subsquares of S represented by the paths

$$\begin{aligned} &\alpha\alpha, \alpha\beta, \alpha\gamma, \alpha\delta, \beta\alpha, \beta\beta, \beta\gamma, \beta\delta, \\ &\gamma\alpha, \gamma\beta, \gamma\gamma, \gamma\delta, \delta\alpha, \delta\beta, \delta\gamma, \delta\delta \end{aligned}$$

respectively. Using the centers of each subsquare to represent each subsquare and joining the centers by lines representing the potential images of the endpoints of the intervals, we get this picture:



And we see there is a problem! Whereas in our first approximation the two possibilities for the endpoint $1/4$ were in adjacent squares, for our second approximation the two possibilities for the endpoint $1/4$ were not adjacent. The image for the third approximation is even worse:



As our goal is to take the limits of approximations to arrive at a well-defined curve, we realize that we will have problems not only ensuring that our limiting function is well-defined, but also that it is continuous. How can we fix it?

At each stage of our approximation, we re-order the subsquares to ensure that the two images for points with multiple base 4 representations are send to adjacent squares. The reordering is defined recursively and uses the two diagonal reflection symmetries of the square. For any square in \mathbb{R}^2 and sides parallel to the coordinate axes, let D represent the symmetry of the square obtained by reflecting over the diagonal line with negative slope, and let O represent the symmetry obtained by reflecting over the diagonal line with positive slope.

- 10.11.18 We define the new ordering recursively as follows. Order the corners of S by $[\alpha, \beta, \gamma, \delta]$ where we start with the bottom-left corner and move counter-clockwise. We refer to the **positions** of this (or any) ordering as 0, 1, 2, and 3. Once we've ordered the corners of a square, when we subdivide each subsquare contains one of those corners. For the square S , the subsquare α is in position 0; β is in position 1; γ is in position 2; and δ is in position 3. Suppose that S' is some subsquare of some subdivision of S and that the corners of S' have been given an ordering. When we subdivide S' , we get four subsquares each containing a corner of S' . Let X be one such subsquare and suppose that it contains the corner of S' which is at position j in the ordering. If $j = 0$, then give the corners of X the same ordering as the corners of $O(S')$. If $j = 1, 2$, then give the corners of X the same ordering as the corners of S' . If $j = 3$, then give the corners of X the same ordering as the corners of $D(S')$. See Figure 10.15 for examples.

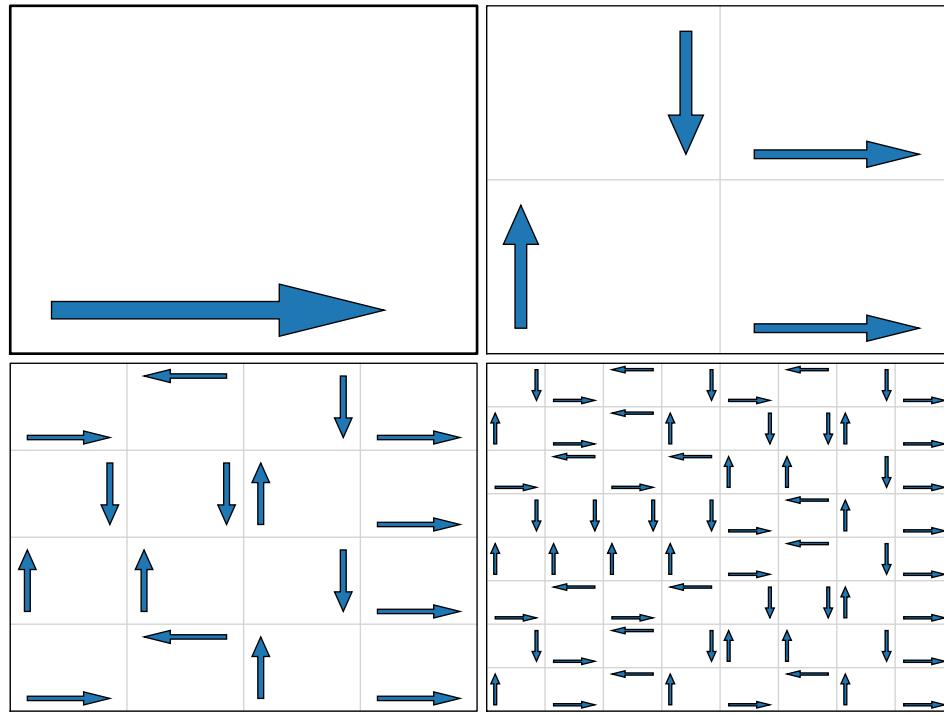


Figure 10.15: The pattern for determining orderings of the corners of the squares. In each case, we draw an arrow from the corner which has value 0 in the ordering to the corner which has value 1 in the ordering.

We then recursively define the approximations to the Hilbert Curve as follows. If a square S' is a subsquare of the n th subdivision, its vertices have been ordered

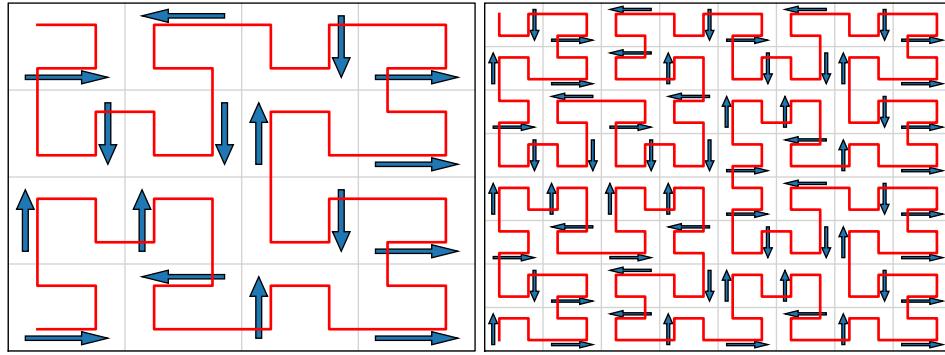


Figure 10.16: At each step, the orderings of the corners of the subsquares in the n th subdivision determine the order in which we connect the subsquares of the $(n+1)$ st subdivision, in order to create the $(n+1)$ st approximation to the Hilbert Curve.

as above. To create the $(n+1)$ st approximation to the Hilbert Curve, we subdivide S' into four subsquares. We join the centers of those subsquares by line segments, according to the ordering of the corners of S' . The left side of Figure 10.16 is a picture of the 3rd approximation to the Hilbert Curve, on top of the grid given by the second subdivision of S . Notice how the arrows of the second subdivision control the 3rd approximation curve. The right side of Figure 10.16 show the creation of the 4th approximation to the Hilbert Curve, obtained from the orderings of the corners of the subsquares of the n th subdivision of S .

We can interpret this in our trees by rearranging the order of the edges descending from each vertex, as in Figure 10.17.

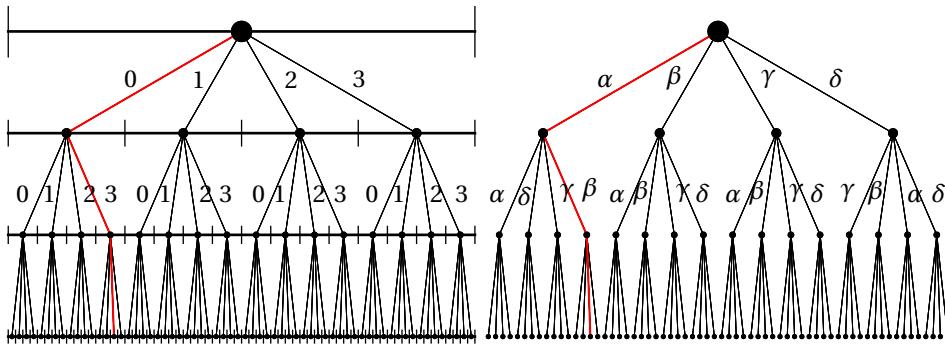


Figure 10.17: A ray in T_I with label sequence beginning $0, 3, 2$ is now matched with a ray in T_S with label sequence beginning α, γ, β .

We are now in a position to define the Hilbert Curve which we again call f . Suppose that $t \in I$. We can express t in base 4 as:

$$t = .4b_1b_2b_3\cdots$$

The sequence (b_i) corresponds to a ray $\rho(t) \in \text{RAYS}(T_I)$. By definition, as we traverse the ray $\rho(t)$, beginning at the root, for each $i \in \mathbb{N}^*$, the edge of the ray $\rho(t)$ departing from the i th vertex has label b_i . We now convert this ray into a ray

$\rho'(t) \in \text{RAYS}(T_S)$. The ray, of course, starts at the root, which is the square S . In general, suppose we have defined the n th vertex $S_n \in \mathcal{S}_n$ of the ray $\rho'(t)$. The corners of the square S_n have an ordering, and this ordering defines an ordering of the edges departing from the vertex S_n in T_S . Departing from the vertex S_n are four edges, with labels $\{\alpha, \beta, \gamma, \delta\}$, not necessarily in that order. Say they are in order e_0, e_1, e_2, e_3 . Let S_{n+1} be the other endpoint of the edge e_{b_n} . For example, if the ordering of the edges departing from S_n is $[\beta, \alpha, \delta, \gamma]$ and if $b_n = 2$, then we would follow the edge labelled δ , because that is the second edge in the ordering.

We have, therefore, recursively defined a ray J_0, J_1, J_2, \dots in the tree T_S . By Theorem 10.11.12, there is a unique element $(x, y) \in S$ such that $(x, y) \in \bigcap_{n \in \mathbb{N}^*} J_n$. We let $f(t) = (x, y)$. Put another way, for each $t \in I$, there is a sequence of nested intervals converging to that t ; that sequence is matched with a sequence of nested subsquares converging to some $(x, y) \in S$. By definition, $f(t) = (x, y)$.

10.11.19 Theorem

The function $f: I \rightarrow S$ is well-defined, surjective, and continuous.

Proof. Since we have a bijection between the rays of T_I and the rays of T_S , for each $t \in I$, there exists at least one $(x, y) \in S$ with $(x, y) = f(t)$. Likewise, for each $(x, y) \in S$, there is at least one $t \in I$ with $f(t) = (x, y)$. Thus, we need only show that f is well-defined and that it is continuous.

We have already seen that the rays in T_I corresponding to t are in bijection with base 4 representations of t . We need only consider, therefore, the possibility that t has one base 4 representation that is eventually constant at 3 and another that is eventually constant at 0. For simplicity, consider the case that

$$t = .40\bar{3} = .41\bar{0}.$$

Let b_i be the i th digit of $.40\bar{3}$ and b'_i be the i th digit of $.41\bar{0}$.

Let J_0, J_1, \dots and J'_0, J'_1, \dots be the rays corresponding to these base 4 representations; both J_0 and J'_0 equal S . According to our matching, J_0, J_1, J_2 has label sequence α, γ and J'_0, J'_1, J'_2 has label sequence β, α . The square S has label order $[\alpha, \beta, \gamma, \delta]$. We can view each finite label sequence in $\{\alpha, \beta, \gamma, \delta\}$ as a permutation of $\{0, 1, 2, 3\}$. For instance, the square J_1 has label sequence α . Passing to the subsquare α of S requires us to reflect the ordering of the corners of S across the diagonal with positive slope, since α has position 0 in that ordering. Thus, the ordering of the corners of J_1 is:

$$\alpha([\alpha, \beta, \gamma, \delta]) = [\alpha, \delta, \gamma, \beta].$$

The subsquare J_2 is whichever subsquare of J_1 has position 3 in the ordering of the corners of J_1 , since $b_2 = 3$. That is square β , which is the bottom right subsquare of J_1 . The label sequence of J_2 is $\alpha\beta$. When we view the label sequences as functions, we need to reverse the order we write them in, since function composition is written from right to left. Thus,

$$\alpha\beta([\alpha, \beta, \gamma, \delta]) = \beta \circ \alpha([\alpha, \beta, \gamma, \delta]) = \beta([\alpha, \delta, \gamma, \beta]) = [\gamma, \delta, \alpha, \beta].$$

Since β occurs in position 3 in the ordering $[\alpha, \delta, \gamma, \beta]$, by our definition at 10.11.18, the ordering of the corners of J_2 is obtained by applying symmetry D to the square J_1 , with its ordering. This produces the final equality.

Since for each $i \geq 2$, we have $b_i = 3$, by induction we have:

$$\alpha \underbrace{\beta \cdots \beta}_{i+1 \text{ times}} ([\alpha, \beta, \gamma, \delta]) = \underbrace{\beta \circ \cdots \circ \beta}_{i \text{ times}} [\gamma, \delta, \alpha, \beta] = [\cdot, \delta, \cdot, \beta].$$

The entries at positions 0 and 2 in the ordering depend on the parity of i , but all we care about is the subsquare in the 3rd position. That is always β .

The square J_1 is the bottom left subsquare (i.e. α) of S . For each $i \geq 1$, the subsquare J_{i+1} is the bottom right subsquare (i.e. β) of J_i . Let (x, y) be the coordinates of $f(t)$. By definition, $(x, y) \in \bigcap_{i=0}^{\infty} J_i$. By Exercise 10.11.11, we conclude

$$\begin{aligned} x &= .2\bar{0}\bar{1} \\ y &= .2\bar{0}\bar{0}. \end{aligned}$$

Now we redo the calculation, using the other base 4 expression for t and confirm that we get the same answer. Consider the sequence J'_0, J'_1, \dots . Since $b'_1 = 1$ and the ordering of the corners of S is $[\alpha, \beta, \gamma, \delta]$, the square J'_1 is the β (i.e. bottom right) subsquare of $J'_0 = S$. The ordering of the corners of J'_1 is:

$$\beta([\alpha, \beta, \gamma, \delta]) = [\alpha, \beta, \gamma, \delta]$$

since the subsquare occurring in position 1 in the ordering receives the same ordering as its predecessor by the definition at 10.11.18. Since $b'_2 = 0$, by similar reasoning we have:

$$\beta\alpha([\alpha, \beta, \gamma, \delta]) = \alpha \circ \beta([\alpha, \beta, \gamma, \delta]) = \alpha([\alpha, \beta, \gamma, \delta]) = [\alpha, \beta, \gamma, \delta]$$

For each $i \geq 2$, the digit $b'_i = 0$; consequently J'_{i+1} is whatever subsquare of J'_i has position 0 in the ordering of the vertices of J'_i . By induction, we see that each of these subsquares will be the α subsquare; i.e. the lower left subsquare. By Exercise 10.11.11,

$$\begin{aligned} x &= .2\bar{1}\bar{0} \\ y &= .2\bar{0}\bar{0}. \end{aligned}$$

Since in base 2, $.2\bar{1}\bar{0} = .2\bar{0}\bar{1}$, we get the same answer for $f(t)$ when we calculate its coordinates using the representation of t as $.4\bar{0}\bar{3}$ as when we use the representation of t as $.4\bar{1}\bar{1}$.

Finish the proof that f is well-defined in general either by adapting the argument we just gave or by using symmetries and the scaling properties of f .

Before continuing to show that f is continuous, show the following:

Suppose that $I_n \in \mathcal{I}_n$ (i.e. I_n is a subsquare of the n th subdivision of I). Show that if $t, t' \in I_n$, then $f(t)$ and $f(t')$ are in the same subsquare of \mathcal{S}_n .

(Suppose that $I_n, I'_n \in \mathcal{I}_n$ are distinct and share an endpoint. Show that if $t \in I_n$ and $t' \in I'_n$, then $f(t)$ and $f(t')$ are in adjacent subsquares of \mathcal{S}_n)

The **diameter** of a square in \mathbb{R}^2 is the maximum distance between any two points in the square.

We now show that f is continuous. Let $a \in I$ and let $\epsilon > 0$ be given. We must show that there is a $\delta > 0$ such that for all $x \in I$, if $|x - a| < \delta$, then $d(f(x), f(a)) < \epsilon$. Here d is the usual Euclidean distance metric on \mathbb{R}^2 . Choose n large enough so that each subsquare in the n th subdivision of S has diameter less than $\epsilon/2$. Let δ be the length of any of the subintervals in the i th subdivision of I . Let J be the subinterval of the n th subdivision of I which contains a . Let A be the subsquare in the n th subdivision of S which contains $f(a)$. Suppose that $x \in I$ and that $|x - a| < \delta$. Either $x \in J$ or x is in a subinterval J' of the n th subdivision of I that is adjacent to J . The map f takes the points in interval J into the square A . It takes the points in interval J' into a square A' of the n th subdivision of S that shares an edge with A . Since both A and A' have diameter less than $\epsilon/2$, we see that $d(f(x), f(x')) < \epsilon$. Hence, f is continuous. \square

Another interesting property of the space-filling curve f is that at no point is f differentiable. For a proof, see [112].

Image Compression

Have you ever tried to email or text a photo, only to have your computer or phone refuse to send it because the image was too large? Compression is the name for the collection of methods to make a collection of information smaller, but without losing more information than necessary. Remarkably, space filling curves, which originated out of purely mathematical and philosophical concerns, have become an essential tool in image compression. They also show up in other image processing methods such as dithering and half-toning [117, 127].

Here is a much-simplified attempt at image compression. Even in this situation, however, we'll be able to see how (an approximation to) a Hilbert curve produces a much better result than a naive approach. Suppose that we have a an image in some sort of uncompressed format that we wish to compress. To do so, we need to understand a little bit of how the computer stores and displays image. To display an image, the computer lights up a large number of small lights (called **pixels**) in some combination of red, green, and blue. The amount of each color is often stored as an 8-bit number. A bit is represented as either a 0 or 1. If we can use 8 bits to represent a number, this means that there are $2^8 = 256$ possibilities for each of red, green, and blue. On many computers, therefore, the color of each pixel is represented as a triple (r, g, b) where each of r, g, b is an integer between 0 and 255. Our image is a rectangle some number (call it n) number of pixels wide and some number (call it m) of pixels tall. The image is stored in the computer as an $m \times n$ array where each entry in the array is an (r, g, b) triple. Since our construction of the Hilbert curve involves repeatedly dividing each dimension of a square by 2, for simplicity we will assume that our original image is a $2^k \times 2^k$

square for some $k \in \mathbb{N}$. For example, here is an image combining two things that Maine is famous for (snow and apples)! The original version of this image has dimensions $2^9 \times 2^9$.



Each pixel requires $3 \cdot 256 = 768$ bits, so the image is 201326592 bits large. A megabyte is 8,000,000 bits¹ so the image is about 25 megabytes of information. Most image processing techniques fundamentally operate on one pixel at a time; that is they treat the $m \times n$ array of pixels as a *list* of mn pixels². This suggests the following (very naive) compression method:

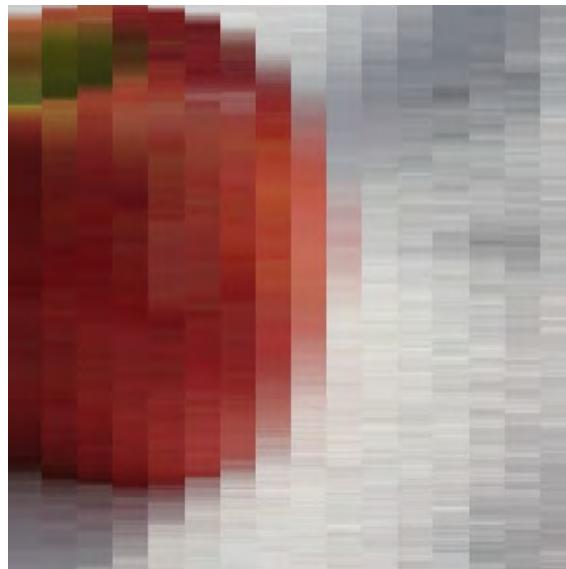
1. Put all of the pixel colors into a list. For our example image, this will be a list of 2^{18} colors.
2. Separate the colors into groupings of the same size (call it σ) . For our example, we will put them in groupings of size $\sigma = 32$.
3. For each grouping, calculate the average red value, the average green value, and the average blue value.
4. Form a new list of pixel colors, by replacing the colors within each grouping by the averages for that grouping.
5. Reconstitute a new $m \times n$ image from our new pixel list.

The new image still has the same number of pixels as the original, but it has at most mn/σ different colors. To store the new image, therefore, we just need to know the dimensions of the image, the number σ of pixels in each block, and the list whose mn/σ entries are the average color for each grouping. This reduces the storage size of the image by approximately a factor of σ .

¹A byte is 8 bits. Historically, a megabyte was 1,048,576 bytes, though many now take it to be 1,000,000 bytes.

²This is the case, for example, if we examine each pixel one at a time by using nested for loops.

For our first attempt to implement this, we will use the image of the apple in the snow above. We form our list L of colors, by listing the colors of all pixels in the first row, then the colors of all the pixels in the second row, then the colors of all the pixels in the third row, and so forth. There are 2^9 pixels in each row and 2^9 rows, so we have a list of 2^{18} colors. Set $\sigma = 32$. We form a new list L' as follows. Calculate the average of the first σ entries of L and make the first σ entries of L' this number. Then calculate the average of the next σ entries of L and make this number the next σ entries of L' . Continue working through L in this way until we reach the end. The list L' is then a list of 2^{18} colors, but consecutive groupings of σ colors are all the same. We then separate L' back into 2^9 rows of 2^9 colors each to create our new image. This is what we end up with:

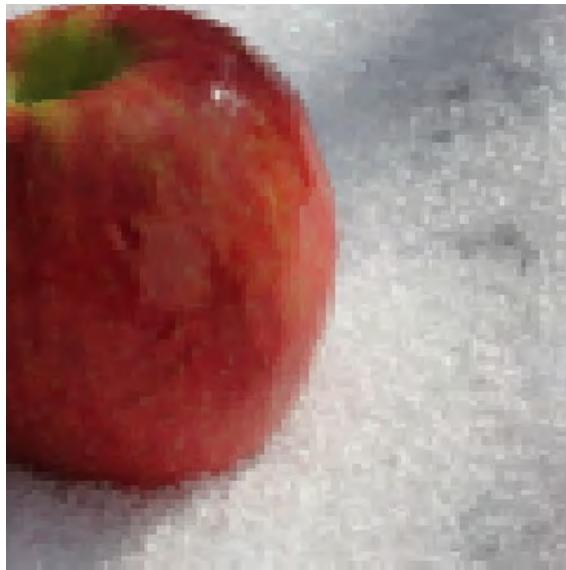


As we can see, the apple is not particularly recognizable. Notable also are the significant bands running through the image. (This is known as **color-banding**.) One obvious improvement to our method would be to average the colors in two-dimensional blocks rather than just across rows. Even doing this, however, we will have very noticeable color transitions between blocks. How can we do better? With the Hilbert curve!

Since our image is $2^k \times 2^k$, we can consider each pixel as the center of a square at the k th approximation to the Hilbert Curve. As we follow the approximating curve, we get a list of the pixels of our image. Indeed, Hilbert's pattern establishes a bijection between $\{1, \dots, 2^{18}\}$ and the pixels. Make the corresponding list of the coordinates of each of these pixels and let L be the corresponding list of pixel colors. As compared to our previous attempt, this list has two main advantages. First, because the approximating curve is continuous, colors that are near each other on the list are also near each other in the original two-dimensional image. Secondly, because the approximating curve is constructed recursively through our square subdivision process, on average colors that are near each other in the image are also near each other in the list.

We now apply the same averaging process to our list L that we did before to ob-

tain the list of colors L' . We then use the list of coordinates to reconstruct a two-dimensional image from L' . This is what we get:



Hilbert to the rescue! We have again reduced the information needed to reconstruct the image by a factor of about 32, but with significantly improved image quality, as compared to our previous method. Rather than using Hilbert's curve we could use any of a variety of other space-filling curves. Using the fractal nature of the curves, it is also possible to scale the amount of compression based on the image itself [35]. Additionally, there are versions of the Hilbert curve for 3-dimensions; these are used for compressing movies. It may be that when you watch a streaming movie, you have 19th century space-filling curves flashing before your eyes.

10.12 Application: Infinity in the Humanities

“[O]nce again she shuddered with the evidence that time was not passing, as she had just admitted, but that it was turning in a circle.”
Gabriel García Márquez¹, *One Hundred Years of Solitude*.

We highlight just a few of the vast influences and parallels that mathematics and humanistic endeavors have exerted on each other over the millenia. This section is intended more to whet your appetite for further thought and study than to present any sort of systematic overview.

¹Gabriel García Márquez (1927-2014) won the 1982 Nobel Prize in Literature. He is likely the most famous author in the magical realism tradition. The quotation is from [89].

Philosophical, Religious, and Mathematical conceptions of the Infinite

For millenia, humankind has pondered the infinite. Throughout literature, art, and theology “infinity” has been used as a metaphor for that which transcends human understanding. Modern mathematics grew out of the mathematical traditions of ancient Greece. Euclid’s *Elements* set the standard of mathematics as the body of knowledge which can be deduced from a particular collection of axioms and definitions. Concerning “the infinite,” ancient philosophers and mathematicians made the distinction between the “potentially infinite” and the “actual infinite.” For them, only the potentially infinite was subject to mathematical investigation. For example, in Euclid there are no lines which go on “forever”; there are only line segments which are of finite length. Postulate 2 of the first book of the *Elements* states that, given a line segment, it may be extended as far as one likes (though it must still remain of finite length¹) Similarly, one may speak of arbitrarily large natural numbers, but may not consider the collection of all natural numbers. That is, natural numbers are “potentially infinite,” though not “actually infinite.” The formulation of the theorem we know as “the infinitude of primes” is then

Theorem. Given any natural number N , there exists a prime number p such that $p \geq N$.

Observe that there is no claim that there are infinitely many prime numbers. Despite the reluctance of mathematicians and philosophers to embrace the notion of the “actually infinite,” Jewish, Christian, and Muslim theologians and mystics sought, in their own way, to comprehend it. For example, in his influential work *City of God*, Augustine writes²

As for their other assertion, that God’s knowledge cannot comprehend things infinite, it only remains for them to affirm, in order that they may sound the depths of their impiety, that God does not know all numbers. For it is very certain that they are infinite; since, no matter of what number you suppose an end to be made, this number can be, I will not say, increased by the addition of one more, but however great it be, and however vast be the multitude of which it is the rational and scientific expression, it can still be not only doubled, but even multiplied. … [W]hile they are simply finite, collectively they are infinite. Does God, therefore, not know numbers on account of this infinity; and does His knowledge extend only to a certain height in numbers, while of the rest He is ignorant? … Far be it, then, from us to doubt that all number is known to Him “whose understanding,” according to the Psalmist, “is infinite.” The infinity of number, though there be no numbering of infinite numbers, is yet not incomprehensible by Him whose understanding is infinite. And thus, if everything which is comprehended is defined or made

¹Strictly speaking, Euclid does not actually assign lengths to line segments in the modern sense, but this summary will do for our purposes.

²I was alerted to this quotation by [66].

finite by the comprehension of him who knows it, then all infinity is in some ineffable way made finite to God, for it is comprehensible by His knowledge. [7]

Until the mid-19th century, Euclid's choice of axioms was seen as a true description of nature, rather than (as we might see them now) as a choice of simplifying assumptions which are amenable to change as necessary. With the discovery of non-Euclidean geometry and counter-intuitive constructions in analysis, European mathematicians felt compelled to revisit the logical underpinnings of mathematics. Most of the efforts to find an acceptable foundation relied on set theory.

As a result of Cantor's work on the cardinality of sets, mathematicians finally had a way for talking about, and indeed using, actual infinities. With the ZFC axioms, the set \mathbb{N} of all natural numbers is an actual infinite - a definite conception of infinitely many objects. In Christian theology, there is a tradition called *apophatic theology* or the *via negativa*, which asserts that we can only know what God is *not* (e.g. God is not a created being or God is neither male nor female.) Similarly, with the definition of an “infinite set” as a set which is not finite we know only what an infinite set is not and we have no positive, useful, characterization of an infinite set. Beginning with Galileo's observation that infinite sets can be put into bijection with a proper subset and extending most magnificently through Cantor's work we begin to create positive conceptions of what infinite sets are.

It is worth mentioning, however, that not all modern mathematicians are happy about admitting the actual infinite into mathematics. (Consequently, these mathematicians are also unhappy with the ZFC axioms, though for different reasons from the category theorists.) Until his recent death, Edward Nelson was the most prominent contemporary mathematician to take this viewpoint. He writes [66]

I confess at the outset to the strong emotions of loathing and feeling of oppression that the contemplation of an actual infinity arouses in me. It is the antithesis of life, of newness of becoming – it is finished.

Although, Nelson's reaction to the existence of an actual infinity is an outlier among mathematicians (but see [40, Section 13]), it is part of a long tradition of reactions to infinity (or “eternity” in some contexts). In 2011, Nelson claimed a proof that the Peano axioms of arithmetic (not just ZFC!) were inconsistent (see the discussion at [9].) However, Terry Tao found a significant error in the proof and Nelson retracted the claim. Perhaps the most remarkable thing about this episode is that it demonstrates the degree of consensus among mathematicians as to what constitutes a valid proof and the value that Nelson placed on that, even above, his attachment to the belief that Peano arithmetic is inconsistent. Similarly, despite the majority belief that Peano arithmetic is consistent, since Nelson's proof was clearly presented, the mathematical community took it seriously, rather than dismissing it out-of-hand.

Finally, we comment that the parallel between religious and philosophical approaches to understanding the infinite and mathematical is not accidental. From

its early days, mathematics was closely connected with religious views (such as the Pythagoreans or Platonic and neo-Platonic philosophy). Philosophers and theologians often turn to mathematics as a source of analogies, metaphors, and test cases. Conversely, Cantor saw his work as contributing to a deeper understanding of the character of God. Additionally, despite enormous opposition, Cantor's faith sustained him in his work. The article [33] quotes a letter from Cantor to his father:

“[M]y soul, my entire being lives in my calling; whatever one wants and is able to do – and to which an unknown, secret voice calls him – that he will surely carry through to success.”

It goes on to say,

“[F]rom the very beginning, Cantor had recognized a special force, a secret voice, unknown, and yet drawing him relentlessly to the study of mathematics. Later generations might forget the philosophy, smile at his abundant references to St. Thomas and the Church fathers, overlook his metaphysical pronouncements, and miss entirely the deeply religious roots of Cantor's later faith in the veracity of his work. But these all contributed to Cantor's resolve not to abandon his transfinite numbers ... His forbearance, as much as anything else he might have contributed, insured that set theory would survive the early years of doubt and denunciation to flourish as a vigorous, revolutionary force in scientific thought of the twentieth century.”

The book [66] contains a very nice collection of articles (with differing viewpoints) on mathematical, philosophical, scientific, and religious understandings of infinity. More recently, it has come to light that certain prominent Russian mathematicians of the early 20th century, whose work was concerned with the infinite, were influenced by mystical traditions of the Orthodox Church [54].

The infinite in literature

Infinity has played an important role in literature for a very long time. The Argentinian Jorge Luis Borges is one author who made good use of notions of the infinite in his work¹. Most famously, the story *The Library of Babel* tells of an infinite library. This library is alluded to in Umberto Eco's novel *The Name of the Rose* and is a presence in Terry Pratchett's DiscWorld series.

The library consists of hexagonal rooms, each with a ventilation shaft in the center and each with five bookshelves along each of four sides. From the center of each room, you can see through to the neighboring rooms, including those above and below. The exact connectivity of the galleries to each other is some-

¹I am indebted to the very readable [62] for some of these observations.

what mysterious¹, but it is possible to get from any one room of the library to any other. The narrator believes that the library contains all possible books, including the book that is a compendium of all other books². This book is the equivalent of the mythical set of all sets, as it is a book that must contain itself.

“On some shelf in some hexagon … there must exist a book that is the cipher and perfect compendium *of all other books*, and some librarian must have examined that book; this librarian is analogous to a god.”

As the inhabitants of the library realize its infinitude, their first reaction is “unbounded joy.”

“All men felt themselves the possessors of an intact and secret treasure. There was no personal problem, no world problem, whose eloquent solution did not exist – somewhere in some hexagon.”

However, eventually they realize that the Library also contains all books that contain incorrect solutions and the “unbridled hopefulness was succeeded, naturally enough, by a similarly disproportionate depression.” The crime rate and the number of suicides increases and the narrator fears that the human species will become extinct leaving only the Library, “enlightened, solitary, infinite, perfectly unmoving, armed with precious volumes, pointless, incorruptible, and secret” to endure.

In a footnote, Borges notes that the vast Library is pointless,

“[S]trictly speaking, all that is required is *a single volume*, of the common size, printed in nine- or ten-point type, that would consist of an infinite number of infinitely thin pages.”

Of course this is reminiscent of the fact that although the set of natural numbers is infinite and unbounded it has the same cardinality as certain bounded subsets of \mathbb{R} . Many other of Borges’ stories contain other references to infinity. Rather than reading a summary of them, however, you are best off spending a few enjoyable hours reading them for yourself.

¹Millen [92] gives some suggestions as to how it might work and wrote a computer program for exploring it.

²All quotations from *The Library of Babel* are from [21].

Key Terms

- subsequence of a sequence
- convergent sequence
- complete metric space
- infimum and supremum

“George said: ‘You know we are on a wrong track altogether. We must not think of the things we could do with, but only of the things that we can’t do without.’ ... Well, we left the list to George, and he began it.”

– Jerome K. Jerome, *Three Men in a Boat (to say Nothing of the Dog)*.

In the previous sections, we’ve had occasion to make lists x_1, x_2, x_3, \dots of elements of certain sets. Such a list is called a sequence. The purpose of this chapter is to explore sequences in more detail and to see how they can be used to understand structures on sets. Two viewpoints are useful for studying sequences. We can view them as a path in some sort of space (such as a graph); we can also view them as the result of a sampling process that may or may not result in successively better approximations to some quantity. Both viewpoints require a way of measuring distance (i.e. a metric), however much of what we do in this chapter is relevant to other settings.

Recall that, formally, an infinite sequence in a set X is a function $s: \mathbb{N} \rightarrow X$ or $s: \mathbb{N}^* \rightarrow X$. We usually write s_n instead of $s(n)$ and (s_n) instead of s . Since a sequence is just a certain type of function we can apply function terminology. Henceforth, we will assume that all of our sequences have domain \mathbb{N}^* . The terminology is easily adapted to other settings.

11.0.1

Definition

Suppose that (s_n) is a sequence in a set X . Then:

- (s_n) is **injective** (or a **sequence of distinct terms** or a **sequence without repetitions**) if whenever $s_n = s_m$ we have $n = m$, for all $n, m \in \mathbb{N}^*$.
- (s_n) is **surjective** if for every $x \in X$, there exists $n \in \mathbb{N}^*$ such that $s_n = x$.
- The **range** of (s_n) is the set $\{x \in X : \exists n \in \mathbb{N}^* \text{ such that } s_n = x\}$.
- (s_n) is **constant** if there exists $a \in X$ such that for all $n \in \mathbb{N}^*$, $s_n = a$.
- (s_n) is **eventually constant** if there exists $N \in \mathbb{N}$ and $a \in X$ such that for every $n \geq N$, $s_n = a$.

11.0.2

Exercise

Give an example of:

1. a sequence in \mathbb{R}^2 that is neither injective nor eventually constant.
2. a sequence in \mathbb{Z} that is surjective.
3. a sequence in the set $\{-1, 1\}$ that is eventually constant but not constant.

Sequences in \mathbb{R} play a special role in mathematics. For our purposes we highlight two properties a sequence in \mathbb{R} may or may not have.

11.0.3

Definition

Suppose that (s_n) is a sequence in a subset of \mathbb{R} . The sequence (s_n) is **increasing** if for every n in the domain, $s_n \leq s_{n+1}$. If the inequality is always strict, then (s_n) is **strictly increasing**. The sequence (s_n) is **decreasing** if for every n in the domain, $s_n \geq s_{n+1}$. If the inequality is always strict, then (s_n) is **strictly decreasing**. If (s_n) is increasing or if (s_n) is decreasing, we say that it is **monotonic**. If there exist real numbers $a < b$ such that $s_n \in [a, b]$ for all n in the domain of (s_n) , then (s_n) is **bounded**.

11.0.4

Example

Theorem 9.1.7 defined a sequence (x_n) recursively by letting $s_0 = \sqrt{2}$ and $s_{n+1} = \sqrt{2 + s_n}$ for all $n \geq 0$. We can list the terms of this sequence as:

$$\sqrt{2}, \sqrt{2 + \sqrt{2}}, \sqrt{2 + \sqrt{2 + \sqrt{2}}}, \sqrt{2 + \sqrt{2 + \sqrt{2 + \sqrt{2}}}}, \dots$$

We showed that for every n , $s_n < 2$ (i.e. the sequence is bounded) and that $s_n < s_{n+1}$ (i.e. the sequence is increasing). Theorem 11.4.9 below shows

11.0.4

that every increasing but bounded sequence in \mathbb{R} converges to some real number. Thus, our sequence converges to a real number that we may denote by

$$S = \sqrt{2 + \sqrt{2 + \sqrt{2 + \sqrt{2 + \dots}}}}$$

Using the fact that $S^2 = 2 + S$, the quadratic formula shows that $S = \frac{1+\sqrt{5}}{2}$, the so-called golden ratio.

11.1 Subsequences

“All from the crowded lists they drive with speed”

–Ludovico Ariosto¹, *Orlando Furioso*

From a sequence with repetitions, we may want to exclude the repeated terms (as we did in Theorem 9.4.7). Similarly, we may desire a sequence to consist of better and better approximations to some fixed quantity, but every so often there may be outliers that are poor approximations. In many cases, we can create a more useful sequence by using only carefully chosen terms of the sequence and skipping the others. This is called “passing to a subsequence”. Here’s how to do it.

11.1.1

Definition ▶ Subsequence

Suppose that (s_n) is a sequence in a set X and that (n_k) is a strictly increasing sequence in \mathbb{N}^* . Then the sequence (s_{n_k}) is a **subsequence** of (s_n) .

We can view subsequences in terms of functions. Suppose that $s: \mathbb{N}^* \rightarrow X$ is a sequence and let $f: \mathbb{N}^* \rightarrow \mathbb{N}^*$ be a function which is strictly increasing. Then the composition $s \circ f$ is a subsequence of s .

11.1.2

Example

Suppose that, for all $n \in \mathbb{N}^*$, $s_n = \frac{n}{n+1}$. We have

$$(s_n) = 0, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{5}{6}, \dots$$

Define $n_k = k^2$, then the sequence:

$$(s_{n_k}) = 0, \frac{1}{2}, \frac{4}{5}, \frac{9}{10}, \frac{16}{17}, \frac{25}{26}, \dots$$

is a subsequence of (s_n) , since we have taken the 0th, 1st, 4th, 9th, 16th, 25th, etc. terms of (s_n) .

¹Ludovico Ariosto (1474-1573) was an influential poet of the Italian Renaissance. This quotation is from the translation by William Stuart Rose.

Notice that the terms of a subsequence are always “moving out” in the original sequence. In the notation (s_{n_k}) for a subsequence of (s_n) , the label n_k is the position in the original sequence and the k is the position in the subsequence, as Figure 11.1. In that figure, observe that:

$$\begin{aligned} n_0 &= 1 \\ n_1 &= 4 \\ n_2 &= 5 \\ n_3 &= 8 \\ n_4 &= 10. \end{aligned}$$

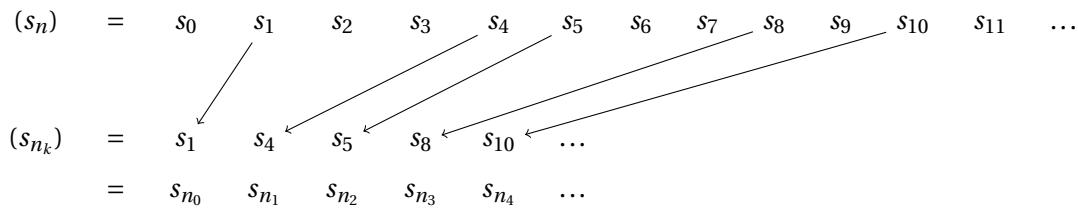


Figure 11.1: Creating a subsequence from the 1st, 4th, 5th, 8th, 10th, etc. terms of a sequence.

11.1.3 Example ▶ (non-subsequence)

Let (s_n) be the sequence in \mathbb{R} defined by $s_n = 1/(n+1)$ for all $n \in \mathbb{N}^*$. Then:

$$(y_k) = \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \dots$$

is not a subsequence of (s_n) because $y_k = \frac{1}{2}$ for all k and so

$$(y_k) = x_1, x_1, x_1, x_1, \dots$$

The sequence (y_k) is not perpetually moving outwards in (s_n) .

The next example emphasizes the important point that to specify a subsequence, we need to do more than just say what each term of the subsequence is.

11.1.4 Example

Let

$$(s_n) = \frac{1}{2}, 0, \frac{1}{2}, 1, \frac{1}{2}, 2, \frac{1}{2}, 3, \frac{1}{2}, 4, \frac{1}{2}, 5, \frac{1}{2}, 6, \frac{1}{2}, \dots$$

(i.e. $s_n = \frac{1}{2}$ for all odd $n \in \mathbb{N}$ and $s_n = n/2 - 1$ for all even $n \in \mathbb{N}$.) Is:

$$(y_j) = \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \dots$$

a subsequence of (s_n) ?

Answer: Yes and no.

Yes, because we can define $n_k = 2k$ for all $k \in \mathbb{N}^*$. Since $(2k)$ is a strictly increasing sequence in \mathbb{R} , $(s_{n_k}) = (y_j)$ is a subsequence of (s_n) .

No, because we can define $n_k = 0$ for all $k \in \mathbb{N}^*$. Then, as in the previous example $(s_{n_k}) = (y_j)$ is not a subsequence of (s_n) since (n_k) is not a strictly increasing sequence in \mathbb{R} .

11.1.5

Warning ▶ Subsequences are defined by location, not just terms.

We insist that when specifying a subsequence (s_{n_k}) of a sequence (s_n) we specify not just the terms s_{n_k} of the subsequence, but also the indices n_k .

The reason for the warning is that it doesn't make sense to say that (s_n) is a *subsequence* without specifying what it is a subsequence *of*. This is similar to how it doesn't make sense to say that Y is a *subset* without specifying what it is a subset *of*. Furthermore, as we've seen in the previous examples we need to not only say what (s_n) is a subsequence of, but also how it sits inside the original sequence. This is similar to how when we say that a subset $H \subset G$ of a group G is a subgroup, we insist that the group operation for H is the same as the group operation for G .

We often construct subsequences recursively. Here is an example:

11.1.6

Theorem

Suppose that (x_n) is an increasing sequence in \mathbb{R} . Then either (x_n) is eventually constant or (x_n) has a subsequence which is strictly increasing.

Proof. Assume that (x_n) is an increasing sequence in \mathbb{R} and that (x_n) is not eventually constant. We will show that (x_n) has a subsequence (x_{n_k}) which is strictly increasing.

Define $n_0 = 0$ so that $x_{n_0} = x_0$. (The starting term of the subsequence is also the starting term of the sequence.) Now assume that we have defined n_0, \dots, n_k (for a fixed k) so that the following hold:

- (i) $n_0 < n_1 < \dots < n_k$
- (ii) $x_{n_0} < x_{n_1} < \dots < x_{n_k}$.

Condition (i) guarantees that as we build our subsequence, it is actually a subsequence of (x_n) . Condition (ii) guarantees that we are building a strictly increasing subsequence.

We will show that we can define n_{k+1} so that:

- (i') $n_0 < n_1 < \dots < n_k < n_{k+1}$
- (ii') $x_{n_0} < x_{n_1} < \dots < x_{n_k} < x_{n_{k+1}}$.

We consider the set of indices that are strictly larger than the last index we've defined (namely n_k) and whose terms are larger than any of the terms we've selected so far. Let

$$S = \{m \in \mathbb{N}^* : m > n_k \text{ and } x_m > x_{n_k}\}$$

Claim: $S \neq \emptyset$.

Suppose, to the contrary, that $S = \emptyset$. Then for all $m > n_k$, $x_m \leq x_{n_k}$. Since the sequence (x_n) is increasing and $m > n_k$, $x_m \geq x_{n_k}$. Hence, $x_m = x_{n_k}$. Since $x_m = x_{n_k}$ for all $m \geq n_k + 1$, the sequence (x_n) is eventually constant. This contradicts our initial assumption, so $S \neq \emptyset$.

Let $n_{k+1} \in S$. Then, by the definition of S , $n_{k+1} > n_k$. Thus, by (i), condition (i') also holds. Similarly, by the definition of S , $x_{n_{k+1}} > x_{n_k}$ and so (ii') also holds.

Consequently, by induction, we have defined a subsequence (x_{n_k}) of (x_n) which is strictly increasing. \square

The organization of the proof above is typical. Here is a summary.

TO CONSTRUCT A SUBSEQUENCE

To show: Let (x_n) be a sequence such that \langle certain properties hold \rangle . Construct a subsequence (x_{n_k}) such that \langle certain other properties \rangle hold.

We define the subsequence inductively.

Base Case: Define $n_0 \in \mathbb{N}^*$ so that x_{n_0} could be the start of the desired subsequence. (For example if we are trying to define a subsequence where every term is positive, be sure that x_{n_0} is positive.)

Inductive Step: Assume that we have defined n_0, \dots, n_k so that

$$(i) \quad n_0 < n_1 < n_2 < \dots < n_k$$

$$(ii) \quad x_{n_0}, \dots, x_{n_k} \text{ could be the start to the desired subsequence.}$$

Show that we can define n_{k+1} so that:

$$(i') \quad n_0 < n_1 < n_2 < \dots < n_k < n_{k+1}$$

$$(ii') \quad x_{n_0}, \dots, x_{n_k}, x_{n_{k+1}} \text{ could be the start to the desired subsequence.}$$

\langle Do the necessary work to show n_{k+1} exists! \rangle

By recursion, we will have constructed a subsequence (x_{n_k}) .

\langle Explain why (x_{n_k}) has the desired properties. \rangle

The next two theorems provide some practice. The second theorem is reminiscent of Theorem 9.4.7. It can be proved similarly.

11.1.7

Theorem

Suppose that (x_n) is a sequence in a finite set $Y = \{y_1, y_2, \dots, y_m\}$. Prove that (x_n) has a constant subsequence.

11.1.8

Theorem

Suppose that (a_n) is a sequence in a set X such that range (a_n) is infinite. Then (a_n) has an injective subsequence (a_{n_k}) with the same range as (a_n) .

11.2 Convergent Sequences

“Far off like floating seeds the ships
Diverge on urgent voluntary errands”
– W.H. Auden¹, *On This Island*

A standard result from Calculus says that bounded, increasing sequences in \mathbb{R} converge. It’s desirable to apply these notions in other settings, in particular \mathbb{R}^n for $n \geq 2$. In this section we adapt our terminology to metric spaces. Figure 11.2 indicates the basic idea of convergence. Recall that in a set X with metric d , a **ball** (or **disc**) of radius $\epsilon > 0$ centered at $a \in X$ is the set

$$B_\epsilon(a) = \{x \in X : d(x, a) < \epsilon\}.$$

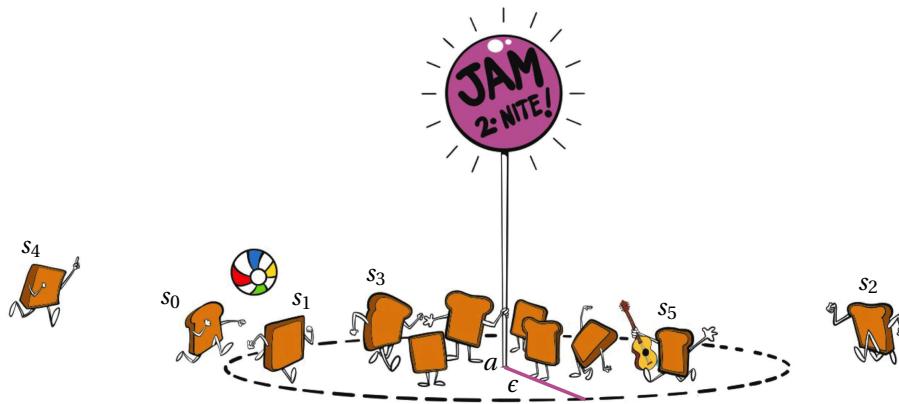


Figure 11.2: The sequence of toast people converges to the point a if, no matter what $\epsilon > 0$, eventually all the toast people lie in the disc $B_\epsilon(a)$. In this case, maybe after $N = 5$, all toast people are within this particular ϵ of a .

¹W.H. Auden (1907-1973) was one of the most influential twentieth century poets.

11.2.1

Definition

Suppose that (s_n) is a sequence in a metric space X with metric d . Then:

- (s_n) is **bounded** if there exists $M \in \mathbb{R}$ such that for all $n \in \mathbb{N}^*$, $s_n \in B_M(s_0)$. That is, the sequence is contained in some ball centered at the initial term.
- The sequence (s_n) **diverges to infinity** if for every $M \in \mathbb{N}^*$, there exists $N \in \mathbb{N}^*$ such that for all $n \geq N$, $s_n \notin B_M(s_0)$. That is, eventually the sequence is outside any given ball centered at the initial term.
- (s_n) **converges** or **is convergent** if there exists $a \in X$ such that for all $\epsilon > 0$, there exists $N \in \mathbb{N}^*$ such that for all $n \geq N$, $s_n \in B_\epsilon(a)$. That is, eventually the sequence is contained in any given ball centered at a . We say that a is a **limit** of (s_n) and write $a = \lim(s_n)$. If a sequence does not converge, it **diverges**.

11.2.2

Exercise

Sketch a picture of a bounded sequence in \mathbb{R}^2 (using the euclidean metric) and also sketch a picture of a sequence in \mathbb{R}^2 which diverges to infinity.

11.2.3

Exercise

In Definition 11.0.3 we gave a definition of what it means for a sequence in \mathbb{R} to be bounded. The set \mathbb{R} is also a metric space with the euclidean metric d , so we now have two definitions of what it means for a sequence in \mathbb{R} to be bounded. Are there any sequences which are bounded with respect to one definition but not the other? Why or why not?

Even though, from Calculus, we likely have an intuitive sense for what “convergence” means, we need to be sure that our intuition is connected to the reality of what the definition actually says. We begin by considering sequences as a sampling process which has the aim of approximating some number. As usual in mathematics, our goal is to have approximations which are arbitrarily close to the item being approximated.

Suppose that a hot paella has just been removed from the oven and is now cooling on the kitchen counter. The young scientist in the house measures the temperature of the paella every minute. Let (s_n) be the temperature of the paella n minutes after it is taken out of the oven. If R is the room temperature, then no matter what $\epsilon > 0$ we choose, eventually the temperature s_n of the paella will be within ϵ of R . That is, (s_n) converges to R .

The number $\epsilon > 0$ can be thought of as the allowable error tolerance when we approximate the point a by the terms of the sequence (s_n) . Thus, the phrase “for every $\epsilon > 0$ ” means “no matter what positive error tolerance we set”. The number N tells us how far out in the sequence (s_n) we need to go before our approximations are guaranteed to be within the allowable error tolerance. Thus,

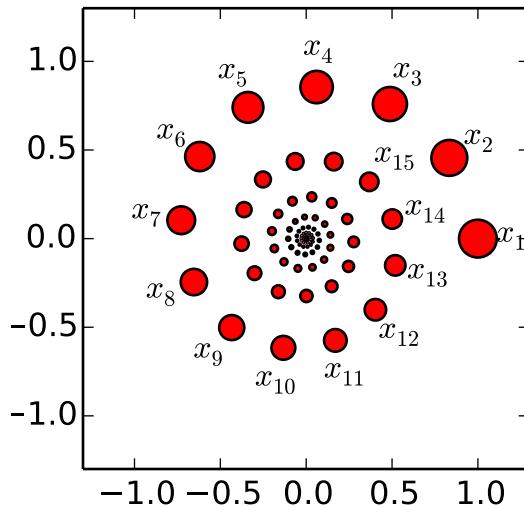


Figure 11.3: An example of a sequence (x_n) in \mathbb{R}^2 (with the euclidean metric) converging to the origin. The first 15 terms of the sequence have been labelled, the others continue in the obvious pattern spiralling toward the origin. The sizes of the points have been scaled for readability. The sequence is convergent since, for any $\epsilon > 0$, eventually all the remaining terms of the sequence are within distance ϵ of the origin.

the phrase “there is $N \in \mathbb{N}$ ” says that no matter what error tolerance we set, we can go far enough out in the sequence so that good things happen. What are those good things? “For every $n \geq N$, $d(s_n, a) < \epsilon$. Figure 11.3 gives another example of a convergent sequence.

11.2.4 Example

Consider the sequence $(x_n)_{n=0}^{\infty} = 1, 1/2, 1/3, 1/4, 1/5, \dots$ in \mathbb{R} defined by $x_n = \frac{1}{n+1}$. This sequence samples certain real numbers and seems to eventually provide good approximations to the number 0. Indeed, if $\epsilon > 0$ is our acceptable error, then for large enough n we are guaranteed that x_n is within ϵ of 0. That is, for large enough n , we are guaranteed that $|x_n - 0| < \epsilon$. That is, $\lim(x_n) = 0$.

When making approximations, it would be surprising if we could approximate two different limits equally well with the same sequence of samplings. The next theorem makes this precise. It shows that the limit of a sequence in a metric space, if it exists, is unique.

11.2.5 Theorem ▶ Limits are unique

Suppose that a sequence (x_n) in a metric space (X, d) converges to both $a \in X$ and $b \in X$. Then $a = b$.

We can also think of a sequence in a metric space X as being like a path: a way of moving around in the space. Thinking of a sequence (x_n) in a metric space as a kind of “discrete path”, we see that it converges if, for all practical purposes, the path arrives at some destination. The phrase “for all practical purposes” means that the terms of the sequence are guaranteed eventually to be as close as we could possibly wish to the limit point, even though the limit point itself may not be one of the terms of the sequence. You may not be exactly standing on the destination, but you can touch it (no matter how short your arms are.)

In Calculus, you have likely studied infinite series. These are helpful in our context as they allow us to define the “total length” of a sequence in a metric space in a way that is analogous to the definition of “length of a curve” using integrals. We begin with a reminder of how to work with infinite series.

11.2.6

Definition ▶ Series

Suppose that $a = (a_n)$ is a sequence in \mathbb{R} . The **n th partial sum** of the sequence a is

$$s_n = a_1 + \cdots + a_n = \sum_{k=1}^n a_k.$$

The **series** with terms (a_k) is the sequence (s_n) of partial sums. We let $\sum_{k=1}^{\infty} a_k$ denote both the sequence (s_n) and, if it converges, its limit. If the sequence $(s_n) = \sum_{k=1}^{\infty} a_k$ diverges to ∞ (i.e. if for all $M \in \mathbb{N}$, there exists $N \in \mathbb{N}$ such that for all $n \geq N$, we have $s_n \geq M$) then we write $\sum_{k=1}^{\infty} a_k = \infty$.

11.2.7

Example

Consider the series $\sum_{k=1}^{\infty} \frac{1}{k^2}$. The *terms* of this series are: $1, 1/4, 1/9, 1/16, \dots$. The *partial sums* of this series are:

$$s_1 = 1$$

$$s_2 = 1 + \frac{1}{4} = \frac{5}{4}$$

$$s_3 = 1 + \frac{1}{4} + \frac{1}{9} = \frac{49}{36}$$

$$s_4 = 1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} = \frac{205}{144}$$

etc.

11.2.8

Definition ▶ Total length of a sequence

Suppose that (x_n) is a sequence in a metric space X with metric d . The **total length** is defined to be the limit of the series

$$\ell(x_n) = \sum_{k=1}^{\infty} d(x_k, x_{k+1}).$$

The total length of a path may be infinite, even when the sequence of points converges, as the next example shows.

11.2.9

Example

See Figure 11.4. Let (x_k) in \mathbb{R}^2 be the sequence defined by

$$x_k = \begin{cases} \left(\frac{2}{k}, \frac{2}{k}\right) & k \text{ even} \\ \left(\frac{2}{k+1}, 0\right) & k \text{ odd} \end{cases}$$

Observe that the sequence (x_k) converges to the origin. Consider the partial sum $s_n = \sum_{k=1}^n d(x_k, x_{k+1})$. This sum is realized by the sum of the lengths of the line segments in \mathbb{R}^2 from each x_k to x_{k+1} . Looking at just the vertical line segments (i.e. when k is odd), we see that, for even $n = 2m$

$$s_n \geq \sum_{j=1}^m d(x_{2j-1}, x_{2j}) = \sum_{j=1}^m \frac{1}{j}$$

Since the harmonic series $\sum_{j=1}^{\infty} 1/j$ diverges to ∞ , the sequence (s_n) diverges to infinity. Thus, $\ell(x_k) = \infty$.

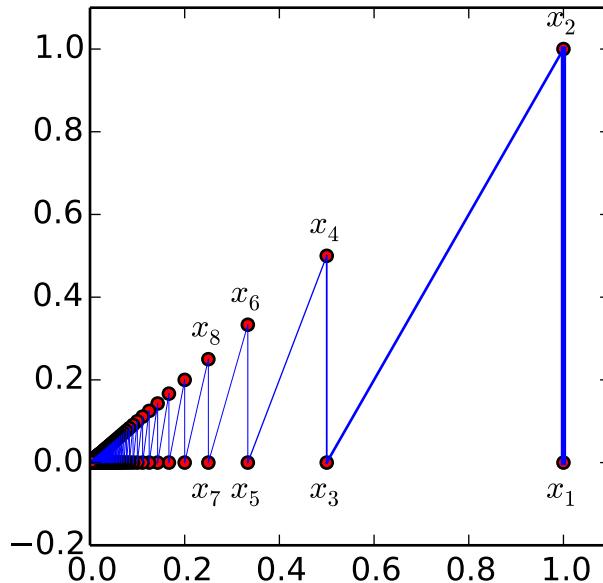


Figure 11.4: A sequence of points in \mathbb{R}^2 converging to the origin, but with infinite length.

11.2.10

Exercise

Suppose that (x_k) is a sequence in a metric space X and that (x_k) converges to some $a \in X$. Let (x_{n_k}) be a subsequence. Show that (x_{n_k}) also converges to a .

11.3 Completeness

“The true work, it is done from within. The little grey cells

– remember always the little grey cells, *mon ami!*”

–Hercule Poirot [27]

In our examples and pictures of convergent sequences, we’ve seen how the terms far out in the sequence seem to cluster together. We will show that this always happens, but first we need a precise definition. It is a definition that turns out to be relevant even for some nonconvergent sequences! Figure 11.5 depicts the main features.

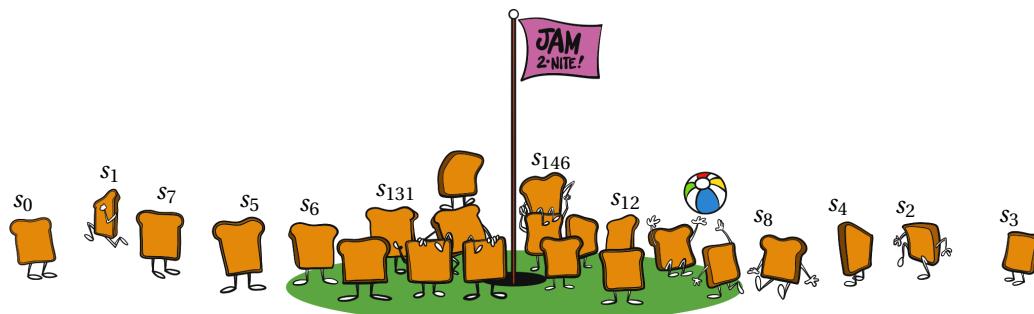


Figure 11.5: The sequence of toast people is Cauchy if, no matter what $\epsilon > 0$ is given, there is a disc of radius ϵ such that eventually all the toast people are within the disc. Unlike in the definition of convergence, the center of the disc may depend on the choice of ϵ .

11.3.1 Definition ▶ Cauchy Property

Suppose that X is a metric space with metric d . A sequence (x_n) in X is **Cauchy** (or **has the Cauchy property**) if for every $\epsilon > 0$, there exists $a \in X$ and $N \in \mathbb{N}$, such that for all $n \geq N$, $x_n \in B_\epsilon(a)$. That is, eventually the terms of the sequence are contained in some ball of any given radius; the center of the ball may depend on the radius.

11.3.2

Warning ▶ Cauchy vs. Converge

Don't confuse a sequence begin convergent with a sequence being Cauchy! The distinction is subtle, but important. In both cases, we have a center a and a radius ϵ such that eventually the sequence is within the radius of the center (i.e. in $B_\epsilon(a)$). For convergence, the center is independent of the radius, while for the Cauchy property it may depend on the radius. The definition of convergence, is of the form:

"There exists a center $a \in X$, such that for all radii $\epsilon > 0 \dots$ "

while the definition of the Cauchy property is of the form:

"For all radii $\epsilon > 0$, there exists a center $a \in X \dots$ "

The definition of the Cauchy property we gave is not the standard phrasing. The next exercise shows that it is equivalent to the standard definition.

11.3.3

Exercise

Suppose that (X, d) is a metric space and that (x_n) is a sequence in X . Prove that (x_n) is Cauchy if and only if for every $\epsilon > 0$, there exists $N \in \mathbb{N}$ such that for all $n, m \geq N$

$$d(x_n, x_m) < \epsilon.$$

(Hint: Use the triangle inequality for d and notice there are two meanings for ϵ : the one from Definition 11.3.1 and the one in the statement of this exercise. Use different symbols to represent them.)

Our definition has the advantage of making the proof of the next theorem easy.

11.3.4

Theorem

Suppose that (x_n) is a sequence in a metric space (X, d) which converges to $a \in X$. Then (x_n) is Cauchy.

The Cauchy property is very powerful: if a Cauchy sequence has a convergent subsequence, then the entire sequence converges. Informally, this is because the terms of the entire sequence are eventually very close together and the terms of some subsequence are eventually very close to a limit point, so eventually all the terms of the sequence must be close to that limit point. Here is your chance to write a formal proof.

11.3.5

Theorem

Suppose that X is a metric space and that (x_k) is a Cauchy sequence in X . If (x_k) has a subsequence (x_{n_k}) which converges to $a \in X$, then (x_k) also converges to a .

Observe that the standard definition of the Cauchy property requires that for any n and m that are large enough, the distance from x_n to x_m is small enough. It is

tempting to replace that requirement with the less restrictive requirement that, for n large enough, adjacent terms are close enough. The next exercise shows that the less restrictive requirement does not imply the Cauchy property.

11.3.6

Exercise

Let $a_n = 1/n$ for all $n \in \mathbb{N}$ and let $s_n = a_1 + \dots + a_n$. Then the sequence (s_n) in \mathbb{R} (with the usual metric) is not Cauchy, but has the property that for all $\epsilon > 0$, there exists $N \in \mathbb{N}$ such that $d(s_n, s_{n+1}) < \epsilon$, for all $n \geq N$.

The sequence (s_n) in the previous example, being the harmonic series, does not converge. The next theorem, on the other hand, shows that every sequence of finite total length is Cauchy.

11.3.7

Corollary

If (x_n) is a sequence in a metric space (X, d) of finite total length, then (x_n) is Cauchy.

Proof. Let $\alpha = (x_n)$ be a sequence in X . Assume that $\text{length}(\alpha) < \infty$. Let $\epsilon > 0$. We will show that there is an $N \in \mathbb{N}$ such that for all $n, m \geq N$, we have $d(x_n, x_m) < \epsilon$. By definition of series convergence, if we let $s_k = \sum_{n=0}^k d(x_i, x_{i+1})$ the sequence (s_k) converges to some $a \in \mathbb{R}$. Since convergent sequences are Cauchy, By Theorem 11.3.4, this implies that there is an $N \in \mathbb{N}$ such that for all $n, m \geq N - 1$ with $m \geq n$, we have $s_{m-1} - s_{n-1} < \epsilon$. However,

$$s_{m-1} = s_{n-1} + \sum_{i=n}^{m-1} d(x_i, x_{i+1})$$

so by the polygon inequality (see Exercise (2) in Section 9.9):

$$0 \leq d(x_m, d_n) \leq \sum_{i=n}^{m-1} d(x_i, x_{i+1}) = s_{m-1} - s_{n-1} < \epsilon,$$

as desired. □

11.3.8

Example

Example 11.2.9 gave an example of a sequence (x_n) in \mathbb{R}^2 of infinite total length which converged to the origin in \mathbb{R}^2 . Since it converges, that sequence is Cauchy by Theorem 11.3.4. Thus, not every Cauchy sequence has finite total length. Notice in that example, however, that the infinite length of the sequence came from a lot of zig-zagging. The next theorem shows that if you cut out the zig-zags (so to speak) from a Cauchy sequence, we end up with a subsequence of finite total length.

11.3.9

Theorem

Suppose that (x_n) is a sequence in a metric space X having metric d such that (x_n) is Cauchy. Then (x_n) has a subsequence of finite total length.

(Hint: Having chosen n_k , choose n_{k+1} so that $d(x_{n_k}, x_{n_{k+1}}) < \frac{1}{2^k}$. Then use the comparison test, which is Theorem 11.4.10 below, and standard facts about geometric series.)

On the other hand, there is no guarantee that Cauchy sequences or even sequences of finite total length converge.

11.3.10

Exercise

Let $X = \mathbb{R} \setminus \{0\}$ have the standard euclidean metric and let $x_n = 1/n$ for all $n \in \mathbb{N}$. Then (x_n) is Cauchy, but does not converge to a point in X .

Of course, the key point in the previous exercise is that (x_n) does not converge in X . It does, however, converge in \mathbb{R} . The reason that not every Cauchy sequence in $X = \mathbb{R} \setminus \{0\}$ converges is that X has a “hole”. Thinking of the sequence $\alpha = (1/n)$ in X as a discrete path, we can calculate its length as

$$\ell(\alpha) = \sum_{k=1}^{\infty} \frac{1}{k} - \frac{1}{k+1} = 1.$$

In a sense, in the space X we can go for a finite length walk along the path α and end up outside the space. Spaces without such holes are called “complete.” We formalize this in Definition 11.3.11.

11.3.11

Definition

A metric space X is **complete** if for every Cauchy sequence (x_n) in X , there exists $a \in X$ such that (x_n) converges to a .

11.3.12

Exercise

Show that \mathbb{Q} with the euclidean metric is not complete.

11.3.13

Corollary

A metric space X is complete if and only if every sequence of finite total length converges.

11.4 Sequences and subsequences in \mathbb{R}

“You’re always learning, always refining your skills. You never stop accumulating a more intimate understanding of your craft.”

–Dieter Goldkuhle¹ [74]

In the first section of this chapter, we defined what it meant for a sequence in \mathbb{R} to be increasing or decreasing (i.e. monotonic). Closely related to monotonic sequences are the infima and suprema of subsets of \mathbb{R} . These are like maxima and minima except they may not belong to the subset or they may be $+\infty$ or $-\infty$.

11.4.1

Definition ▶ Inf and Sup

The **extended real numbers** is the set $\mathbb{R}^* = \mathbb{R} \cup \{-\infty, \infty\}$ and we define, for all $x \in \mathbb{R}$: $x < \infty$ and $-\infty < x$. Of course, $-\infty < \infty$, as well.

Suppose that $A \subset \mathbb{R}$. An element $\alpha \in \mathbb{R}^*$ is a **lower bound** for A if for all $a \in A$, $\alpha \leq a$. Similarly, $\beta \in \mathbb{R}^*$ is an **upper bound** for A if for all $a \in A$, $a \leq \beta$.

The number α is the **infimum** of A (and we write $\alpha = \inf A$) if α is a lower bound for A and if whenever α' is a lower bound for A , $\alpha' \leq \alpha$ (that is, α is the “greatest lower bound” for A .)

The number β is the **supremum** of A (and we write $\beta = \sup A$) if β is a upper bound for A and if whenever β' is a upper bound for A , $\beta' \geq \beta$ (that is, β is the “least upper bound” for A .)

11.4.2

We should consider ∞ and $-\infty$ to be symbols with certain properties. They are not real numbers and should not be treated as such. Our use of these symbols should not be imbued with any particular philosophical meaning, though the choice of these particular symbols is influenced by philosophical conceptions of infinity.

11.4.3

Example

As a partial explanation of why we must be careful in our usage of the symbol ∞ , consider the following bogus “proof” that $2 = 1$.

Many people might agree that $2 \cdot \infty = \infty$ and that $\infty / \infty = 1$. Then, assuming the normal rules of arithmetic,

$$1 = \frac{\infty}{\infty} = \frac{2\infty}{\infty} = 2 \cdot \frac{\infty}{\infty} = 2.$$

¹Dieter Goldkuhl (1938 - 2011) was a master stained glass artisan. In this quote, he is discussing his craft, but it applies more widely. In particular, mathematics is also a craft, though primarily of the mind rather than hand.

11.4.4

Example

For the following sets $A \subset \mathbb{R}$ we specify $\inf A$ and $\sup A$:

1. $A = (0, 1)$; $\sup A = 1$, $\inf A = 0$. Note that neither $\sup A$ nor $\inf A$ is an element of A .
2. $A = [0, 1]$; $\sup A = 1$, $\inf A = 0$. Note that $\sup A \notin A$ but $\inf A \in A$.
3. $A = (0, 1]$; $\sup A = 1$, $\inf A = 0$. Note that $\sup A \in A$ but $\inf A \notin A$.
4. $A = [0, 1]$; $\sup A = 1$, $\inf A = 0$. Note that both $\sup A, \inf A \in A$.
5. $A = (-2, 3] \cup (4, 17]$; $\sup A = 17$, $\inf A = -2$
6. $A = \{1/n : n \in \mathbb{N}\}$; $\sup A = 1$, $\inf A = 0$.
7. $A = \{3, 3.1, 3.14, 3.141, 3.1415, 3.14159, \dots\}$ (the truncations of the decimal expansion for π). Then $\sup A = \pi$ and $\inf A = 3$.
8. $A = \mathbb{R}$; $\inf A = -\infty$, $\sup A = \infty$.
9. $A = \emptyset$; $\inf A = \infty$, $\sup A = -\infty$.

The fundamental property of the real numbers is that infima and suprema exist as real numbers for bounded sets.

11.4.5

Theorem ▶ Fundamental Theorem of the Real Numbers

Suppose that $A \subset \mathbb{R}$ is non-empty and has an upper bound that is a real number. Then $\sup A$ exists and $\sup A \in \mathbb{R}$. Similarly, if $A \subset \mathbb{R}$ is non-empty and has a lower bound that is a real number, then $\inf A$ exists and $\inf A \in \mathbb{R}$.

The proof of this theorem relies on a precise definition of \mathbb{R} which we have not yet given.

Proof. (The proof that the supremum exists is deferred to Theorem 12.3.24.)

Once we know that suprema exist, it is easy to deduce the existence of infima. We do this by reflecting \mathbb{R} so that infima become suprema and vice versa.

Suppose that $A \subset \mathbb{R}$ is non-empty and has a lower bound m which is a real number. Let $-A = \{a \in \mathbb{R} : -a \in A\}$. Let $b \in -A$. Then $-b \in A$ and so $m \leq -b$. Consequently, $-m \geq b$. Hence, $-A$ has an upper-bound which is a real number. By the previous (unproved) result, $\sup(-A) \in \mathbb{R}$. Let $\beta = -\sup(-A)$. Since $-m$ is an upper-bound for $-A$, $\sup(-A) \leq -m$. Thus, $\beta \geq m$. This is true for all lower-bounds m for A and so, $\beta = \inf A$ is a real number. \square

11.4.6

Lemma

Suppose that $A \subset B \subset \mathbb{R}$. Then $\inf B \leq \inf A$ and $\sup A \leq \sup B$.

We will need the next result later, there is a similar result for infima.

11.4.7

Theorem

Suppose that (x_n) is a sequence in \mathbb{R} and let A be the range of the sequence. Then either $\sup A \in A$ or (x_n) has a subsequence which is strictly increasing.

Proof. Let A be the range of (x_n) and suppose that $\sup A \notin A$. We will construct a strictly increasing subsequence of A . Let $n_0 = 0$, so that $x_{n_0} = x_0$. Now assume that we have defined n_0, \dots, n_k so that $n_0 < n_1 < \dots < n_k$ and so that $x_{n_0} < x_{n_1} < \dots < x_{n_k}$. We will define n_{k+1} so that $n_0 < n_1 < \dots < n_{k+1}$ and so that $x_{n_0} < x_{n_1} < \dots < x_{n_{k+1}}$. By induction we will then have our desired subsequence.

Consider $S = \{m \in \mathbb{N} : m > n_k \text{ and } x_m > x_{n_k}\}$. If $S = \emptyset$, then for all $m > n_k$ we have $x_m \leq x_{n_k}$. Since there are only finitely many terms of (x_n) which come before x_{n_k} , either one of those terms or x_{n_k} is the supremum of A . This contradicts the assumption that $\sup A \notin A$. Consequently, $S \neq \emptyset$. Let $n_{k+1} \in S$. Then $n_{k+1} > n_k > \dots > n_0$ and $x_{n_{k+1}} > x_{n_k} > \dots > x_0$, so we are done. \square

We use the existence of suprema and infima to prove that all sequences in \mathbb{R} have monotonic subsequences.

11.4.8

Theorem

Suppose that (x_n) is a sequence in \mathbb{R} . Then (x_n) has a monotonic subsequence, i.e. a subsequence which is either increasing or decreasing.

Proof. Suppose that (x_n) is a sequence in \mathbb{R} such that no subsequence of (x_n) is increasing. We will prove that (x_n) has a subsequence which is strictly decreasing.

Let A be the range of (x_n) . By Theorem 11.4.7, $\sup A \in A$. Let $n_0 \in \mathbb{N}^*$ be the number such that $x_{n_0} = \sup A_0$. Assume that we have defined n_0, \dots, n_k so that the following hold:

- (i) $n_0 < \dots < n_k$
- (ii) $x_{n_0} > \dots > x_{n_k}$
- (iii) For each $j \in \{0, \dots, k\}$, $x_{n_j} = \sup A \setminus \{x_0, \dots, x_{n_{j-1}}\}$.

We will show that there exists n_{k+1} so that

- (i') $n_0 < \dots < n_k < n_{k+1}$
- (ii') $x_{n_0} > \dots > x_{n_k} > x_{n_{k+1}}$
- (iii') For each $j \in \{0, \dots, k+1\}$, $x_{n_j} = \sup A \setminus \{x_0, \dots, x_{n_{j-1}}\}$.

By induction we will have created the desired subsequence (x_{n_k}) .

Let $S = A \setminus \{x_0, \dots, x_{n_k}\}$. Since (x_n) does not have an increasing subsequence, it does not have a constant subsequence. Thus, by Theorem 11.1.7, A is an infinite set. Since $\{x_0, \dots, x_{n_k}\}$ is finite, the set S is non-empty. By Theorem 11.4.7, $\sup S \in S$. Choose $n_{k+1} \in \mathbb{N}$ be the number such that $x_{n_{k+1}} = \sup S$. Thus, (iii') holds.

If $n_{k+1} \leq n_k$, then $x_{n_{k+1}} \in \{x_0, \dots, x_{n_k}\} = A \setminus S$. This is impossible since $x_{n_{k+1}} \in S$. Thus, (i) holds.

Finally, note that

$$\{x_0, \dots, x_{n_{k-1}}\} \subset \{x_0, \dots, x_{n_k}\}$$

which implies that

$$A \setminus \{x_0, \dots, x_{n_{k-1}}\} \supset A \setminus \{x_0, \dots, x_{n_k}\}.$$

Hence, by Lemma 11.4.6,

$$x_{n_k} = \sup A \setminus \{x_0, \dots, x_{n_k}\} \geq A \setminus \{x_0, \dots, x_{n_k}\} = x_{n_{k+1}}.$$

Since $x_{n_k} \neq x_{n_{k+1}}$, we have (ii'). □

11.4.9

Theorem ▶ Monotonic Bounded Sequences Converge

Suppose that (x_n) is a monotonic sequence in \mathbb{R} and that there exists $a < b$ such that for all n , $x_n \in [a, b]$. Then (x_n) converges to some real number $r \in [a, b]$. Furthermore, if (x_n) is increasing then r is the supremum of the range of (x_n) and if (x_n) is decreasing then r is infimum of the range of (x_n) .

Proof. Let A be the range of the monotonic sequence (x_n) and assume that $A \subset [a, b]$. Since A is bounded, $\sup A$ and $\inf A$ exist and are real numbers.

Assume, first, that (x_n) is increasing. Let $\beta = \sup(x_n)$. We claim that (x_n) converges to β . To prove that, we must show that for all $\epsilon > 0$ there exists $N \in \mathbb{N}$ such that $d(x_n, \beta) < \epsilon$ if $n \geq N$.

Suppose that there exists $n_0 \in \mathbb{N}$ with $d(x_{n_0}, \beta) < \epsilon$. Since (x_n) is an increasing sequence and since β is an upper bound for A , we have that for all $n \geq n_0$, $d(x_n, \beta) < \epsilon$, implying that (x_n) converges to β . Assume, therefore, that no such n_0 exists. Thus, $A \cap (\beta - \epsilon, \beta) = \emptyset$. This implies that $\beta - \epsilon/2$ is also an upper bound for A . However, β was the infimum (least upper bound) for A , and so we contradict the choice of β . Thus, (x_n) must converge to β .

Now assume that (x_n) is decreasing. Let $\alpha = \inf(x_n)$. We will show that (x_n) converges to α . The sequence $(-x_n)$ is an increasing sequence and $-\alpha$ is the supremum of its range. Thus, by the previous paragraph $(-x_n)$ converges to $-\alpha$. That is, for every $\epsilon > 0$, there exists $N \in \mathbb{N}$ such that

$$\epsilon > d(-x_n, -\alpha) = |-\alpha + x_n| = |\alpha - x_n| = d(x_n, \alpha).$$

Thus, by the definition of convergence, (x_n) converges to α . □

Here is an example of how Theorem 11.4.9 can be applied. This theorem should

be familiar to you from calculus.

11.4.10 **Theorem ▶ Comparison Test**

Suppose that the sequences (a_k) and (b_k) are sequences of non-negative real numbers and that for all k , $a_k \leq b_k$. If the series $\sum_{k=0}^{\infty} b_k$ converges, then so does the series $\sum_{k=0}^{\infty} a_k$.

(Hint: Remember that you need to show that the sequence $(s_n) = a_1, a_1 + a_2, a_1 + a_2 + a_3, \dots$ converges. Use that fact that each a_k is non-negative to conclude that (s_n) is monotonic. Use the hypothesis that the sequence of partial sums $b_1, b_1 + b_2, \dots$ converges to show that (s_n) is bounded.)

As another application, we can combine Theorem 11.4.8 and Theorem 11.4.9 to produce the following very useful result:

11.4.11 **Theorem ▶ Bolzano-Weierstrass**

Suppose that (x_n) is a sequence in $[a, b] \subset \mathbb{R}$. Then (x_n) has a convergent subsequence.

The Bolzano-Weierstrass Theorem plays such an important role in analysis and topology that it gives rise to the concept of “compactness.” Although compactness is a crucial concept in mathematics, we do not explore it in this text.

Finally, we reinterpret completeness in terms of lengths of paths.

11.4.12 **Theorem**

Let X be a metric space with the property that every finite length sequence converges. Then X is complete.

Taking the contrapositive, this theorem tells us that if a space is not complete then there is some finite length sequence that does not converge – i.e. a finite length walk may bring us outside the space.

Proof. Assume that X has the property that every sequence of finite length converges. Let α be a Cauchy sequence. We must show α converges. By Theorem 11.3.5, it suffices to show that α has a convergent subsequence. We will find such a subsequence by constructing a subsequence of finite length and then applying our hypothesis that all sequences of finite length converge.

We construct our subsequence recursively. By the definition of Cauchy, there exists $n_0 \in \mathbb{N}$ such that for all $m \geq n_0$, $d(x_{n_0}, x_m) < 1$. Assume that we have defined $n_0 < n_1 < \dots < n_k$ such that for $i \in \{0, \dots, k\}$ and if $m \geq n_i$, then

$$d(x_{n_i}, x_m) < \frac{1}{2^i}.$$

We will show that there is $n_{k+1} \in \mathbb{N}$ such that $n_{k+1} > n_k$ and if $m \geq n_{k+1}$, then

$$d(x_{n_{k+1}}, x_m) < \frac{1}{2^{k+1}}.$$

Let $\epsilon = \frac{1}{2^{k+1}}$. Since α is Cauchy, there exists $N \in \mathbb{N}$ such that for all $s, m \geq N$,

$$d(x_s, x_m) < \frac{1}{2^{k+1}}.$$

Let $n_{k+1} > \max\{N, n_k\}$. Thus, for all $m \geq n_{k+1}$ we have

$$d(x_{n_{k+1}}, x_m) < \frac{1}{2^{k+1}}.$$

By induction, we have a subsequence (x_{n_k}) such that for all k , $d(x_{n_k}, x_{n_{k+1}}) < \frac{1}{2^k}$. Thus, by the comparison test, the series

$$\sum_{k=0}^{\infty} d(x_{n_k}, x_{n_{k+1}}) \leq \sum_{k=1}^{\infty} \frac{1}{2^k} = 1.$$

Thus, we have a subsequence of finite total length as desired. \square

One of the most important results in mathematics is that \mathbb{R} with the Euclidean metric is complete. In Chapter 12, we give a *definition* of \mathbb{R} so that this holds. The more traditional route is to define the set \mathbb{R} so that Theorem 11.4.5 holds (using a different method from Chapter 12.) The Bolzano-Weierstrass theorem is then used to show that \mathbb{R} is complete (do you see how?).

11.5 Application: Circular Billiards

“To use a cue at billiards well is like using a pencil, or a German flute, or a small-sword – you cannot master any one of these implements at first, and it is only by repeated study and perseverance, joined to a natural taste, that a [person] can excel in the handling of either.”

–William Makepeace Thackeray, *Vanity Fair*

Have you ever played billiards, or some other traditional pool-table game? Perhaps as you did so you wondered if it was possible to hit the ball in a certain direction so that, if there were enough energy, the ball would bounce off of every point on the wall of the table (except for the pockets in the corners)? The considerations of Chapter 10 show the answer to is “no” - even with an infinite amount of energy, the ball (thought of as a point mass) would never hit every point on the walls. Of course, pool balls aren’t point masses and so we might ask:

Is it possible to hit the ball from some initial position and in some direction so that, if it had infinite energy, it will come arbitrarily close to each of the points on the walls?

In this chapter we explore this question for circular pool tables without pockets. For the case when the pool table is a rectangle and has pockets and many other possibilities, see [122]. We begin by revisiting rotations of a circle.

Rotations of a Circle

In this section, we elaborate on the example of Section 8.4. Let $\theta \in \mathbb{R}$ be thought of as an angle and let R_θ be the rotation of the circle $S^1 = \{(a, b) \in \mathbb{R}^2 : a^2 + b^2 = 1\}$ counter-clockwise by an angle of θ . If θ is negative, this means that we rotate S^1 clockwise by an angle of $|\theta|$. Since two real numbers which differ by an integer multiple of 2π are the same angle, we have $R_\theta = R_{\theta+2\pi k}$ for all $k \in \mathbb{Z}$. Also, since rotations don't change the distance between points in \mathbb{R}^2 , if there is a point $x \in S^1$ such that $R_\theta(x) = R_\psi(x)$, then there is $k \in \mathbb{Z}$ such that $\theta = \psi + 2\pi k$. As a consequence, observe that $R_{\theta+\psi} = R_\psi \circ R_\theta$ for all $\theta, \psi \in \mathbb{R}$. For $n \in \mathbb{N}$, we define $R_{n\theta}$ to be the composition of R_θ with itself n times. Similarly, $R_{-n\theta}$ is the composition of $R_{-\theta}$ with itself n times.

Given the initial point $x_0 = (1, 0) \in S^1$ and the real number θ , we can create an iterated function sequence (x_n) by letting

$$x_n = R_{n\theta}(x_0) = R_\theta(R_{(n-1)\theta}(x_0))$$

be the point obtained by rotating x_0 counter-clockwise n -times by an angle θ . In Theorem 8.4.10, we found that the sequence (x_n) has repeated terms if and only if θ is a rational multiple of π . In the remainder of this section, we consider what happens when θ is an irrational multiple of π . We show that the terms of the sequence (x_n) get as close as we could possibly wish to every point on the circle.

11.5.1

Theorem

If θ is an irrational multiple of π , then for every $p \in S^1$ and every $\epsilon > 0$, there exists $n \in \mathbb{N}$ such that $d(x_n, p) < \epsilon$.

The distance measure d we use in the statement of the theorem is the absolute value of the smaller of the two angles between the point x_n and the point p . Since the circle has unit radius, this is equal to the length of the shorter arc of the circle between x_n and p . Our proof is modelled on that in [122]

Proof. We begin by showing that the theorem holds if $p = x_0$ and that for all $k \in \mathbb{N}$, there exists $n_k \in \mathbb{N}$ such that $d(x_0, x_{n_k}) < \frac{|\theta|}{2^k}$. We prove this by induction on N .

We say that a point $c \in S^1$ is **between** points $a, b \in S^1$ if $d(a, b) < \pi$ and the arc of S^1 between a and b of length less than π contains c .

Base Case: $k = 1$.

Since θ is an irrational multiple of π , by Theorem 8.4.10, none of the points in the sequence x_1, x_2, x_3, \dots is equal to x_0 . Since the distance along S^1 between adjacent points in the sequence is equal to θ , by the well-ordering principle, there exists a smallest $m \in \mathbb{N}$ such that the point x_0 is between x_m and x_{m+1} .

\langle Show that either $d(x_0, x_m) \neq d(x_0, x_{m+1})$ \rangle

Let $n_k = n_1$ be either m or $m + 1$ so that x_{n_1} is whichever of x_m or x_{m+1} is closer to x_0 .

(Explain why $d(x_0, x_k) < |\theta|/2$.)

Inductive Step: Assume that for some $k \in \mathbb{N}$, there exists $n_k \in \mathbb{N}$ such that $d(x_{n_k}, x_0) < \frac{|\theta|}{2^k}$. We will show that there exists $n_{k+1} \in \mathbb{N}$ such that $d(x_{n_{k+1}}, d(x_0)) < \frac{|\theta|}{2^{k+1}}$.

Let ψ be the angle from x_0 to x_{n_k} , chosen so that $|\psi| < \pi$. Observe that $R_\psi = R_{n_k\theta}$, since the two rotations applied to x_0 both produce x_{n_k} . Thus, ψ and $n_k\theta$ differ by an integer multiple of 2π . In particular, this means that ψ is an irrational multiple of π and that for all $a \in \mathbb{N}$, the rotation $R_{an_k\theta} = R_{a\psi}$. See Figure 11.6 for the case when $k = 1$.

Let x_0 and y_m be the result of applying R_ψ to x_0 , m -times, for each $m \in \mathbb{N}$. By applying the base case to the rotation R_ψ instead of R_θ , we see that there exists $m_1 \in \mathbb{N}$ such that $d(y_{m_1}, x_0) < |\psi|/2$.

Let $n_{k+1} = m_1 n_k$. We claim that $d(x_{n_{k+1}}, x_0) < |\theta|/2^{k+1}$. To see this, recall that $x_{n_{k+1}}$ is equal to the result of rotating x_0 by an angle of $n_{k+1}\theta$. Since $n_{k+1}\theta = m_1 n_k \theta$ is the same angle as $m_1\psi$, we have that $R_{n_{k+1}\theta}(x_0) = R_{m_1\psi}(x_0)$. Thus, $x_{n_{k+1}} = y_{m_1}$. Consequently,

$$\begin{aligned} d(x_{n_{k+1}}, x_0) &= d(y_{m_1}, x_0) \\ &< |\psi|/2 = \frac{1}{2}d(x_{n_k}, x_0) \\ &< \frac{1}{2} \cdot \frac{|\theta|}{2^k} \\ &= \frac{|\theta|}{2^{k+1}}. \end{aligned}$$

Since the base case and inductive hypothesis hold, for all $k \in \mathbb{N}$, there exists $n_k \in \mathbb{N}$ such that $d(x_{n_k}, x_0) < |\theta|/2^k$.

Now suppose that $p \in S^1$ and $\epsilon > 0$ are given. There exists $k \in \mathbb{N}$, such that $|\theta|/2^k < \epsilon$. Hence, by the claim, there exists $n_k \in \mathbb{N}$ such that $d(x_{n_k}, x_0) < \epsilon$. As in the inductive step, let ψ be the angle between from x_0 to x_{n_k} , chosen so that $|\psi| < \pi$. Recall that ψ is the same angle as $n_k\theta$. Let $I \subset S^1$ be the closed interval of length $|\psi|$ and with endpoints x_0 and x_{n_k} . Applying $R_\psi = R_{n_k\theta}$ to I produces an interval I_1 of length $|\psi|$, having the point $x_{n_k} = R_\psi(x_0)$ as an endpoint and with $I_1 \cap I = \{x_{n_k}\}$. Recursively define I_{m+1} to be the result of applying R_θ to I_m . It is an interval of length $|\psi|$ and having $I_m \cap I_{m+1} = \{R_{m\psi}(x_0)\}$. Let N be the natural number such that $N|\psi| < 2\pi$ and $(N+1)|\psi| > 2\pi$. The union of the intervals, I_1, I_2, \dots, I_{N+1} is, therefore, equal to S^1 . Hence, there exists $a \in \{1, \dots, N+1\}$ such that $p \in I_a$. The endpoints of I_a are points in the sequence x_0, x_1, x_2, \dots and so there exists one of those endpoints x_n , with $n \in \mathbb{N}$ such that

$$d(x_n, p) < |\psi| < \epsilon.$$

□

11.5.2

Exercise

Explain how to adapt the previous proof to show that, when θ is an irrational multiple of π , there is a subsequence (x_{n_k}) of n_k converging to x_0 .

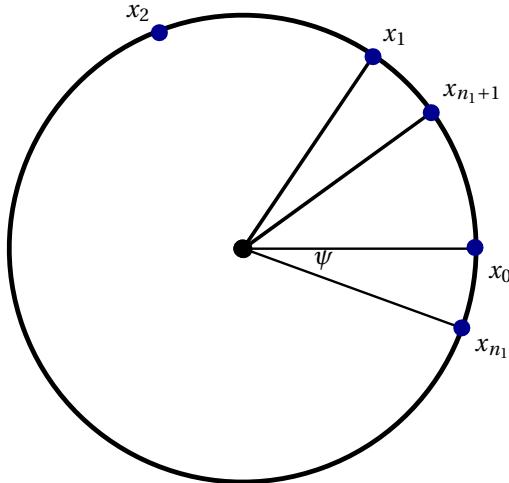


Figure 11.6: The angles and points appearing in the proof of Theorem 11.5.1.

11.5.3

Exercise

Using the statement, but not the proof, of Theorem 11.5.1, prove that when θ is an irrational multiple of π , for every $p \in S^1$, the sequence (x_n) has a subsequence converging to p .

11.5.4

Exercise

In the previous proof, we used, as our measurement of distance, the distance along the circle S^1 . Is the result still true if we were instead to use the Euclidean metric on \mathbb{R}^2 ? Why or why not?

Circular pool tables

In this section, consider the disc $D = \{(a, b) \in \mathbb{R}^2 : a^2 + b^2 \leq 1\}$ as an idealized model of a circular pool table without pockets. We will consider a point P inside D as an idealized ball. If the ball P is propelled in some direction, it will hit the wall $S^1 = \{(a, b) \in \mathbb{R}^2 : a^2 + b^2 = 1\}$ of the table and bounce. It bounces according to the Law of Reflection: the angle of reflection is equal to the angle of incidence. Angles at a point $x \in S^1$ are defined with respect to the tangent line to the circle S^1 at the point x . We will assume that there is no loss of energy as P travels across D and bounces off the wall. We arrive at an infinite sequence of points (x_n) in S^1 . The point x_1 is the first place where P hits the wall; the point x_2 the second place, etc.

11.5.5

Theorem

Suppose that the ball P starts at a position $x_0 \in S^1$ and that it is initially propelled in a direction forming an angle $\beta \in (-\pi/2, \pi/2)$ with the diameter of S^1 . If β is an irrational multiple of π , then, for all $p \in S^1$, the sequence (x_n) of points in S^1 hit by P has a subsequence converging to p . In other words, the ball will come arbitrarily close to each point on the wall of the table.

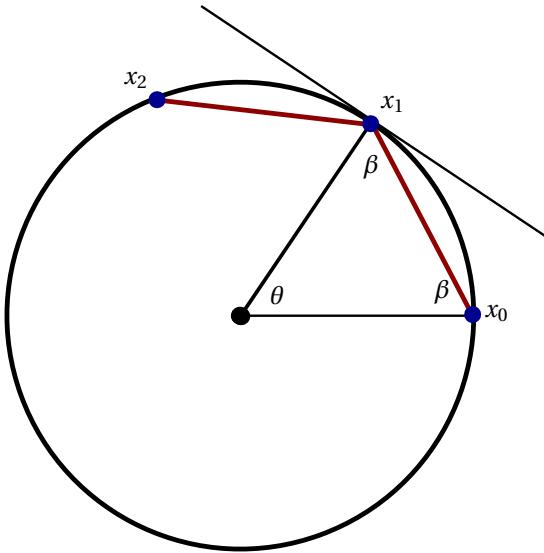


Figure 11.7: The angles and points appearing in the proof of Theorem 11.5.5.

Proof Sketch. Recall that $x_0 \in S^1$ is the starting point of P and that x_1 is the first place on S^1 where P bounces. Let O be the center of the circle. The triangle with corners x_0 , x_1 , and O , is an isosceles triangle with the angles at x_0 and x_1 having measure $|\beta|$ and the angle θ at O having measure $|\theta| = \pi - 2|\beta|$. Observe that since β is an irrational multiple of π , so is θ . The point x_1 is, therefore, obtained from x_0 by rotating by the angle θ . (We choose the sign of θ so that if we rotate counter-clockwise to get from x_0 to x_1 , then θ is positive. Otherwise θ is negative.) See Figure 11.7.

Since the diameter of a circle is perpendicular to the lines tangent to the circle at its endpoints, by the Law of Reflection, as P bounces off S^1 at x_1 , it bounces at an angle β with respect to the diameter of the circle with endpoint x_1 . Consequently, x_2 is obtained from x_1 by rotating x_1 by an angle of θ . A proof by induction shows that, in general, x_{k+1} is obtained from x_k by rotating S^1 by an angle of θ .

Without loss of generality, by rotating the circle, we may assume that $x_0 = (1, 0)$. Thus, by Theorem 11.5.1 and Exercise 11.5.3, the sequence (x_n) has a subsequence converging to any given $p \in S^1$. \square

11.5.6

Exercise

Turn the previous proof sketch into a complete proof. In particular, write the induction proof with a correctly stated base case and inductive hypothesis.

11.6 Additional Problems

“Don’t add new injuries to the long, long list of injuries you have done me!”

– Charles Dickens, *David Copperfield*

- Let \mathcal{S} be the set of sequences in a metric space (X, d) . If (x_n) and (y_n) are elements of \mathcal{S} , define $(x_n) \sim (y_n)$ if and only if either $(x_n) = (y_n)$ or for all $\epsilon > 0$, there exists $N \in \mathbb{N}$ such that whenever $n, m \geq N$ then $d(x_n, y_m) < \epsilon$. Prove that \sim an equivalence relation.
- Suppose that X and Y are complete metric spaces with metrics d_X and d_Y respectively. Give $X \times Y$ the product metric

$$d((x_1, y_1), (x_2, y_2)) = \max(d_X(x_1, x_2), d_Y(y_1, y_2))$$

Prove that $X \times Y$ is complete.

- Do the same as the previous problem, but with the product metric

$$d((x_1, y_1), (x_2, y_2)) = \sqrt{(d_X(x_1, x_2)^2 + d_Y(y_1, y_2)^2)}$$

- Prove that \mathbb{R}^n is complete for all $n \geq 2$.

12 | New Numbers from Completed Spaces

“[T]wixt which regions
There is some space. A space whose ev’ry cubit
Seems to cry out”
William Shakespeare, *The Tempest*

Earlier in this book, we saw how we can start with the empty set \emptyset and construct all the extended natural numbers \mathbb{N}^* . Using equivalence relations we can then construct the integers \mathbb{Z} and the rational numbers \mathbb{Q} . But how can we construct the real numbers \mathbb{R} ? We’ve discovered that \mathbb{R} is uncountable, whereas \mathbb{N} , \mathbb{Z} , and \mathbb{Q} are all countable. Our results on countable sets suggest that we need some new idea to create \mathbb{R} as simply putting different copies of rationals together to try to form the reals will likely only end up creating a countable set, rather than the uncountable set we are hoping for.

The key is to remember that real numbers can be approximated by rationals. That is, for every real number $r \in \mathbb{R}$ there exists a sequence of rationals (x_n) converging to r . That is, for every $\epsilon > 0$, as long as n is large enough $|x_n - r| < \epsilon$. This suggests that notions of *distance* will be important. For example, the sequence of rational numbers $3, 3.1, 3.14, 3.141, 3.1415, \dots$ converges to π and $\pi = 3.14159\dots$. Similarly, the sequence of rational numbers $1, 1.4, 1.41, 1.414, 1.4142, \dots$ (continued in the appropriate way) converges to $\sqrt{2}$ and $\sqrt{2} = 1.4142\dots$. So if the rationals are all we know about, perhaps we can consider π to be the sequence $3, 3.1, 3.14, 3.1415, \dots$. Perhaps we can consider $\sqrt{2}$ to be the sequence $1, 1.4, 1.41, 1.414, \dots$.

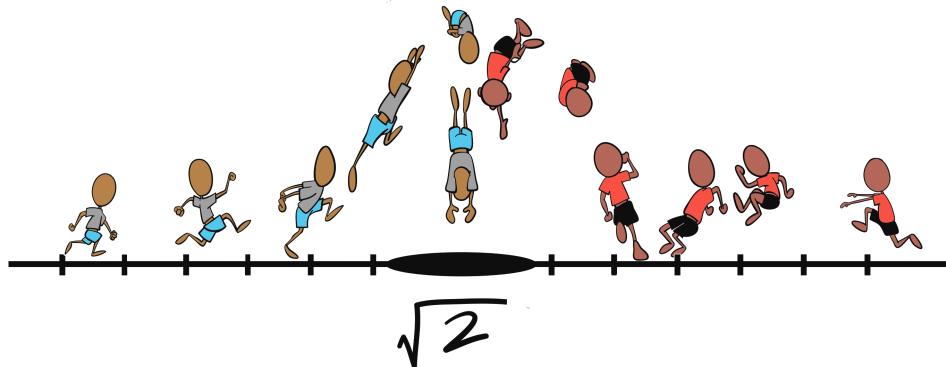
But, there’s a problem. For a given real number r there is more than one sequence of rationals converging to it. For example,

$$\alpha = 1, 1.4, 1.41, 1.414, 1.4142, 1.41421, \dots$$

converges to $\sqrt{2}$, but so does

$$\beta = 1.5, 1.42, 1.415, 1.4143, 1.41422, \dots$$

We can’t consider $\sqrt{2}$ to be both α and β since $\alpha \neq \beta$ – they are different sequences!



How can we consider α and β to be equal, even though they are different? Equivalence relations! The basic strategy for creating \mathbb{R} from \mathbb{Q} will be to impose an equivalence relation on a set of sequences in \mathbb{Q} and then consider \mathbb{R} to be the quotient set. The key to coming up with the right equivalence relation is to use the distance function on \mathbb{Q} . Essentially, the distance function d will tell us where the “holes” in the rationals are. For one of these holes, we’ll look at the sequences that converge to it and declare these sequences to be equivalent. The real number that fills the hole is then *defined* to be the equivalence class of those sequences.

This line of inquiry is remarkably productive, for by changing our notion of distance, we can create new number systems, different from \mathbb{R} . We discover that the *spatial* properties of the rationals \mathbb{Q} determine the *arithmetic* properties of the new number systems.

12.1 Metric Completions

“Now come, my Ariel, bring a corollary”
—William Shakespeare, *The Tempest*

We begin by working more generally. Throughout this section assume that X is a metric space with metric d . Recall from the definition of “metric,” that the metric is a function $d: X \times X \rightarrow [0, \infty)$. Notice that this means we already are working with the reals. We’ll explain how to avoid this later, but for now assume that we do have the real numbers and understand their usual arithmetic properties.

In X , a **Cauchy sequence** is a sequence (x_n) with the property that given an error threshold $\epsilon > 0$, as long as n and m are large enough, $d(x_n, x_m) < \epsilon$. That is, the terms of the sequence are eventually arbitrarily close together. Cauchy sequences are the sequences that “should” converge. In a complete space (Section 11.3) every Cauchy sequence converges. That is, a complete space has no holes. Compare to the discussion of sequences of finite total length in Theorem 11.3.9.

We have seen how \mathbb{Q} is an example of an incomplete space (Exercise 11.3.12) and alluded to how \mathbb{R} is a complete space (Section 11.4). We may think of \mathbb{R} as a way

of filling the (uncountably many) holes in \mathbb{Q} using the irrationals. In this section we show how given any metric space we may fill in the holes. The challenge, however, is that for an arbitrary metric space (unlike for \mathbb{Q}) we do not know what the holes are – so how can we fill them in? What we do is that we consider the Cauchy sequences *themselves* to be the holes and we add in those sequences as new points in our space.

Recalling that X is a metric space with metric d , let \mathcal{C} denote the set of Cauchy sequences in X . We define an equivalence relation, called **Cauchy equivalence** and denoted \sim , on \mathcal{C} as follows. Suppose that (r_k) and (s_k) are two Cauchy sequences. This means that eventually, all the terms of (r_k) are close to each other and all the terms of (s_k) are close to each other. We define $(r_k) \sim (s_k)$ if and only if eventually all the terms of (r_k) are close to all the terms of (s_k) . More precisely, $(r_k) \sim (s_k)$ if and only if for all $\epsilon > 0$, there exists $N \in \mathbb{N}$ such that for all $n, m \geq N$, we have $d(r_n, s_m) < \epsilon$.

12.1.1

Theorem

The relation \sim is an equivalence relation on \mathcal{C} .

We let $\hat{X} = X/\sim$ be the quotient set. We want to show that \hat{X} has a metric \hat{d} relative to which it is complete and, furthermore, that there is a way to make X sit inside \hat{X} in a way similar to how the rationals sit inside the reals. The set \hat{X} is called the **metric completion** of X . Here's how we do it.

We begin by observing that pairs of sequences of points in \hat{X} give us a sequence of distances.

12.1.2

Theorem

Let $a = (a_k)$ and $b = (b_k)$ be Cauchy sequences in X . Then the sequence $(d(a_k, b_k))$ is a Cauchy sequence in \mathbb{R} .

Proof. Let $d_k = d(a_k, b_k)$ and let $\epsilon > 0$. We will show that there is $N \in \mathbb{N}$ such that for all $n, m \geq N$, we have $|d_n - d_m| < \epsilon$.

Since a is Cauchy, there exists $N_a \in \mathbb{N}$ such that for all $n, m \geq N_a$, we have $d(a_n, a_m) < \epsilon/2$. Similarly, there exists $N_b \in \mathbb{N}$ such that for all $n, m \geq N_b$, we have $d(b_n, b_m) < \epsilon/2$. Let $N = \max(N_a, N_b)$. Let $n, m \geq N$ with $d_n \geq d_m$. Then we have,

$$\begin{aligned} 0 &\leq d_n - d_m \\ &= d(a_n, b_n) - d(a_m, b_m) \\ &\leq d(a_n, a_m) + d(a_m, b_n) - d(a_m, b_m) \\ &\leq d(a_n, a_m) + d(a_m, b_m) + d(b_m, b_n) - d(a_m, b_m) \\ &= d(a_n, a_m) + d(b_m, b_n) \\ &< \epsilon. \end{aligned}$$

□

Since \mathbb{R} is complete, the sequence $(d(a_k, b_k))$ converges whenever $a = (a_k), b = (b_k) \in \mathcal{C}$. Let $\hat{d}(a, b)$ be its limit. It turns out this limit is independent of the

representatives from the equivalence classes.

12.1.3

Theorem

Suppose that $a = (a_k), a' = (a'_k), b = (b_k), b' = (b'_k)$ are elements of \mathcal{C} with $a \sim a'$ and $b \sim b'$. Then $\hat{d}(a, b) = \hat{d}(a', b')$.

(Hint: Let $\epsilon > 0$ be arbitrary. Show that for k large enough, $d(a_k, b_k)$ is within ϵ of $d(a'_k, b'_k)$. Explain why this suffices to show the result.)

Consequently, we can declare $\hat{d}([a], [b]) = \hat{d}(a, b)$ for all $a, b \in \mathcal{C}$ and have a concept that is well-defined. The next step shows that \hat{d} is a metric.

12.1.4

Theorem

The space \hat{X} is a metric space with metric \hat{d} .

We now consider how to make X sit inside \hat{X} . We define a function $\iota: X \rightarrow \hat{X}$ which does not change distance. In particular, for $x \in X$, let \hat{x} be the equivalence class of the constant sequence $\bar{x} = (x)$. Define $\iota: X \rightarrow \hat{X}$ by $\iota(x) = \hat{x}$. The function ι is called an **embedding** and it turns out that the range of ι is **dense** in X . That is, every open ball in \hat{X} contains a point of range ι .

12.1.5

Theorem

The function ι is distance-preserving. That is, for all $x, y \in X$, we have $d(x, y) = \hat{d}(\hat{x}, \hat{y})$. Furthermore, the range of ι is dense in \hat{X} .

Proof. We have

$$\hat{d}(\hat{x}, \hat{y}) = \hat{d}(\bar{x}, \bar{y}) = \lim d(x, y) = d(x, y)$$

since \bar{x} and \bar{y} are constant sequences.

Now suppose that $\alpha = [(r_k)] \in \hat{X}$. Let $\epsilon > 0$. We must show that there exists $x \in X$ such that $\hat{d}(\alpha, \hat{x}) < \epsilon$. Since α is Cauchy, there exists $N \in \mathbb{N}$ such that for all $n, m \geq N$ we have $d(r_n, r_m) < \epsilon$. Let $x = r_N$. Then,

$$\hat{d}(\alpha, \hat{x}) = \hat{d}((r_k), \bar{x}) = \lim d(r_k, x) = \lim d(r_k, r_N) < \epsilon.$$

□

Finally, we need to prove that \hat{X} is complete. This means that we need to show that a Cauchy sequence of equivalence classes of Cauchy sequences converges! We begin with a restricted class of Cauchy sequences. Consider a Cauchy sequence $(x_k) \in \mathcal{C}$. Each term of the sequence is an element of X . We convert each of those elements x_k into a constant sequence \bar{x}_k . We then have a sequence of constant sequences, namely (\bar{x}_k) . Taking equivalence classes, we arrive at a sequence in \hat{X} , namely $([\bar{x}_k])$. Recall that $\hat{x}_k = [\bar{x}_k]$, so we can also write this sequence as (\hat{x}_k) .

12.1.6

Example

Consider the situation when $X = \mathbb{Q}$ and d is the usual euclidean metric on X . The set \mathcal{C} consists of all Cauchy sequences in X . The sequence $(1/k)$ for $k \in \mathbb{N}$ is one such sequence. For each $k \in \mathbb{N}$, the term $x_k = 1/k \in \mathbb{Q}$. Convert each term of (x_k) into a constant sequence. This gives us a sequence (\bar{x}_k) of constant sequences:

$$\begin{aligned}\bar{x}_1 &= 1, 1, 1, 1, \dots \\ \bar{x}_2 &= \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \dots \\ \bar{x}_3 &= \frac{1}{3}, \frac{1}{3}, \frac{1}{3}, \frac{1}{3}, \dots \\ &\vdots\end{aligned}$$

Considering equivalence classes, we have the sequence $([\bar{x}_k]) = (\hat{x}_k)$. The first term of this sequence is the equivalence class:

$$\hat{x}_1 = [\bar{x}_1] = [1, 1, 1, \dots] = [1.1, 1.01, 1.001, 1.0001, \dots],$$

for example.

We claim that this sequence $([\bar{x}_k])$ in \hat{X} converges to $([x_k])$, which is the equivalence class of our original sequence in X . To see this, let $\epsilon > 0$. We must show that there exists $N \in \mathbb{N}$ such that for all $k \geq N$,

$$\hat{d}([\bar{x}_k], [x_m]) < \epsilon.$$

Since (x_k) is Cauchy, there exists $N \in \mathbb{N}$ such that for all $n, m \geq N$ we have $d(x_n, x_m) < \epsilon$. Hence, for all $n \geq N$,

$$\hat{d}(\bar{x}_n, x_m) < \epsilon.$$

Thus by the definition of \hat{d} on \hat{X} , we have, for all $n \geq N$,

$$\hat{d}([\bar{x}_n], [x_m]) < \epsilon,$$

as desired.

It is now relatively easy to prove that \hat{X} is complete.

12.1.7

Theorem

\hat{X} is complete.

Proof. Let (α_k) be a Cauchy sequence in \widehat{X} . We must show that there exists $\alpha \in \widehat{X}$ such that for all $\epsilon > 0$, there exists $N \in \mathbb{N}$ so that for all $k \geq N$,

$$\widehat{d}(\alpha_k, \alpha) < \epsilon.$$

By Theorem 12.1.5, for each k , there exists a point $x_k \in X$, such that $\widehat{d}(\alpha_k, \widehat{x}_k) < \frac{1}{2^k}$.

(Show that (x_k) is Cauchy.)

Let $\beta = [(x_k)] \in \widehat{X}$.

(Show that (α_n) converges in \widehat{X} to β .)

□

12.2 The 10-adic numbers

“O wonder! How many goodly creatures are there here!”

—William Shakespeare, *The Tempest*

Why is

0.123123123123...

a number, but

...123123123123.0

not?

The answer is provided by Calculus. The decimal representation

0.123123123123...

refers to the infinite series

$$\frac{1}{10} + \frac{2}{100} + \frac{3}{1000} + \frac{1}{10^4} + \dots$$

This series converges since the sequence of partial sums converges (it is an increasing, bounded sequence).

The decimal representation

...123123123123.0

on the other hand refers to the infinite series

$$3 + 2 \cdot 10 + 1 \cdot 10^2 + 3 \cdot 10^3 + 2 \cdot 10^4 + 1 \cdot 10^5 + \dots$$

which diverges to infinity, since the sequence of partial sums diverges to infinity.

However, if we change our metric (and, thus, our notion of convergence) we can create a number system where

$$\dots 123123123123.0$$

is, in fact, a genuine number. We do this by imposing a new distance metric on \mathbb{Q} to get a metric space we call \mathbb{Q}_{10} and then taking the metric completion to obtain a metric space $\overline{\mathbb{Q}}_{10}$.

12.2.1

Definition ▶ rational 10-adic metric

For $a \in \mathbb{Z} \setminus \{0\}$, let $v(a)$ be the number $n \in \mathbb{N}^*$ such that $a = 10^n m$ where $m \in \mathbb{Z}$ is not a multiple of 10. For a fraction $\frac{a}{b} \in \mathbb{Q} \setminus \{0\}$, let

$$v(a/b) = v(a) - v(b).$$

12.2.2

Example

We have:

- $v(7) = v(10^0 \cdot 7) = 0$.
- $v(700) = v(10^2 \cdot 7) = 2$.
- $v(20/37) = v(20) - v(37) = 1 - 0 = 1$.
- $v(-\frac{19}{700}) = 0 - 2 = -2$.

12.2.3

Exercise

Show that v is well-defined on $\mathbb{Q} \setminus \{0\}$.

We now define a version of absolute value.

12.2.4

Definition

For $r \in \mathbb{Q}$, let

$$|r|_{10} = \begin{cases} 10^{-v(r)} & r \neq 0 \\ 0 & r = 0 \end{cases}$$

12.2.5

Example

We have:

- $|7|_{10} = 10^0 = 1$.
- $|700|_{10} = 10^{-2} = .01$.
- $|20/37|_{10} = 10^{-1} = .1$.
- $|-\frac{19}{700}|_{10} = 10^2 = 100$.

12.2.6

Exercise

Prove the following for all $q, r \in \mathbb{Q}$.

- $|q|_{10} \geq 0$ with equality if and only if $q = 0$.
- $|qr|_{10} \leq |q|_{10}|r|_{10}$
- $|q+r|_{10} \leq |q|_{10} + |r|_{10}$.

12.2.7

Exercise

Let $s_n = 1 + 10 + 100 + \dots + 10^n$. Show that for all $n \in \mathbb{N}$,

$$|s_n - s_{n-1}|_{10} = \frac{1}{10^n}.$$

Now, as we do with absolute value, we can turn the 10-adic norm into a metric on \mathbb{Q} .

12.2.8

Definition ▶ 10-adic metric

For $q, r \in \mathbb{Q}$. Let

$$d_{10}(q, r) = |q - r|_{10}.$$

12.2.9

Theorem

The function d_{10} is a metric on \mathbb{Q} .

Henceforth, we let \mathbb{Q}_{10} denote the metric space (\mathbb{Q}, d_{10}) .

12.2.10

Exercise

Let $s_n = 1 + 10 + 100 + \dots + 10^n$. Show that (s_n) is a Cauchy sequence in \mathbb{Q}_{10} .

The next two exercises gives an example of the very different behaviour of \mathbb{Q} with the metric d_{10} from \mathbb{Q} with the usual metric.

12.2.11

Exercise

Let $s_n = 1 + 10 + 100 + \dots + 10^n$. Prove that the sequence (s_n) converges in \mathbb{Q}_{10} to $-\frac{1}{9}$. Conclude that in \mathbb{Q}_{10} , we have

$$\dots 1111.0 = -\frac{1}{9}.$$

12.2.12

Exercise

Let $s_n = \frac{1}{10} + \frac{1}{100} + \cdots + \frac{1}{10^n}$. Prove that the sequence (s_n) is unbounded in (\mathbb{Q}, d_{10}) and is therefore not Cauchy. Conclude that the series

$$0.1111\dots$$

diverges to ∞ .

12.2.13

Exercise

1. Give examples of $a, b \in \mathbb{N}$ such that $a < b$ and b is closer in \mathbb{Q}_{10} to 0 than is a i.e.

$$d_{10}(0, b) < d_{10}(0, a).$$

2. Give examples of $a, b \in \mathbb{N}$ such that $a < b$ and a is closer in \mathbb{Q}_{10} to 0 than is b i.e.

$$d_{10}(0, a) < d_{10}(0, b).$$

3. Give examples of $a, b \in \mathbb{N}$ such that $a < b$ and

$$d_{10}(0, a) = d_{10}(0, b).$$

12.2.14

Exercise

Show that for all $n \in \mathbb{Z}$,

$$d_{10}(0, n) \leq 1.$$

That is, the copy of \mathbb{N} sitting inside of \mathbb{Q}_{10} is bounded.

We let $\widehat{\mathbb{Q}}_{10}$ denote the metric completion of \mathbb{Q}_{10} .

12.2.15

Theorem

For each $i \in \mathbb{N}$, let $d_i \in \{0, 1, 2, \dots, 9\}$. Prove that the sequence (s_n) defined by

$$s_n = d_1 + d_2 \cdot 10 + d_3 \cdot 10^3 + \cdots + d_n 10^n$$

is a Cauchy sequence in (\mathbb{Q}, d_{10}) and thus

$$\cdots d_4 d_3 d_2 d_1.0 \in \widehat{\mathbb{Q}}_{10}.$$

For $\widehat{\mathbb{Q}}_{10}$ to be considered a new number system and not just a new space, we must genuinely be able to add, subtract, multiply, etc. It is not difficult to show that since we can add, subtract, multiply Cauchy sequences in \mathbb{Q}_{10} to get new Cauchy sequences in \mathbb{Q}_{10} these operations carry over to $\widehat{\mathbb{Q}}_{10}$. We then have then a new number system, containing the rationals, that is complete but which is

genuinely different from \mathbb{R} .

12.2.16 Exercise

The usual absolute value on \mathbb{R} (or \mathbb{Q}) has the property that $|ab| = |a||b|$ for all a, b . Show that $|\cdot|_{10}$ does not have this property.

Looking back at what we've done, we can see that there was nothing special about the number 10 - we could have replaced it with any $p \in \mathbb{N}$ such that $p \geq 2$ to obtain a new number system $\hat{\mathbb{Q}}_p$, called the **p -adics**. These number systems are extremely useful in number theory, especially when p is chosen to be a prime number, for in that case $|\cdot|_p$ does function more like an absolute value. For more, see [56].

12.3 Constructing \mathbb{R}

Miranda: "You have often
Begun to tell me what I am, but stopp'd
And left me to a bootless inquisition,
Concluding, 'Stay: not yet.'"
Prospero: "The hour's now come"
—William Shakespeare, *The Tempest*

We have discussed how to build the rationals from the integers using an equivalence relation on pairs of integers and how to complete a metric space using an equivalence relation on Cauchy sequences. This suggests that we might be able to construct \mathbb{R} from \mathbb{Q} using an equivalence relation on Cauchy sequences in \mathbb{R} . The difficulty, as we have already noted is that in the construction of the completed \hat{X} from X we used the fact that \mathbb{R} was complete. Here we sketch how to overcome this logical bind. According to [41], this approach is originally due to Cantor. We begin by reframing our definitions in such a way that we only start with the algebraic and metric properties of \mathbb{Q} . We let d denote the euclidean metric $d(a, b) = |a - b|$ on \mathbb{Q} for all $a, b \in \mathbb{Q}$. Observe that the distance between two rationals is always a rational. The following definitions are nearly the same as before, except that we consider only *rational* values for ϵ .

12.3.1 Definition

Let (a_n) be a sequence in \mathbb{Q} . It **converges** to $a \in \mathbb{Q}$ if for all $\epsilon \in \mathbb{Q}$ such that $\epsilon > 0$, there exists $N \in \mathbb{N}$ so that for all $n \geq N$,

$$d(a_n, a) < \epsilon.$$

Similarly, the sequence (a_n) is **Cauchy** if for all $\epsilon \in \mathbb{Q}$ with $\epsilon > 0$, there exists $N \in \mathbb{N}$ such that for all $n, m \geq N$ we have

$$d(a_n, a_m) < \epsilon.$$

Let \mathcal{C} denote the set of Cauchy sequences in \mathbb{Q} .

12.3.2

Definition

For $(a_n), (b_n) \in \mathcal{C}$, define $(a_n) \sim (b_n)$ if and only if for all $\epsilon \in \mathbb{Q}$ with $\epsilon > 0$ there exists $N \in \mathbb{N}$ with

$$d(a_n, b_m) < \epsilon$$

for all $n, m \geq N$.

As before \sim is an equivalence relation. Let \mathbb{R} be the set of equivalence classes. For $a \in \mathbb{Q}$, we let $\bar{a} = (a)$ be the constant sequence and \hat{a} its equivalence class in \mathbb{R} .

12.3.3

Exercise

Suppose that $(a_n), (b_n) \in \mathcal{C}$. Then the sequence $(d(a_n, b_n)) \in \mathcal{C}$. Furthermore, if $(a_n) \sim (a'_n)$ and $(b_n) \sim (b'_n)$ then $(d(a_n, b_n)) \sim (d(a'_n, b'_n))$.

12.3.4

Definition

Suppose that $[(a_n)], [(b_n)] \in \mathbb{R}$. Define $\hat{d}([(a_n)], [(b_n)])$ to be the equivalence class of the sequence $(d(a_n, b_n))$.

At this point for two elements a and b of \mathbb{R} , we can calculate another element $\hat{d}(a, b)$ of \mathbb{R} . Clearly, this will be our distance. Before we can consider convergence properties, we need to develop more of the algebraic structure of \mathbb{R} . We begin with its ordering.

12.3.5

Definition

Let $[(s_k)] \in \mathbb{R} = \mathcal{C}/\sim$. We say that $[(s_k)]$ is **positive** if there exists a rational number $\kappa > 0$ and $N \in \mathbb{N}$ such that for all $k \geq N$, we have $s_k > \kappa$. Similarly, we say that $[(s_k)]$ is **negative** if there exists a rational number $\kappa < 0$ and $N \in \mathbb{N}$ such that for all $k \geq N$, we have $s_k < \kappa$.

In other words, an equivalence class of Cauchy sequences of rational numbers is positive if eventually all the terms are positive and are bounded away from 0 by some rational κ .

12.3.6

Exercise

Give two distinct examples of Cauchy sequences in \mathbb{Q} which have positive equivalence classes.

Of course, we need to check that our definitions are well-defined.

12.3.7

Theorem

Suppose that $(r_k), (s_k) \in \mathcal{C}$ with $(r_k) \sim (s_k)$. Then, $[(r_k)]$ is positive (resp. negative) if and only if $[(s_k)]$ is positive (resp. negative.).

Proof. Suppose that $[(r_k)]$ is positive. By definition, there exists $\kappa > 0$ and $N_r \in \mathbb{N}$ such that for all $k \geq N_r$, we have $r_k > \kappa$. Since $(r_k) \sim (s_k)$, there exists $N \in \mathbb{N}$ such that for all $k, \ell > N$, we have $-\kappa/2 < s_\ell - r_k < \kappa/2$. Let $N_s = \max(N_r, N)$. We will show that for all $\ell \geq N_s$, we have $s_\ell > \kappa/2$. Let $\ell \geq N_s$ and choose $k \geq N_s$. We have

$$s_\ell = (s_\ell - r_k) + r_k > -\kappa/2 + \kappa = \kappa/2.$$

Thus, for all ℓ , $s_\ell > \kappa/2 > 0$. Consequently, if $[(r_k)]$ is positive, then $[(s_k)]$ is positive. Interchanging the rs and ss shows the converse.

$$\langle \text{Prove } [(r_k)] < 0 \Leftrightarrow [(s_k)] < 0 \rangle.$$

□

The next theorem shows we have a trichotomy:

12.3.8

Theorem

Suppose that $[(r_k)] \in \mathbb{R}$. Then exactly one of the following holds:

1. $[(r_k)]$ is positive.
2. $[(r_k)]$ is negative.
3. $[(r_k)] = \widehat{0}$.

If (r_k) and (s_k) are Cauchy sequences in \mathbb{Q} , we let $(r_k) \pm (s_k) = (r_k \pm s_k)$ and $(r_k) \cdot (s_k) = (r_k \cdot s_k)$. These operations make sense since addition and multiplication in \mathbb{Q} has already been defined.

12.3.9

Exercise

Show that if $(r_k), (s_k) \in \mathcal{C}$, then $(r_k) \pm (s_k) \in \mathcal{C}$ and $(r_k) \cdot (s_k) \in \mathcal{C}$.

We wish to show that these definitions preserve our notion of equivalence.

12.3.10

Theorem

Suppose that $(r_k), (r'_k), (s_k), (s'_k) \in \mathcal{C}$ and that $(r_k) \sim (r'_k)$ and $(s_k) \sim (s'_k)$, then $(r_k + s_k) \sim (r'_k + s'_k)$ and $(r_k \cdot s_k) \sim (r'_k \cdot s'_k)$.

Consequently, we may give well-defined definitions $+$, $-$, and \cdot on \mathbb{R} .

12.3.11

Definition

Suppose that $[(r_k)], [(s_k)] \in \mathbb{R}$. Define:

- $[(r_k)] \pm [(s_k)] = [(r_k \pm s_k)]$.
- $[(r_k)] \cdot [(s_k)] = [(r_k \cdot s_k)]$.

12.3.12

Exercise

Show that the operations $+$ and \cdot on \mathbb{R} satisfy the usual commutative, associative, and distributive properties. Also show that for all $[(s_k)] \in \mathbb{R}$,

- $[(s_k)] + \hat{0} = [(s_k)]$
- $[(s_k)] - [(s_k)] = \hat{0}$.

12.3.13

Exercise

Define division on $\mathbb{R} \setminus \{\hat{0}\}$. Remember that a sequence other than $\bar{0}$ may still have terms that are zero and that you should never divide by them.

We may now define our ordering on \mathbb{R} .

12.3.14

Definition ▶ Ordering

For $[(r_k)], [(s_k)] \in \mathbb{R}$. Define $[(r_k)] > [(s_k)]$ if $[(s_k)] - [(r_k)]$ is positive.

12.3.15

Exercise

Explain why the definition of \leq on \mathbb{R} is well-defined.

Suppose that $r \in \mathbb{R}$. We have defined what it means for r to be positive and we now have a definition for what it means for $r > \hat{0}$. We should confirm that these definitions are equivalent.

12.3.16

Theorem

Let $r \in \mathbb{R}$. Then r is positive if and only if $r > \hat{0}$.

Proof. Suppose first that $r = [(r_k)]$ is positive. We will show that $r > \hat{0}$. By definition of “positive”, there exists a rational $\kappa > 0$ such that for large enough k , $r_k > \kappa$. Thus, for large enough k , $r_k - 0 > \kappa$. Thus, for large enough k , the k th term of the sequence $(r_k - 0) = (r_k) - \bar{0}$ is greater than κ . By definition of “positive”, the class $[(r_k)] - \hat{0}$ is positive and so, by definition $r = [(r_k)] > \hat{0}$. Now suppose that $r = [(r_k)] > \hat{0}$. By definition, this means that $r - \hat{0}$ is positive. Thus, there exists a rational $\kappa > 0$ such that for large enough k , $r_k - 0 > \kappa$. Consequently, for large enough k , $r_k > \kappa$ and this is what is required for r to be positive. \square

12.3.17

Exercise

Let $r \in \mathbb{R}$. Then r is negative if and only if $r < \hat{0}$.

12.3.18

Theorem ▶ Total Order on \mathbb{R}

For $r, s \in \mathbb{R}$ exactly one of the following holds: $r = s$, $r < s$, or $r > s$. Furthermore, if $r, s, t \in \mathbb{R}$ and $r \leq s$ and $s \leq t$, then $r \leq t$.

We can now show that \hat{d} is a metric on \mathbb{R} .

12.3.19

Theorem

The following hold:

1. For $r, s \in \mathbb{R}$, $\hat{d}(r, s) \geq \hat{0}$ with equality if and only if $r = s$.
2. For $r, s \in \mathbb{R}$, $\hat{d}(r, s) = \hat{d}(s, r)$.
3. For all $r, s, t \in \mathbb{R}$, $\hat{d}(r, t) \leq \hat{d}(r, s) + \hat{d}(s, t)$.

Proof. Let $r = [(r_k)]$ and $s = [(s_k)]$ and $t = [(t_k)]$.

Proof of (1): By definition, $\hat{d}(r, s)$ is the equivalence class of the Cauchy sequence $(d(r_k, s_k))$. For all k , $d(r_k, s_k) \geq 0$, since d is a rational-valued metric on \mathbb{Q} . Thus, there does not exist a rational $\kappa < 0$ so that for large enough k , $d(r_k, s_k) < \kappa$. Thus, the class $d(r, s) = [(d(r_k, s_k))]$ is not negative. Hence, $d(r, s) > \hat{0}$ or $d(r, s) = \hat{0}$. Suppose that $d(r, s) = \hat{0}$. This means that $(d(r_k, s_k)) \sim \hat{0}$. Hence, for all $\epsilon > 0$, there exists $N \in \mathbb{N}$ such that

$$d(r_k, s_k) = |d(r_k, s_k) - 0| < \epsilon$$

whenever k is large enough. But this is exactly what is required for $(r_k) \sim (s_k)$. Consequently, $r = [(r_k)] = [(s_k)] = s$, as desired.

Proof of (2): The real number $\hat{d}(r, s)$ is, by definition, the equivalence class of the sequence $(d(r_k, s_k))$. Likewise, $\hat{d}(s, r)$ is the equivalence class of the sequence $(d(s_k, r_k))$. Since d is a rational-valued metric on \mathbb{Q} , for all k we have $d(r_k, s_k) = d(s_k, r_k)$. Thus the sequences $(d(r_k, s_k))$ and $(d(s_k, r_k))$ are equal. Consequently, their equivalence classes are equal.

Proof of (3): For all k , we have

$$d(r_k, t_k) \leq d(r_k, s_k) + d(s_k, t_k),$$

since d is a rational-valued metric on \mathbb{Q} . Thus, the class of sequence $(d(r_k, s_k) + d(s_k, t_k) - d(r_k, t_k))$ is non-negative. Hence,

$$d(r, s) + d(s, t) - d(r, t) = [(d(r_k, s_k))] + [(d(s_k, t_k))] - [(d(r_k, t_k))] \geq \hat{0}$$

By definition, therefore,

$$d(r, t) \leq d(r, s) + d(s, t).$$

□

We can now consider convergence properties. We begin by showing that \mathbb{Q} sits inside \mathbb{R} as a dense subset.

12.3.20

Theorem

For all $q, p \in \mathbb{Q}$, we have $\widehat{d}(\widehat{q}, \widehat{p}) = \widehat{d}(q, p)$. Furthermore, suppose that $r \in \mathbb{R}$ and that $\epsilon > \widehat{0}$ is real. Then there exists $q \in \mathbb{Q}$ such that $\widehat{d}(r, \widehat{q}) < \epsilon$.

The proof is similar to what we've done before.

Proof. Let $q, p \in \mathbb{Q}$. Then $\widehat{d}(q, p)$ is the equivalence class of the constant sequence $(d(q, p))$. On the other hand, $\widehat{d}(\widehat{q}, \widehat{p})$ is the equivalence class of the sequence whose k th term is the rational distance between the k th term of the constant sequence \widehat{q} and the k th term of the constant sequence \widehat{p} . Since those sequences are constant, $\widehat{d}(\widehat{q}, \widehat{p})$ is also the equivalence class of the constant sequence $d(q, p)$. Thus, $\widehat{d}(\widehat{q}, \widehat{p}) = \widehat{d}(q, p)$.

Let $r = [(r_k)], \epsilon = [(\epsilon_k)] \in \mathbb{R}$ with $\epsilon > \widehat{0}$. By definition, there exists a rational $\kappa > 0$ such that for large enough k , $\kappa < \epsilon_k$. Thus, if we produce $q \in \mathbb{Q}$ with $\widehat{d}(r, \widehat{q}) < \widehat{\kappa}$, we will also have $\widehat{d}(r, \widehat{q}) < \epsilon$.

Since (r_k) is Cauchy, there exists $N \in \mathbb{N}$ such that for all $n, k \geq N$, we have $d(r_n, r_k) < \kappa$. Thus, for all $k \geq N$, we have $d(r_N, r_k) < \kappa$. Consequently, $\widehat{d}(\widehat{r_N}, r) < \widehat{\kappa}$, as desired. \square

Henceforth, we identify each element q of \mathbb{Q} with its image $\iota(q) \in \mathbb{R}$. In particular, we will write 0 instead of $\widehat{0}$ for the additive identity in \mathbb{R} . Note that a sequence in \mathbb{R} is a sequence of equivalence classes of sequences in \mathbb{Q} .

12.3.21

Definition ▶ Convergence/Cauchy Sequence in \mathbb{R}

A sequence $(r_k) = [(r_{k,n})_n]$ in \mathbb{R} **converges** to $r \in \mathbb{R}$ if for every real $\epsilon > \widehat{0}$, there exists $N \in \mathbb{N}$ such that for all $k \geq N$, we have

$$\widehat{d}(r_k, r) < \epsilon.$$

A sequence $(r_k) = [(r_{k,n})_n]$ in \mathbb{R} is **Cauchy** if for every real $\epsilon > \widehat{0}$, there exists $N \in \mathbb{N}$ such that for all $k, \ell \geq N$, we have

$$\widehat{d}(r_k, r_\ell) < \epsilon.$$

The proof of the next theorem is similar to what we did in the previous section when we showed that given a metric space X , the completed metric space \widehat{X} is a complete metric space.

12.3.22

Theorem ▶ \mathbb{R} is complete

If (r_k) is a Cauchy sequence in \mathbb{R} , then there exists $r \in \mathbb{R}$ such that (r_k) converges to r .

A fundamental property of \mathbb{R} is the existence of infima and suprema. We now set about showing that our construction of \mathbb{R} has these properties.

12.3.23

Definition ▶ infimum, supremum

Suppose that $S \subset \mathbb{R}$. An **upper bound** for S is an element $M \in \mathbb{R}$ such that for all $s \in S$, $s \leq M$. The number M is the **supremum** of S (and we write $M = \sup S$) if whenever $x \in \mathbb{R}$ is an upper bound for S , we have $M \leq x$.

A **lower bound** for S is an element $M \in \mathbb{R}$ such that for all $s \in S$, $s \geq m$. The number M is the **infimum** of S (and we write $M = \inf S$) if whenever $x \in \mathbb{R}$ is a lower bound for S , we have $x \leq m$.

12.3.24

Theorem

Suppose that $S \subset \mathbb{R}$ has an upper bound. Then there exists $\alpha \in \mathbb{R}$ such that $\alpha = \sup S$.

Proof. We do a proof by contradiction. Assume that whenever M is an upper bound for S , there exists another upper bound M' such that $M' < M$.

(Show that if M is an upper bound for S then $M \notin S$).

Consequently, if $x \in S$, then there exists $x' \in S$, with $x < x'$. We now construct two sequences (M_k) and (x_k) recursively. Choose $x_0 \in S$ and M_0 an upper bound for S . Recall that $x_0 < M_0$. Assume, therefore, that we have defined $M_0 \geq \dots \geq M_k$ and $x_0 \leq \dots \leq x_k$ with each M_i an upper bound for S and each $x_i \in S$. Also assume that one of the following holds for each $i > 0$:

- $M_i = (M_{i-1} + x_{i-1})/2$ and $x_i = x_{i-1}$.
- $x_i > (M_{i-1} + x_{i-1})/2$ and $M_i = M_{i-1}$.

Let $\alpha = (M_k + x_k)/2$. Observe that $x_k < \alpha < M_k$. If α is an upper bound for S , let $M_{k+1} = \alpha$ and $x_{k+1} = x_k$. Otherwise, there exists $x_{k+1} \in S$ such that $\alpha \leq x_{k+1}$ and let $M_{k+1} = M_k$. By induction we have sequences (x_k) and (M_k) .

Notice that for all $k \in \mathbb{N}$, $\widehat{d}(M_k, x_k) \leq \frac{1}{2^k} \widehat{d}(M_0, x_0)$ and if $\ell \geq k$, then $\widehat{d}(M_\ell, x_\ell) \leq \widehat{d}(M_\ell, x_k)$.

Claim: (M_k) is a Cauchy sequence in \mathbb{R} .

Let $\epsilon > 0$. For $k, \ell \in \mathbb{N}$ with $\ell \geq k$, we have

$$\begin{aligned} \widehat{d}(M_k, M_\ell) &\leq \widehat{d}(M_k, x_k) + \widehat{d}(M_\ell, x_k) \\ &\leq \widehat{d}(M_k, x_k) + \widehat{d}(M_\ell, x_\ell) \\ &\leq (\frac{1}{2^k} + \frac{1}{2^\ell}) \widehat{d}(M_0, x_0) \\ &\leq \frac{1}{2^{k-1}} \widehat{d}(M_0, x_0) \end{aligned}$$

Since the sequence $\left(\frac{1}{2^{k-1}}\right)$ in \mathbb{Q} converges to $0 \in \mathbb{Q}$, the corresponding sequence in \mathbb{R} converges to $\widehat{0}$. In particular, for k large enough, we will have

$$\frac{1}{2^{k-1}} \widehat{d}(M_0, x_0) < \epsilon.$$

Thus, (M_k) is Cauchy.

Claim: For all $\epsilon > 0$, there exists $N \in \mathbb{N}$ such that for all $k, \ell \geq N$, we have $\hat{d}(x_k, M_\ell) < \epsilon$.

⟨ Prove the Claim ⟩

Since \mathbb{R} is complete, the sequence (M_k) converges to some α .

Claim: The sequence (x_k) converges to α .

⟨ Prove the Claim ⟩

Claim: α is an upper bound for S .

Let $x \in S$. We must show that $x \leq \alpha$. Suppose, for a contradiction that $x > \alpha$. Let $\epsilon = \hat{d}(x, \alpha) > 0$. By the definition of converge, there exists $k \in \mathbb{N}$ such that $\hat{d}(M_k, \alpha) < \epsilon$. Thus, $M_k < x$. But this contradicts the fact that M_k is an upper bound for S .

Claim: $\alpha = \sup S$.

Let $M < \alpha$. Let $\epsilon = \hat{d}(M, \alpha)$. By the definition of converge, there exists $k \in \mathbb{N}$ such that $\hat{d}(x_k, \alpha) < \epsilon$. Hence, $M < x_k < \alpha$. But this means that M is not an upper bound for S . Consequently, for all upper bounds M of S , we have $\alpha \leq M$ and so $\alpha = \sup S$. \square

12.3.25

Exercise

Prove that if $S \subset \mathbb{R}$ has a lower bound, then there exists $\inf S \in \mathbb{R}$.

Remark 12.3.1. We have outlined how to use the standard metric on \mathbb{Q} to construct \mathbb{R} via completing Cauchy sequences. To complete the project we should show that \mathbb{R} satisfies all of the axioms of a “totally ordered field”. Also, there are other ways (most notably “Dedekind cuts”) of constructing \mathbb{R} from \mathbb{Q} . It would be nice to know that any two such ways of constructing \mathbb{R} give essentially the same theory. This can be done, but we will not embark on that project here.

Be cheerful, our revels now are ended.

Axioms

In this chapter, we collect many of the axioms that are used throughout the text. Do not worry about understanding them until you have encountered them in the main body of the text.

Group

A set G , together with an element $\mathbb{1} \in G$ (called the **identity** of the group), and a way (denoted \circ) of combining elements of the set, is a **group** if the following hold:

(G1) (closure) For every $a \in G$ and $b \in G$ there is a some element $c \in G$ such that $c = a \circ b$. Furthermore, this combination is unique. In other words, if $a = a'$ and $b = b'$, then:

$$a \circ b = a' \circ b'.$$

(G2) (identity) The following hold:

- For every $a \in G$, $a \circ \mathbb{1} = a$.
- For every $a \in G$, $\mathbb{1} \circ a = a$.

(G3) (inverses) For every $a \in G$ there exists $b \in G$ (more traditionally denoted a^{-1}) such that the following hold:

- For every $a \in G$, $a \circ b = \mathbb{1}$.
- For every $a \in G$, $b \circ a = \mathbb{1}$.

(G4) (associativity) For every $a, b, c \in G$

$$(a \circ b) \circ c = a \circ (b \circ c).$$

Metric Space

A set X is a **metric space** with **metric** d if the following hold:

(M1) (positive) For every $x, y \in X$, there exists a unique real number $d(x, y) \in \mathbb{R}$ with $d(x, y) \geq 0$.

(M2) (definite) For every $x, y \in X$, $d(x, y) = 0$ if and only if $x = y$.

(M3) (symmetry) For every $x, y \in X$, $d(x, y) = d(y, x)$.

(M4) (triangle inequality) For every $x, y, z \in X$,

$$d(x, z) \leq d(x, y) + d(y, z).$$

Natural Number System

Suppose that N is a set, that $\mathbf{0} \in N$ is a particular element (called the **initial object**), and that S is a successor function on N . A subset $A \subset N$ is a **counting subset** if for every $n \in A$, $S(n) \in A$. We say that the triple $(N, \mathbf{0}, S)$ is a **natural number system** if the following axioms are satisfied:

- (P1) The initial object $\mathbf{0}$ does not have a predecessor. That is, there does not exist $n \in N$ such that $S(n) = \mathbf{0}$.
- (P2) No element has more than one predecessor. That is, for every $n, m \in N$, if $S(m) = S(n)$ then $m = n$.
- (P3) If $A \subset N$ is a counting subset such that $\mathbf{0} \in A$, then $A = N$.

The function S is called a **successor function** for \mathbb{N} . The axioms are called **Peano's Axioms**.

Event Space

Let X be a set. An **event space** on X is a subset $\mathcal{E} \subset \mathcal{P}(X)$ such that the following hold:

- (E1) $\emptyset \in \mathcal{E}$
- (E2) If $A \in \mathcal{E}$ then $A^c \in \mathcal{E}$
- (E3) If $A_i \in \mathcal{E}$ for all $i \in \mathbb{N}$, then $\bigcup_{i \in \mathbb{N}} A_i \in \mathcal{E}$.

Elements of \mathcal{E} are called **events**.

A function $P: \mathcal{E} \rightarrow [0, 1]$ is a **probability function** if the following hold:

1. $P(\emptyset) = 0$. (“The probability of nothing happening is zero.”)
2. $P(X) = 1$. (“The probability of something happening is one.”)
3. If E_i is an event for all $i \in \mathbb{N}$ and if for all $i, j \in \mathbb{N}$ with $i \neq j$, we have $E_i \cap E_j = \emptyset$, then

$$P\left(\bigcup_{i \in \mathbb{N}} E_i\right) = \sum_{i=1}^{\infty} P(E_i).$$

A triple (X, \mathcal{E}, P) where X is a set, \mathcal{E} is an event space, and P is a probability function is said to be a **probability space**.

Set Theory

These are some of the ZFC axioms for set theory; some of them are imprecisely stated and not all of them are traditionally included as axioms.

1. (Extensionality) If X and Y are sets such that $X \subset Y$ and $Y \subset X$, then $X = Y$.
2. (Existence) There exists a set.
3. (Subset Selection) Let X be a set and let $P(a)$ be a predicate in one free variable. Then there is a set

$$Y = \{a \in X : P(a)\}$$

4. (Power Sets) If X is a set then there is a set $\mathcal{P}(X)$ such that $A \in \mathcal{P}(X)$ if and only if $A \subset X$.
5. (Unions) Suppose that \mathcal{H} is a set. Then there exists a set $\bigcup_{H \in \mathcal{H}} H$ such that $x \in \bigcup_{H \in \mathcal{H}} H$ if and only if there exists $H \in \mathcal{H}$ such that $x \in H$.
6. (Replacement) Suppose that $P(a, b)$ is a predicate in two variables and that Λ is a set. Suppose that for each $\lambda \in \Lambda$, there is a unique set A_λ , such that $P(\lambda, A_\lambda)$ is true. Then $\{A_\lambda : \lambda \in \Lambda\}$ is a set.
7. (Infinity) There is a set N such that $\emptyset \in N$ and for all $A \in N$, we have that $S(A) = A \cup \{A\}$ is a set and $S(A) \in N$.
8. (Foundation) If X is a non-empty set then there is an $A \in X$ such that $A \cap X = \emptyset$.
9. (Choice) Suppose that \mathcal{H} is a non-empty set such that $\emptyset \notin \mathcal{H}$. Then for each $U \in \mathcal{H}$, there exists $a_U \in U$ such that $A = \{a_U : U \in \mathcal{H}\}$ is a set.

A summary of proof techniques

PROOF OF EXISTENCE

To show: There exists a satisfying property P .

Structure of Proof: Let $a = \dots$

(State exactly what a is.)

We now show that a has property P .

(Do work to show that a has the required property P)

PROOF OF UNIQUENESS (VERSION 1)

To show: There exists a unique element of a set X with a particular property P .

Structure of Proof: First we show that such an element exists. Define $x \in X$ by:

(Explain how to define x)

Next we verify that x has property P :

(Show that x has property P)

Hence, there exists an element of X with property P .

Now we prove uniqueness. Assume that $y \in X$ and $z \in X$ both have property P .

(Show that $y = z$.)

Alternatively, we could simply show that if $y \in X$ has property P , then $y = x$, where x is the element we previously verified had property P . □

PROOF OF UNIQUENESS (VERSION 2)

To show: The object a is the unique object satisfying property P .

Structure of Proof: First, we show that a has property P .

(Do work to show that a has property P)

Now we show that a is unique. We do a proof by contradiction. Suppose that a satisfies property P , but is not unique. Then there exists $b \neq a$ also satisfying property P .

(Do work to encounter a contradiction.)

Since we have encountered a contradiction, if a satisfies property P , then it is the unique object satisfying property P .

ELEMENT ARGUMENT VERSION 1

To show: Every element x of a set X has a particular property.

Structure of Proof:

Assume $x \in X$ is arbitrary.

(Do a bunch of work to show x has the desired property.)

Hence, x has the desired property. Since x was arbitrary, every element of X has the desired property. \square

ELEMENT ARGUMENT VERSION 2

To show: $X \subset Y$

Structure of Proof:

Assume $x \in X$ is arbitrary.

(Do a bunch of work.)

Hence, $x \in Y$. Since $x \in X$ was arbitrary, $X \subset Y$. \square

PROVING SET EQUALITY

To show: $A = B$ where A and B are sets.

Structure of Proof:

Claim 1: $A \subset B$.

Assume $a \in A$. We will show $a \in B$.

(Do it!)

Claim 2: $B \subset A$.

Assume $b \in B$. We will show $b \in A$.

(Do it!)

Since $A \subset B$ and $B \subset A$, we have shown $A = B$.

DIRECT PROOF OF AN IMPLICATION

To show: $P \Rightarrow Q$ **Structure of Proof:**

We assume P and we will show that Q holds.

(Sequence of tightly reasoned statements, each following from what has already been done. At some point, possibly at the beginning, possibly later on, the assumption that P is true is used. Usually at the end we encounter a statement which shows us, without any additional work that Q is true.)

Thus, Q is true. \square .

PROOF BY CONTRADICTION

To show: P is true.**Structure of Proof:** We prove the statement by contradiction and so assume that P is false.

(Sequence of tightly reasoned statements, each following from what has already been done and concluding with a contradiction.)

Since we have encountered a contradiction, P cannot be false. Hence, P is true.

PROOF BY CONTRAPOSITION

To show: $P \Rightarrow Q$ **Structure of Proof:** We prove the statement by contraposition. We assume that Q is false and will show that P is also false.

(Sequence of tightly reasoned statements, each following from what has already been done.)

Thus, P is false. Since we have shown that $\neg Q \Rightarrow \neg P$, it must be the case that $P \Rightarrow Q$.

PROOF BY INDUCTION

To show: $P(n)$ is true for all integers $n \geq n_0$.**Structure of Proof:** We do a proof by induction on n .**Base Case:** Let $n = n_0$.

(Prove that the statement is true when $n = n_0$.)

Inductive Step: Assume that $P(k)$ is true. We will show that $P(k + 1)$ is true.

(Rephrase $P(k + 1)$ as a statement about k . Use the inductive hypothesis (emphasizing where you do so) for $P(k)$ and then do some work to show that $P(k + 1)$ is true.)

Since we have shown both the Base Case and the Inductive Step, mathematical induction implies that $P(n)$ is true for all n . \square

PROOF BY COMPLETE INDUCTION

To show: $P(n)$ is true for all $n \in \mathbb{N}$.

Structure of Proof: We do a proof by complete induction on n .

Base Case: Let $n = 1$.

(Prove that the statement is true when $n = 1$.)

Inductive Step: Assume that there is some $k \in \mathbb{N}$ such that for all $j \in \mathbb{N}$ with $1 \leq j \leq k$, the statement $P(j)$ is true. We will show that $P(k + 1)$ is true.

(Rephrase $P(k + 1)$ as a statement about j for some $j \in \{1, \dots, k\}$. Use the inductive hypothesis (emphasizing where you do so) for $P(j)$ and then do some work to show that $P(k + 1)$ is true.)

Since we have shown both the Base Case and the Inductive Step, mathematical induction implies that $P(n)$ is true for all n . □

PROOF USING THE WELL-ORDERING PRINCIPLE

To show: There exists $a \in \mathbb{N}^*$ such that properties $P(a)$ and $Q(a)$ hold for a .

Structure of Proof: Let $S = \{n \in \mathbb{N}^* : P(n) \text{ is true}\}$.

(Prove that $S \neq \emptyset$.)

Since $S \neq \emptyset$, by the Well-Ordering Principle, S has a least element a .

(Prove that $Q(a)$ is true using the fact that a is the least element of S .)

□

PROOF BY MINIMAL COUNTEREXAMPLE

To show: A statement $P(s)$ is true for all elements s of some set S .

Structure of Proof: Assume that the theorem is false. That is, assume that there exists some $s \in S$ so that $P(s)$ is false. We will show that we encounter a contradiction.

(Define some function $c: S \rightarrow \mathbb{N}$ which measures the complexity of the elements of S)

Out of all elements of S which are counter-examples to the theorem, choose one s_0 for which $c(s_0)$ is as small as possible.

(Find a contradiction by either showing how to create a counter-example with strictly small complexity or by using the fact that if $s \in S$ has $c(s) < c(s_0)$ then s is not a counter-example.)

Thus, we encounter a contradiction and so $P(n)$ is true for all $n \in \mathbb{N}$. □

DEFINING A SEQUENCE RECURSIVELY

To define: a sequence (x_n) in a non-empty set X so that $x_1 \in X$ and so that (x_n) has a property P .

Structure of Proof: We define (x_n) recursively. Choose some $x_1 \in X$. Assume that we have defined $x_k \in X$ for all $k \in \{1, \dots, n\}$ in such a way that we haven't yet contradicted the possibility of the final sequence having property P . We now define x_{n+1} .

⟨Define $x_{n+1} \in X$ in terms of x_1, \dots, x_n .⟩

By induction (but see the remark below) we have a sequence (x_n) in X .

⟨Verify that f satisfies P .⟩

CONSTRUCTION OF A FUNCTION

To construct: A function $f: X \rightarrow Y$.

Structure of Proof: For each $x \in X$, define

$f(x) = \langle$ formula or description saying what $f(x)$ is \rangle

To verify that $f: X \rightarrow Y$ is a function we show:

1. (domain condition) That $f(x)$ exists and that $f(x) \in Y$ for every $x \in X$.
2. (well-defined condition) That, for all $a, b \in X$, if $a = b$, then $f(a) = f(b)$.

⟨Prove all of the previous statements unless completely obvious.⟩

PROVING INJECTIVITY

To show: $f: X \rightarrow Y$ is injective.

Structure of Proof: Assume $a, b \in X$ and that $f(a) = f(b)$. We will show that $a = b$.

⟨Apply the definition of f and then do work.⟩

Thus, $a = b$. Since this is true for all $a, b \in X$, the function f is injective. □

PROVING SURJECTIVITY

To show: $f: X \rightarrow Y$ is surjective.

Structure of Proof: Assume $y \in Y$. We will show that there exists $x \in X$ such that $f(x) = y$.

⟨ Define a particular $x \in X$ ⟩

⟨ Show $f(x) = y$ ⟩

Thus, f is surjective. □

Typography

Mathematics draws on a wide range of alphabets to encapsulate various concepts. Here we list some of the more common ones.

Symbol	Name	Alphabet/Font	L ^A T _E X
α	lower-case alpha	Greek	\alpha
β	lower-case beta	Greek	\beta
γ, Γ	lower-case, upper-case gamma	Greek	\gamma, \Gamma
δ, Δ	lower-case, upper-case delta	Greek	\delta, \Delta
ϵ	lower-case epsilon	Greek	\epsilon
ζ	lower-case zeta	Greek	\zeta
η	lower-case eta (“ay-tah”)	Greek	\eta
θ, Θ	lower-case, upper-case theta	Greek	\theta, \Theta
κ	lower-case kappa	Greek	\kappa
λ, Λ	lower-case, upper-case lambda	Greek	\lambda, \Lambda
μ	lower-case mu	Greek	\mu
ν	lower-case nu	Greek	\nu
ξ, Ξ	lower-case, upper-case xi (“ek-see”)	Greek	\xi, \Xi
π, Π	lower-case, upper-case pi	Greek	\pi, \Pi
ρ	lower-case rho	Greek	\rho
σ, Σ	lower-case, upper-case sigma	Greek	\sigma, \Sigma
τ	lower-case tau	Greek	\tau
ϕ, Φ	lower-case, upper-case phi (“fee”)	Greek	\phi, \Phi
χ	lower-case chi (“k-eye”)	Greek	\chi
ψ, Ψ	lower-case, upper-case psi (“p-see”)	Greek	\psi, \Psi
ω, Ω	lower-case, upper-case omega	Greek	\omega, \Omega
\aleph	Aleph	Hebrew	\aleph
\mathcal{A}	script “A”	caligraphic	\mathcal{A}
\mathbb{R}	blackboard bold “R”	blackboard bold	\mathbb{R}
a, b, etc.	fraktur “a”, “b”, etc.	fraktur	\mathfrak{a}, \mathfrak{b}

Bibliography

- [1] *Who came up with the arrow notation?*, Mathematics StackExchange, available at <http://math.stackexchange.com/questions/144821/who-came-up-with-the-arrow-notation-x-rightarrow-y>.
- [2] *What would remain of current mathematics without the power set?*, available at <http://mathoverflow.net/questions/133597/what-would-remain-of-current-mathematics-without-axiom-of-power-set>.
- [3] *Maine Question 1, Ranked-Choice Voting Delayed Enactment and Automatic Repeal Referendum (June 2018)*, Ballotpedia, available at [https://ballotpedia.org/Maine_Question_1,_Ranked-Choice_Voting_Delayed_Enactment_and_Automatic_Repeal_Referendum_\(June_2018\)](https://ballotpedia.org/Maine_Question_1,_Ranked-Choice_Voting_Delayed_Enactment_and_Automatic_Repeal_Referendum_(June_2018)).
- [4] Martin Aigner and Günter M. Ziegler, *Proofs from The Book*, 5th ed., Springer-Verlag, Berlin, 2014. Including illustrations by Karl H. Hofmann. MR3288091
- [5] Aeschylus (David Grene and Richmond Lattimore, eds.), translated by David Grene, University of Chicago Press.
- [6] Laura Alcock, Mark Hodds, Somali Roy, and Matthew Inglis, *Investigating and improving undergraduate proof comprehension*, Notices of the American Mathematical Society **62** (2015).
- [7] Augustine, *City of God*, translated by Marcus Dods.
- [8] ———, *On Free Will*, 1974.
- [9] John Baez, *The inconsistency of arithmetic*, available at https://golem.ph.utexas.edu/category/2011/09/the_inconsistency_of_arithmeti.html.
- [10] *Fallacies, flaws, and flimflams*, The College Mathematics Journal **28** (1997), no. 4, 264–269.
- [11] Charles Babbage, *On the influence of signs in mathematical reasoning*, Transactions of the Cambridge Philosophical Society **2** (1827), no. 2, 325–377.
- [12] Michael Bader, *Space-filling curves*, Texts in Computational Science and Engineering, vol. 9, Springer, Heidelberg, 2013. An introduction with applications in scientific computing. MR2985717
- [13] John L Bell, *The Axiom of Choice*.
- [14] Dave Benson, *Music: a mathematical offering*, Cambridge University Press, Cambridge, 2007. MR2283500
- [15] Jo Boaler, *What's Math Got to Do With It? How teachers and parents can transform mathematics learning and inspire success*, Penguin Books, 2015.
- [16] R. P. Boas, *Can We Make Mathematics Intelligible?*, Amer. Math. Monthly **88** (1981), no. 10, 727–731, DOI 10.2307/2321471. MR1539821
- [17] Imre Bokor, Diarmuid Crowley, Stefan Friedl, Fabian Hebestreit, Daniel Kasprowski, Markus Land, and Johnny Nicholson, *Connected sum decompositions of high-dimensional manifolds* (2019), available at <arxiv:1909.02628>.
- [18] Anthony Bonato, *The Intrepid Mathematician*, 2019.
- [19] George Boole, *Selected manuscripts on logic and its philosophy*, Science Networks. Historical Studies, vol. 20, Birkhäuser Verlag, Basel, 1997. Edited and with an introduction by Ivor Grattan-Guinness and Gérard Bornet. MR1451370
- [20] Lawrence Brenton and Thomas G. Edwards, *Sets of sets: a cognitive obstacle*, College Math. J. **34** (2003), no. 4, 31–38.
- [21] Jorge Luis Borges, *Collected Fictions*, translated by Andrew Hurley, Penguin, 1999.
- [22] William Byers, *How mathematicians think*, Princeton University Press, Princeton, NJ, 2007. Using ambiguity, contradiction, and paradox to create mathematics. MR2311817
- [23] Italo Calvino, *Invisible Cities*, translated by William Weaver, Harcourt Brace, 1974.

- [24] Bonnie Jo Campbell.
- [25] Gunnar Carlsson, *Topology and data*, Bull. Amer. Math. Soc. (N.S.) **46** (2009), no. 2, 255–308, DOI 10.1090/S0273-0979-09-01249-X. MR2476414
- [26] Jean Chrétien, *Chrétien: A proof is a proof*.
- [27] Agatha Christie, *The Murder on the Links*, The Bodley Head, 1923.
- [28] Marcus Tullius Cicero, *On the Good Life*, translated by Michael Grant, Penguin Classics, 1971.
- [29] Pete L. Clark, *The instructor's guide to real induction*, Math. Mag. **92** (2019), no. 2, 136–150, DOI 10.1080/0025570X.2019.1549902. MR3929271
- [30] Mariana Cook, *Mathematicians: an outer view of the inner world*, American Mathematical Society, Providence, RI, 2018. Portraits by Mariana Cook; With an introduction by Robert Clifford Gunning and an afterword by Brandon Fradd; Corrected reprint of [MR2542778]. MR3837509
- [31] Leo Corry, *The development of the idea of proof*, The Princeton Companion to Mathematics, 2008, pp. 129–142.
- [32] Richard Courant and Herbert Robbins, *What is mathematics?* (Ian Stewart, ed.), Oxford University Press, New York, 1996. An elementary approach to ideas and methods.
- [33] Joseph W. Dauben, *Georg Cantor and Pope Leo XIII: Mathematics, Theology, and the Infinite*, Journal of the History of Ideas **38** (Jan.), no. 1, 85–108.
- [34] Michael M. DeMers, *GIS for Dummies*, Wiley Publishing, Inc., 2009.
- [35] Revital Dafner, Daniel Cohen-Or, and Yossi Matias, Eurographics '2000 **19** (2000), no. 3.
- [36] Philip J. Davis and Reuben Hersh, *The mathematical experience*, Birkhäuser, Boston, Mass., 1980. With an introduction by Gian-Carlo Rota. MR601591
- [37] *On the Syllogism, No. III, and on Logic in general*, Trans. Cam. Phil. Soc. **10** (1863), no. 1, 173.
- [38] Keith J. Devlin, *Fundamentals of contemporary set theory*, Springer-Verlag, New York-Heidelberg, 1979. Universitext. MR541746 (80j:04001)
- [39] Keith Devlin, *The joy of sets*, 2nd ed., Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1993. Fundamentals of contemporary set theory. MR1237397
- [40] Peter Doyle and J.H. Conway, *Division by Three*, available at <http://arxiv.org/pdf/math/0605779.pdf>.
- [41] H.-D. Ebbinghaus, H. Hermes, F. Hirzebruch, M. Koecher, K. Mainzer, J. Neukirch, A. Prestel, and R. Remmert, *Numbers*, Graduate Texts in Mathematics, vol. 123, Springer-Verlag, New York, 1991. With an introduction by K. Lamotke; Translated from the second 1988 German edition by H. L. S. Orde; Translation edited and with a preface by J. H. Ewing; Readings in Mathematics. MR1415833
- [42] T.S. Eliot, *Four Quartets* (1971).
- [43] Jordan S. Ellenberg and Dion Gijswijt, *On large subsets of \mathbb{F}_1^n with no three-term arithmetic progression*, available at [arxiv/1605.09223](https://arxiv.org/abs/1605.09223).
- [44] Susanna S. Epp, *The role of logic in teaching proof*, Amer. Math. Monthly **110** (2003), no. 10, 886–899.
- [45] Leonhard Euler, *Solutio problematis ad geometriam situs pertinentis* (1735), available at <http://eulerarchive.maa.org>.
- [46] José Ferreirós, *the crisis in the foundations of mathematics*, The Princeton Companion to Mathematics, 2008, pp. 142 – 156.
- [47] ———, *Labyrinth of thought*, 2nd ed., Birkhäuser Verlag, Basel, 2007. A history of set theory and its role in modern mathematics. MR2348484
- [48] William Flesch, *Set theory for poets/Poetry for set theorists*, Arcade (2019).
- [49] Michael Frayn, *Copenhagen*, Anchor Books, 1998.
- [50] Galileo Galilei, *Two New Sciences*, translated by Stillman Drake, Wall & Thompson, 1989.
- [51] Martin Gardner, *Mathematical carnival*, 2nd ed., Mathematical Association of America, Washington, DC, 1989. With a foreword by John Conway. MR1007833
- [52] Darren Glass, *Reviews*, The American Mathematical Monthly **127** (2020), no. 2, 189–192, DOI 10.1080/00029890.2020.1685835.
- [53] Daniel Henry Gottlieb, *All the way with Gauss-Bonnet and the sociology of mathematics*, Amer. Math. Monthly **103** (1996), no. 6, 457–469, DOI 10.2307/2974712. MR1390575

- [54] Loren Graham and Jean-Michel Kantor, *Naming infinity*, The Belknap Press of Harvard University Press, Cambridge, MA, 2009. A true story of religious mysticism and mathematical creativity. MR2526973
- [55] Jeremy Gray, *Plato's ghost*, Princeton University Press, Princeton, NJ, 2008. The modernist transformation of mathematics. MR2452344
- [56] Fernando Q. Gouv  a, *p-adic numbers*, 2nd ed., Universitext, Springer-Verlag, Berlin, 1997. An introduction. MR1488696
- [57] ———, *Was Cantor surprised?*, Amer. Math. Monthly **118** (2011), no. 3, 198–209. MR2800330
- [58] Barbara Guest, *Words*, Selected Poems (1995), 1995.
- [59] JoAnn Growney, *Intersections – Poetry with Mathematics*.
- [60] P.R. Halmos, *How to write mathematics*, L'Enseignement Math  matique **16** (1970).
- [61] Richard Hammack, *Book of Proof*, Creative Commons.
- [62] Lorna B. Hanes, *Mathematics in Literature*, Bridges 2003 (Granada, Spain, 2003), Meeting Alhambra, ISAMA-BRIDGES Conference Proceedings (Nathaniel Friedman Javier Barrallo Juan Antonio Maldonado, ed.), University of Granada, pp. 109–118, available at <http://archive.bridgesmathart.org/2003/bridges2003-109.html>.
- [63] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 5th ed., The Clarendon Press, Oxford University Press, New York, 1979. MR568909
- [64] Kevin Hartnett, *A mathematician whose only constant is change*, Quanta Magazine (June 13, 2019).
- [65] Brian Hayes, *Crinkly Curves*, American Scientist **101** (June, 2013 May), no. 3, DOI doi.org/10.1511/2013.102.178.
- [66] Michael Heller and W. Hugh Woodin (eds.), *Infinity*, Cambridge University Press, Cambridge, 2011. New research frontiers. MR2850464
- [67] Linda Dalrymple Henderson, *The fourth dimension and non-Euclidean geometry in modern art*, MIT Press, Cambridge, MA, 2013. Revised edition of the 1983 original. MR3026954
- [68] Allison K Henrich, Emille D Lawrence, Matthew A Pons, and David G Taylor (eds.), *Living Proof: Stories of Resilience Along the Mathematical Journey*, American Mathematical Society: Mathematical Association of America, 2019.
- [69] Douglas Hofstadter, *G  del, Escher, Bach: an eternal golden braid*, Basic Books, 1999.
- [70] Joshua Holden, *The mathematics of secrets*, Princeton University Press, Princeton, NJ, 2017. Cryptography from Caesar ciphers to digital encryption. MR3587713
- [71] Susan Holmes, *Statistical proof? The problem of irreproducibility*, Bull. Amer. Math. Soc. **55** (2018), 31–55.
- [72] Kevin Houston, *How to think like a mathematician: A companion to undergraduate mathematics*, Cambridge University Press, 2009.
- [73] Karel Hrbacek and Thomas Jech, *Introduction to set theory*, 3rd ed., Monographs and Textbooks in Pure and Applied Mathematics, vol. 220, Marcel Dekker, Inc., New York, 1999. MR1697766
- [74] Marjorie Hunt and Paul Wagner, *Good Work: Masters of the Building Arts*, Smithsonian Center for Folklife and Cultural Heritage and American Focus, Inc., 2016. Video produced by PBS.
- [75] Eug  ne Ionesco, translated by Derek Prouse, Grove Press, New York, 1960.
- [76] Allyn Jackson, *AMS President Robert Bryant: His early life and his views on mathematics*, Notices of the AMS **63** (June 2016), no. 6.
- [77] Jesse Johnson, *The Shape of Data* (2019).
- [78] Jay Jorgenson and Steve G. Krantz, *Serge Lang, 1927–2005*, Notices Amer. Math. Soc. **53** (2006), no. 5, 536–553. MR2254400
- [79] David Joyner, *Adventures in group theory*, 2nd ed., Johns Hopkins University Press, Baltimore, MD, 2008. Rubik's cube, Merlin's machine, and other mathematical toys. MR2599606
- [80] R. Kannan, A. K. Lenstra, and L. Lov  sz, *Polynomial factorization and nonrandomness of bits of algebraic and some transcendental numbers*, Math. Comp. **50** (1988), no. 181, 235–250, DOI 10.2307/2007927. MR917831
- [81] Erica Klarreich, *Simple Set Game Proof Stuns Mathematicians*, Quanta Magazine (May 31, 2016), available at <https://www.quantamagazine.org/20160531-set-proof-stuns-mathematicians/>.
- [82] Gina Kolata, *What does it mean to be random?*, Science **231** (March 7, 1986), 1068–1070.
- [83] Erica Klarreich, *Sphere packing solved in higher dimensions*, Quanta Magazine (March 30, 2016), available at <https://www.quantamagazine.org/20160330-sphere-packing-solved-in-higher-dimensions/>.
- [84] F. William Lawvere and Robert Rosebrugh, *Sets for mathematics*, Cambridge University Press, Cambridge, 2003. MR1965482

- [85] Tom Leinster, *Rethinking set theory*, Amer. Math. Monthly **121** (2014), no. 5, 403–415, DOI 10.4169/amer.math.monthly.121.05.403. MR3193723
- [86] Thomas Lux, *The Cradle Place*, Houghton Mifflin Harcourt, 2004.
- [87] Kevin M. Lynch and Frank C. Park, Cambridge University Press, 2017.
- [88] Saunders MacLane, *Categories for the working mathematician*, Springer-Verlag, New York-Berlin, 1971. Graduate Texts in Mathematics, Vol. 5. MR0354798
- [89] Gabriel García Márquez, *One Hundred Years of Solitude*, Avon Books, 1971.
- [90] Sophia D. Merow, *A Pivotal Moment: A Conversation with Moon Duchin*, Math Horizons **XXV** (Nov. 2017), 7.
- [91] Robert Meusel, Oliver Lehmberg, Christian Bizer, and Sebastiano Vigna, *Web Data Commons - Hyperlink Graphs* (July 9, 2018).
- [92] Jonathan K. Millen, *Gallery Layout in Borges' Library of Babel*, Bridges 2015 (Phoenix, Arizona, 2015), Proceedings of Bridges 2015: Mathematics, Music, Art, Architecture, Culture (Craig S. Kaplan Kelly Delp Douglas McKenna and Reza Sarhangi, ed.), Tessellations Publishing, pp. 359–362, available at <http://archive.bridgesmathart.org/2015/bridges2015-359.html>.
- [93] Gregory H. Moore, *Zermelo's axiom of choice*, Studies in the History of Mathematics and Physical Sciences, vol. 8, Springer-Verlag, New York, 1982. Its origins, development, and influence. MR679315
- [94] L. J. Mordell, *Book Review: Diophantine geometry*, Bull. Amer. Math. Soc. **70** (1964), no. 4, 491–498, DOI 10.1090/S0002-9904-1964-11164-2. MR1566303
- [95] William Morris, *Useful Work Versus Useless Toil*, Penguin, 2008.
- [96] Sam Northshield, *Two short proofs of the infinitude of primes*, CMJ **48** (May, 2017), 214–216.
- [97] John J O'Connor and Edmund F. Robertson, *MacTutor History of Mathematics*, University of St Andrews, Scotland.
- [98] Eugene Ostashevsky, *The Pirate Who Does Not Know the Value of Pi*, New York Books Poets, New York Review of Books, 2017.
- [99] P.K. Page, *The Figures*, 2002.
- [100] Pavel A. Pevzner, Haixu Tang, and Michael S. Waterman, *An eulerian path approach to DNA fragment assembly*, PNAS **98** (August 14, 2001).
- [101] H. Poincaré, *Science and hypothesis*, Dover Publications, Inc., New York, 1952. With a preface by J. Larmor. MR0050528
- [102] Michael Polanyi, *Personal Knowledge: Towards a post-critical philosophy*, University of Chicago Press, 1974.
- [103] Geoffrey Pullum, *Scooping the loop snooper*, available at <http://www.lel.ed.ac.uk/~gpullum/loopsnoop.html>.
- [104] Margaret A. and Taylor Readdy Christine, *Women's History Month*, Notices of the AMS **65** (2018), no. 3, 248–303.
- [105] David S. Richeson, *Euler's gem*, Princeton University Press, Princeton, NJ, 2012. The polyhedron formula and the birth of topology; First paperback printing. MR2963735
- [106] Don Michael Randel, *Harvard Concise Dictionary of Music*, Belknap Press, 1995.
- [107] Siobhan Roberts, *Her Key to Modeling Brains: Ignore the Right Details*, Quanta Magazine (June 19, 2018).
- [108] Gian-Carlo Rota, *Indiscrete thoughts*, Modern Birkhäuser Classics, Birkhäuser Boston, Inc., Boston, MA, 2008. Reprint of the 1997 edition [Birkhäuser Boston, Boston, MA; MR1419503]; With forewords by Reuben Hersh and Robert Sokolowski; Edited, with notes and an epilogue by Fabrizio Palombi. MR2374113
- [109] Felix Salmon, *Recipe for disaster: the formula that killed Wall Street*, Wired Magazine (February 23, 2009).
- [110] Carol Schumacher, *Chapter Zero*, Pearson, 2000.
- [111] Saadia, *Book of Doctrines and Beliefs*, 1974.
- [112] Hans Sagan, *Space-filling curves*, Universitext, Springer-Verlag, New York, 1994. MR1299533
- [113] A. Shen and N. K. Vereshchagin, *Basic set theory*, Student Mathematical Library, vol. 17, American Mathematical Society, Providence, RI, 2002. Translated from the 1999 Russian edition by Shen. MR1915128
- [114] Margot Lee Shetterly, *Hidden Figures: The American Dream and the Untold Story of the Black Women Mathematicians Who Helped Win the Space Race*, Harper Collins, 2016.
- [115] William Jay Smith, *Galileo Galilei*, 2004.
- [116] Ramond Smullyan, *Alice in Puzzle-land*, Penguin, 1982.

- [117] R.J. Stevens, A.F. Lehar, and F.H. Preston, *Manipulation and Presentation of Multidimensional Image Data Using the Peano Scan*, IEEE Transactions on Pattern Analysis and Machine Intelligence **5** (May, 1983), 520-526, DOI 10.1109/T-PAMI.1983.4767431.
- [118] Tom Stoppard, *Arcadia*, Faber and Faber, 1993.
- [119] Francis Edward Su, *Some guidelines for good mathematical writing*, MAA Focus **35** (August/September 2015), no. 4, 20 – 22.
- [120] ———, *Mathematics for Human Flourishing*, Princeton, 2020.
- [121] Wislawa Szymborska, *View with a Grain of Sand* (1995).
- [122] Serge Tabachnikov, *Geometry and billiards*, Student Mathematical Library, vol. 30, American Mathematical Society, Providence, RI; Mathematics Advanced Study Semesters, University Park, PA, 2005. MR2168892
- [123] John Tantalo, *Planarity*.
- [124] William P. Thurston, *On proof and progress in mathematics*, Bull. Amer. Math. Soc. (N.S.) **30** (1994), no. 2, 161–177, DOI 10.1090/S0273-0979-1994-00502-6. MR1249357 (94m:00006)
- [125] Edward R. Tufte, *Visual Explanations: Images and Quantities, Evidence and Narrative*, Graphics Press, 2012.
- [126] Elif Unlu, *Maria Gaetana Agnesi*, Biographies of Women Mathematicians (1995).
- [127] Luiz Velho and Jonas de Miranda Gomes, *Digital Halftoning with Space Filling Curves*, Computer Graphics **25** (July, 1991), no. 4.
- [128] Maryna S. Viazovska, *The sphere packing problem in dimension 8*, available at [arXiv:1603.04246](https://arxiv.org/abs/1603.04246).
- [129] Leonard M. Wapner, *The pea & the sun*, A K Peters, Ltd., Wellesley, MA, 2005. A mathematical paradox. MR2138614 (2006a:03001)
- [130] Ronald L. Wasserstein, *ASA Statement on Statistical Significance and P-Values*, The American Statistician **70** (2016), 129–133.
- [131] P.G. Wodehouse, *The Luck of the Bodkins*, The Overlook Press, 1935.
- [132] André Weil, *The apprenticeship of a mathematician*, Birkhäuser Verlag, Basel, 1992. Translated from the 1991 French original by Jennifer Gage. MR1139519
- [133] Simone Weil, *On the Abolition of All Political Parties*, translated by Simon Leys, NYRB Classics, 2014.
- [134] ———, *The Need for Roots*, translated by Arthur Wills, G.P. Putnam's Sons, 1952.
- [135] Ludwig Wittgenstein, *Wittgenstein's Lectures on the Foundations of Mathematics. Cambridge, 1939: from the notes of R.G. Bosanquet, Norman Malcolm, Rush Rhees, and Yorick Smythies* (Cora Diamond, ed.), University of Chicago Press, 1976.
- [136] Martin M. Zuckerman, *Sets and transfinite numbers*, Macmillan Publishing Co., Inc., New York; Collier Macmillan Publishers, London, 1974. MR0396266

Index

\mathbb{N}^* , 44
 σ -algebra, 137
 $\sqrt{2}$, 298
Set, card game, 81

algorithm
 division, 192, 272

and, 57

angle, 186

annulus, 122

Axiom
 choice, 157
 Foundation, 156

axiom
 choice, 240
 Kirchoff's First Law, 260

axioms
 Peano, 43, 285

ball, 398
bijective, 232
billiards, 416
bind, 56
bipartite graph, 39
Bolzano-Weierstrass theorem, 411
Borel, 138
Borges, Jorge Luis, 390

Cantor set, 147
cardinal number, 356
Cartesian product, 122
Cauchy, 403
Cauchy equivalent, 420
Cauchy property, 403
choice, 240
Choice, Axiom, 157
circle, 207, 221
circuit, Eulerian, 319
class, equivalence, 176
codomain, 202

commutative diagram, 226
comparison test, 411
complement, 109
 relative, 110
complete, 406, 411
complete graph, 39
completion, 420
composition, 225
 properties, 226
conclusion, 70
conditional
 statement, 56
conditional statement, 56
configuration space, 139, 195
congruent, 191
Conjecture
 Twin Prime, 81
conjunction, 57
connected graph, 291
constant, 215
Continuum Hypothesis, 358
contrapositive, 70, 91
converge, 398, 399
converse, 70
convex hull, 129
coordinate function, 215
countable, 337
criterion, entrance, 4
cycle, 294
cycle, permutation, 293

definition
 recursive, 301

DeMorgan's laws, 120, 135
dense, 421

diagram
 commutative, 226
 Venn, 109, 111, 116, 210

dictionary order, 198

- digraph, 40, 41
 dimension, 366
 direct proof, 89
 directed graph, 258
 disc, 398
 discrete metric, 35
 disjoint union, 124, 357
 disjunction, 57
 distance, 33
 division algorithm, 192, 272
 domain, 202
 dots and arrows, 210
 element argument, 14
 embedding, 421
 entrance criterion, 4
 equivalence class, 176, 347
 equivalence relation, 172, 347, 420
 equivalent statements, 59, 76
 Euclid, 389
 euclidean metric, 35, 133, 207
 Euler, Leonhard, 81
 event, 137
 event space, 137, 138
 extended naturals, 44
 extended real numbers, 407
 factorial, 311
 Fermat, Pierre, 81
 Fibonacci sequence, 273, 301
 finite sequence, 392
 fixed point, 346
 foundation, 156
 fractions, 298
 free variable, 56
 Frege, Gottlob, 83
 function, 163, 202
 - bijective, 232
 - constant, 215
 - coordinate, 215
 - graph, 209
 - identity, 207, 215
 - injective, 232
 - inverse, 241
 - one-to-one, 231
 - onto, 231
 - restricted, 223
 - successor, 41, 285
- surjective, 232
 function composition, 225
 graph, 125
 - bipartite, 39
 - complete, 39
 - connected, 291
 - directed, 40, 41, 258
 - path, 218
 - planar, 39, 292
- graph of a function, 209
 group, 130, 359
 - homomorphism, 243
- Halting Problem, 86
 halting problem, 87
 homomorphism, 243, 264
 hypothesis, 70
 identity, 215
 identity function, 207
 if and only if, 76
 iff, 76
 implication, 70
 index set, 17, 111
 induction
 - complete, 284
 - regular old, 268
- inductive hypothesis, 268
 inductive task, 268
 infimum, 407, 433
 infinite sequence, 392
 infinity in the humanities, 387
 initial endpoint, 258
 injective, 232
 injective sequence, 303, 393
 integers
 - constructing, 188
- interior, 135
 intermediate value theorem, 96
 intersection, 111
 interval, 13
 inverse function, 241
 irrational number, 298
 iterated function sequence, 416
 Königsberg bridges, 317
 Kirchoff's First Law, 260

- labels, 211
- Lagrange's theorem, 361
- Laws
 - DeMorgan's, 135
- laws
 - DeMorgan's, 120
- leaf, 291, 324
- lemma, 90
- length, 401
- lexicographic order, 198
- light bulbs, 211
- limit, 399
- logically equivalent, 59
- metric, 34
 - discrete, 35
 - euclidean, 35, 133, 207
- metric completion, 420
- metric space, 34, 398
 - complete, 406, 411
- mod, 191
- modular arithmetic, 191
- monotonic, 409
- multiple, 90
- natural numbers, 41
- Nelson, Edward
 - views on infinity, 389
- number
 - cardinal, 356
 - irrational, 298
 - prime, 78, 92
- numbers
 - natural, 41
- one-to-one, 231, 232
- one-to-one correspondence, 232
- onto, 231, 232
- open
 - disc, 133
 - set, 133
- or, 57
- order, lexicographic, 198
- ordered pair, 122
- pairwise disjoint, 255
- partition, 26, 167, 294, 311, 347
- path, 218
 - Eulerian, 319
- in graph, 218
- Peano axioms, 43, 285
- permutation, 276, 294
- place value, 286
- planar graph, 39
- points, 34
- polygon, 274
- polygon, convex, 274
- pool table, 416
- power set, 17, 120
- predicate, 56
- prime, 12
- prime factorization, 285
- prime number, 78, 92
- probability, 311
- Problem
 - Halting, 86
- product of sets, 122
- proof
 - by contradiction, 45
 - by contraposition, 91
 - direct, 89
- proper subset, 12
- property
 - Cauchy, 403
 - reflexive, 172
 - symmetric, 172
 - transitive, 172
- quotient set, 181, 347
- range, 202
- rational numbers
 - constructing, 188
- real numbers
 - extended, 407
- recursion, 396
- recursive definition, 301
- reflexive, 172
- relation, 171
 - equivalence, 172
- restricted function, 223
- robot, 139
- rotation, 207, 413
- rotations of a circle, 221
- Russell's Paradox, 84, 156
- Russell, Bertrand, 83
- Sayers, Dorothy L., 49

- sequence, 216, 392
 - convergent, 399
 - Fibonacci, 273, 301
 - finite, 392
 - infinite, 392
 - injective, 303, 393
 - limit, 399
 - sub-, 394
 - surjective, 393
 - total length, 401
- set
 - Cantor, 147
 - index, 17, 111
 - of functions, 164
 - open, 133
 - power, 17, 120
 - quotient, 181
 - sub-, 12, 107
 - `textbf`, 3
 - universal, non-existence of, 85
- space
 - configuration, 139, 195
 - event, 137, 138
 - metric, 34, 398
- specify, 56
- statement, 56
- subgroup, 130, 359
- subsequence, 394
- subset, 12, 107
 - proper, 12
- successor function, 41, 285
- supremum, 407, 433
- surjective, 232
- surjective sequence, 393
- symmetric, 172
- symmetry, 49
- terminal endpoint, 258
- test
 - comparison, 411
- theology, 389
- Theorem
 - Cantor-Bernstein, 367
 - Euler, 292
 - Fermat's Last, 81
 - Fermat's Little, 81
 - Russell's Paradox, 84, 156
- theorem