Mathematical Inquiry

Dylan Q. Retsek

September 18, 2023

Contents

A Note to the Student

There are few mathematical prerequisites for reading this book, it is almost entirely self contained. A certain depth and breadth of character, on the other hand, are absolutely essential.

Chief among the necessary attributes are:

1. *Passion.* If you are not passionate about your subject, if you view your education merely as a collection of hurdles to clear and grades to post, you have come to the wrong place. Without passion, the virtues that follow are a train with no engine.

2. *Generosity.* Think of this book as the itinerary for a great trek and the class as the expedition party. The trail will be hard going at times, but we will fail and succeed as a group. Prepare to give of your time, your insight, and your passion so that we all may receive.

3. *Curiosity.* Ask "Why?" and "How?" at every opportunity. Let wonder lead the way.

4. *Determination.* We will get stuck. We will flounder. Greet every doubt and every obstacle with a smile and fresh resolve. We are determined to triumph.

5. *Accountability.* You are responsible for your own education. The opportunity to solidify your mathematical future is placed here before you, commit to seizing it. Discere faciendo.

6. *Optimism.* The slate is wiped clean. Whatever your past mathematical successes and failures, focus now on the present. Believe that it is possible for one class to forever change the course of your academic and intellectual life. Believe that this is that class.

This book is an attempt to orchestrate and present conditions suitable for discovery. Discovery of new mathematical ideas, discovery of interconnections between them, and discovery of one's own mathematical voice.

Because no one can discover something for you, nearly every structural object in this text requires *action*.

Definition. Definitions are the key objects in this book. They are agreements upon the meaning of terms or phrases. The defined term or phrase is always in *emphasized* text. These agreements are inviolable and no defined term is ever used loosely. The required actions are memorization, digestion and contextualization.

Example. Examples are provided to highlight or lend interest to a new term or idea and generate discussion. Required actions are digestion and contextualization.

Exercise. Exercises are explicit actions requested of the reader, usually in order to put new terms or ideas to use, test comprehension, and generate discussion.

Proposition. Propositions are statements that may or may not be true. They depend only on definitions, propositions and theorems that have come before them in the book. The first required action is to assess whether the statement is true or false. The remaining required action depends on your assessment. If true, prove it; if false, provide a counterexample to the statement.

Theorem. Theorems are statements that are true and are valuable because of wide applicability or deep consequence. They depend only on definitions, propositions and theorems that have come before them in the book. The required action is to prove the theorem.

This book is not typical. From these pages you will get only what you give. Read with conviction and energy. Have pencil and paper at hand. Take no statement for granted and maintain a healthy skepticism.

This book contains all that you will need and nothing you won't. Do not consult other texts or the internet. In this class, earnest failure outweighs counterfeit success; you need not feel pressure to hunt for solutions outside your own creative and intellectual reserves.

This book is the open road and a full tank of gas.

This book was written for you.

San Luis Obispo, 2023

Chapter 1

The Words Matter

If you don't say it well, people won't know what you're talking about.

1.1 Wordplay

We begin with a definition.

Definition 1.1. The *length* of a word is however many letters long it is. Given a word W, denote its length by $l(W)$.

Example 1.2. $l(\text{book}) = 4$ and $l(\text{trigonometry}) = 12$. □

We would next like to develop a measure of similarity between two words of equal length.

Definition 1.3. The *difference* between two words of equal length is the number of letter positions in which the two words have different letters. Given two equal length words W and V, denote their difference by $d(W, V)$.

Example 1.4. $d(\text{book}, \text{look}) = 1$ because they have different letters in exactly one position (the first position on this example). On the other hand, $d(\text{cat}, \text{hog}) = 3$ because they have different letters in all three letter positions. □

Definition 1.5. A list of distinct words is called *stable* if all the words on the list are the same length and the difference between consecutive words is equal to 1.

With these few definitions in hand, our "theory of words" will now blossom. As you consider the following propositions, remember that their content is not the real prize; you are unlikely to encounter any of these results in your mathematical lives beyond this course. The real prize is your own burgeoning awareness that theories are built on definitions and that deep and precise understanding of the definitions is one of the key prerequisites for mathematical success.

Determine whether each proposition is true or false. Justify your conclusion thoroughly.

Proposition 1.6. *There exists a stable list of five length-4 words.*

Proposition 1.7. *Every stable list of length-2 words has fewer than 1000 words.*

Proposition 1.8. *If W and V are on the same stable list, then $d(W, V) < l(W)$.*

As we define new notions into an existing theory, the theory grows both in richness and complexity.

Definition 1.9. A list of distinct words is called *tight* if all the words on the list are the same length and $d(W, V) \leq 2$ for any two words W and V on the list.

Determine whether each proposition is true or false. Justify your conclusion thoroughly.

Proposition 1.10. *There exists a fourth word W beginning with an "h" such that the list*

$$\{\ \mathrm{sit}, \mathrm{hut}, \mathrm{sum}, W\ \}$$

is tight.

Proposition 1.11. *If the list*

$$\{\ \mathrm{sit}, \mathrm{hut}, \mathrm{sum}, W\ \}$$

is tight and W begins neither with "s" nor "h", then the last letter of W is a "t".

It is natural to wonder about the relationships, if any, between tight and stable lists.

Proposition 1.12. *There exist tight stable lists of length-3 words.*

Proposition 1.13. *All tight lists are stable.*

Proposition 1.14. *All stable lists are tight.*

1.2 Formalizing the Lexicon

In Section 1.1 we began developing a miniature "theory of words" based on a mere four definitions. The definitions and resulting theory were completely contrived and are probably not known to many outside our class.

There is, however, a widely agreed-upon language of mathematics. A high level of fluency in this language will be invaluable to you as you progress into your upper-division coursework.

In this section we introduce important vocabulary and begin to develop the rules of grammar within the language of mathematics.

Definition 1.15. A *proposition* is a statement that is either true or false.

Example 1.16. The following are all propositions:

- Elvis lives.
- Dr. Retsek had eggs for breakfast the morning of his tenth birthday.
- All stable lists are tight.

Example 1.17. Each of the following is not a proposition:

- Van Gogh was the best artist ever.
- What time is it?
- $x^2 = 4$.

The body of mathematical knowledge is a vast collection of propositions. Most of these are combinations of simpler propositions. There are three primary ways in which we combine propositions to form new propositions.

Definition 1.18 (Conjunction)**.** Let P and Q represent propositions. The *conjunction* of P and Q is expressed symbolically

$$P \wedge Q$$

and is read "P and Q". The proposition $P \wedge Q$ is true precisely when the component propositions P and Q are **both** true.

Definition 1.19 (Disjunction)**.** Let P and Q represent propositions. The *disjunction* of P and Q is expressed symbolically

$$P \vee Q$$

and is read "P or Q". The proposition $P \vee Q$ is true precisely when **at least one** of the component propositions P and Q is true.

Definition 1.20 (Negation)**.** Let P represent a proposition. The *negation* of P is expressed symbolically

$$\sim P$$

and is read "not P". The proposition $\sim P$ is true precisely when the component proposition P is **false**.

Exercise 1.21. Consider the following propositions

- P: "All stable lists of words are tight."
- Q: "Cal Poly is on semesters."
- R: ""Elvis lives." is a proposition."

and determine whether each of the following compound propositions is true or false, thoroughly justifying your answers:

(i) $P \vee R$.

(ii) $\sim (Q \wedge R)$.

(iii) $(\sim Q \wedge P) \vee (\sim P \wedge R)$.

Remark 1.22. Note that the symbol $\sim P \wedge Q$ can have a different truth value than the symbol $\sim (P \wedge Q)$; one must take care with parentheses when forming compound propositions.

Mathematics is full of notation that can look impenetrable to the lay person, but is actually quite convenient to those in the know. In many ways, this class is your initiation into the latter group. Consider, for instance, the following *truth tables*:

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

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

P	$\sim P$
T	F
F	T

These truth tables are designed to succinctly summarize definitions 1.18-1.20. To wit, the first truth table above merely indicates that the conjunction $P \wedge Q$ is true only when both constituent propositions P and Q are true.

The second truth table above indicates that the disjunction $P \vee Q$ is true as long as at least one of the constituent propositions P and Q is true.

The final truth table indicates that the proposition $\sim P$ has the opposite truth value as the proposition P.

There is a second utility to truth tables beyond summarizing the definitions of conjunction, disjunction and negation. One can use truth tables to recognize two different looking compound propositional forms as being logically equivalent. For instance, here is the truth table indicating the truth value of the propositional form $\sim (P \wedge Q)$:

P	Q	$P \wedge Q$	$\sim (P \wedge Q)$
T	T	T	F
T	F	F	T
F	T	F	T
F	F	F	T

Exercise 1.23. Construct a truth table for the propositional form $(\sim P) \vee (\sim Q)$. Is there any combination of truth values for the constituent propositions P and Q that yields different truth values for the propositional forms $\sim (P \wedge Q)$ and $(\sim P) \vee (\sim Q)$?

Exercise 1.24. Create a definition for what it means for two propositional forms to be *equivalent*.

Exercise 1.25. Conjecture a propositional form equivalent to $\sim (P \vee Q)$ and use truth tables to verify your conjecture.

The preceding exercises indicate that the negation operation $\sim$ "distributes" across parentheses in a regular and intuitive way. This is an important part of writing useful and stylistic "denials".

Definition 1.26. A *denial* of a proposition P is any proposition with the same truth value as $\sim P$.

Exercise 1.27. Write a denial of the proposition

"Cal Poly is on semesters."

Exercise 1.28. Write a denial of the proposition

"The window is open and the pie is missing."

Exercise 1.29. Write a denial of the proposition

"The function $f(x)$ is unbounded or constant."

1.3 Consider the Implications

Most mathematical theorems are formulated as so-called "if, then" statements. We begin this section by making a rigorous definition of "if, then".

Definition 1.30 (Conditional)**.** Let P and Q represent propositions. The *conditional sentence* "If P, then Q" is expressed symbolically

$$P \Rightarrow Q$$

and has truth table

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

The last two rows of the truth table for $P \Rightarrow Q$ are sometimes an initial shock. We are agreeing in Definition 1.30 that the proposition "If P, then Q" is true when the proposition P is false, no matter whether the proposition Q is itself true or false!?

An example may clarify our reasons for entering into this contract. Let's say I'm the coach of our basketball team and you all are the players. Suppose I tell you

"If you win tonight, then I will give you the day off tomorrow."

What is the only circumstance in which you can rightly claim to have been lied to?

1. If you win and I give you the day off tomorrow, then I have kept my word (first row of truth table).
2. If you lose and I don't give you the next day off, then I have not broken my word (last row of the truth table).
3. If you lose and I *do* give you the next day off, then I have granted you a break despite the loss but have not broken my word (third row of truth table).
4. The only way my "if,then" can possibly end up false is for you to win and for me to not give you the next day off (second row of the truth table).

Exercise 1.31. Determine a propositional form involving some of P, Q, $\wedge$, $\vee$ and $\sim$ that is logically equivalent to $P \Rightarrow Q$ and justify your assertion with truth tables.

Definition 1.32. In the conditional sentence $P \Rightarrow Q$, the proposition P is called the *antecedent* and the proposition Q is called the *consequent*.

Exercise 1.33. Write a true conditional sentence where the consequent is false.

Exercise 1.34. Write a true conditional sentence where the consequent is true.

Exercise 1.35. Write a true conditional sentence where the antecedent is false.

Exercise 1.36. Determine the truth value for each of the following conditional sentences.

(i) "If Euclid was a Leo, then squares have four sides."

(ii) "If $5 < 2$, then $10 < 7$."

(iii) "If $\sin\left(\frac{\pi}{2}\right) = 1$, then Betsy Ross was the first president of the United States."

There are two conditional sentences that are very closely related to the conditional sentence $A \Rightarrow B$.

Definition 1.37. The *converse* of the conditional sentence $P \Rightarrow Q$ is the conditional sentence $Q \Rightarrow P$.

Definition 1.38. The *contrapositive* of the conditional sentence $P \Rightarrow Q$ is the conditional sentence $(\sim Q) \Rightarrow (\sim P)$.

Exercise 1.39. Determine which of the converse and/or contrapositive is logically equivalent to the conditional sentence $P \Rightarrow Q$ and justify your conclusions with truth tables.

Exercise 1.40. Write the converse and contrapositive of the conditional sentence

"If f is an even function, then $f(2) = f(-2)$."

When the implication between propositions P and Q "runs both ways", we have a much stronger logical relationship.

Definition 1.41 (Biconditional)**.** Let P and Q represent propositions. The *biconditional sentence* "P if and only if Q" is expressed symbolically

$$P \Leftrightarrow Q$$

and has truth table

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

Exercise 1.42. Use truth tables to show that $P \Leftrightarrow Q$ is logically equivalent to $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$.

Exercise 1.43. Determine the truth value for each of the following biconditional sentences.

(i) "The moon is made of cheese if and only if the earth is flat."

(ii) "$1 + 1 = 2$ if and only if $\cos(\pi) = -1$."

(iii) ""If $5 < 2$, then $10 < 7$." if and only if "Elvis lives." is a proposition."

As we begin writing mathematics, do not underestimate stylistic considerations. There are many phrases equivalent to the conditional sentence $P \Rightarrow Q$ and a few others equivalent to the biconditional sentence $P \Leftrightarrow Q$. We use these to lend texture and interest to how we *communicate* mathematics. We end this section with a number of these common phrases, feel free to use them correctly and stylistically.

Phrases translated by $P \Rightarrow Q$

If P, then Q.	Q, if P.
P implies Q.	Q whenever P.
P is sufficient for Q.	Q is necessary for P.
P only if Q.	Q, when P.

Phrases translated by $P \Leftrightarrow Q$

P if and only if Q.
P iff Q.
P is equivalent to Q.
P is necessary and sufficient for Q.

1.4 Quantifiers

The mathematical sentence "$x^2 = 4$" is not a proposition. In our discussion of Example 1.17, we decided that "$x^2 = 4$" is neither true nor false, but rather has truth value dependent upon the value of the variable x under consideration. If $x = 2$, it's true; if $x = 3$ it's false. The need to deal with such expressions motivates the following definition.

Definition 1.44. An *open sentence* $P(x_1, x_2, \ldots, x_k)$ is a sentence containing one or more variables that becomes a proposition only when the variables are assigned specific values.

The realm of all possible values that the variables may be assigned is called the *universe*.

The collection of all values of the variables in the universe that make a true proposition upon substitution into the open sentence is called the *truth set* of the open sentence.

Example 1.45. Consider the open sentence $P(x)$: "$x^2 = 4$."

If the universe is the set $\mathbb{R}$ of all real numbers, then the truth set is $\{-2, 2\}$.

On the other hand, if the universe is the set $\mathbb{R}^+$ of positive real numbers, then the truth set is $\{2\}$.

The point is that it is very important to be clear about the universe within which we are considering open sentences and to always stop and ask whenever in doubt. $\square$

Exercise 1.46. Write an open sentence in the universe of real numbers that is true for every member of the universe.

Exercise 1.47. Write an open sentence in the universe of cats that is true for no member of the universe.

Exercise 1.48. Write an open sentence in the universe of vegetables that is true for at least one but not every member of the universe.

The preceding examples illustrate some of the common types of truth sets for open sentences. There is standard notation for each.

Definition 1.49 (Universal Quantifier)**.** Let $P(x)$ be an open sentence with variable x. The proposition

$$(\forall x)P(x)$$

is read "For all x, $P(x)$" and is true precisely when $P(x)$ is true for *every* value of x in the universe. The symbol $\forall$ is called the *universal quantifier*.

Definition 1.50 (Existential Quantifier)**.** Let $P(x)$ be an open sentence with variable x. The proposition

$$(\exists x)P(x)$$

is read "There exists x such that $P(x)$" and is true precisely when $P(x)$ is true for *at least one* value of x in the universe. The symbol $\exists$ is called the *existential quantifier*.

The ability to effectively handle quantified propositions is a necessary condition for reading and writing mathematics. As with all languages, fluency is earned through practice.

Exercise 1.51. Let the universe be the real numbers $\mathbb{R}$. Determine the truth value for each proposition.

(i) $(\forall x)(x^2 + 1 \geq 0)$.

(ii) $(\exists x)(|x| > 0)$.

(iii) $(\forall x)(|x| > 0)$.

(iv) $(\exists x)(2x + 3 = 6x + 7)$.

Exercise 1.52. Name a universe in which $(\exists x)(2x + 3 = 6x + 7)$ is false.

Exercise 1.53. Name a universe in which $(\exists x)(x^2 + 1 = 0)$ is true.

We have seen already in Section 1.3 that the negation $\sim$ interacts nicely with parentheses, $\wedge$ and $\vee$. It is natural to next consider intermingling negations and quantifiers.

Exercise 1.54. Let $P(x)$ be an open sentence in some universe. Determine whether the proposition

$$[\sim (\forall x)P(x)] \Leftrightarrow [(\exists x)(\sim P(x))]$$

is true or false and justify your conclusion.

Exercise 1.55. Let $P(x)$ be an open sentence in some universe. Determine whether the proposition

$$[\sim (\exists x)P(x)] \Leftrightarrow [(\forall x)(\sim P(x))]$$

is true or false and justify your conclusion.

The results of the previous two exercises are particularly useful when formulating denials of quantified propositions.

Exercise 1.56. Write a denial of the proposition

"All even numbers are divisible by four."

Exercise 1.57. Write a denial of the proposition

"Some intelligent people revile mathematicians."

Exercise 1.58. Let the natural numbers $\mathbb{N} = \{1, 2, 3, \ldots\}$ be the universe. Translate the proposition

$$(\forall x)(\,[(x \text{ prime}) \wedge (x \neq 2)] \Rightarrow [(\exists j)(x = 2j + 1)]\,)$$

into English.

Most of the fundamental theorems in real analysis (Math 412 here at Cal Poly) are multiply quantified propositions. Strive always to take your time and calmly assess such statements.

Exercise 1.59. Let the universe be the real numbers $\mathbb{R}$. Determine the truth value for each proposition.

(i) $(\forall x)(\exists y)(x < y)$.

(ii) $(\exists y)(\forall x)(x < y)$.

Exercise 1.60. Let the universe be the real numbers $\mathbb{R}$. Write the negation of each proposition.

(i) $(\forall x)(\exists y)(x < y)$.

(ii) $(\exists y)(\forall x)(x < y)$.

We conclude with the special notation reserved for the situation when an open sentence is true for exactly one member of the universe.

Definition 1.61 (Unique Existential Quantifier)**.** Let $P(x)$ be an open sentence with variable x. The proposition

$$(\exists! x)P(x)$$

is read "There exists a unique x such that $P(x)$" and is true precisely when $P(x)$ is true for *exactly one* value of x in the universe. The symbol $\exists!$ is called the *unique existential quantifier.*

Exercise 1.62. Let the universe be the real numbers $\mathbb{R}$. Determine the truth value for each proposition.

(i) $(\exists! x)(x \geq 0 \wedge x \leq 0)$.

(ii) $(\exists! x)(x > 5)$.

(iii) $(\exists! x)(x^2 = 4)$

Chapter 2

Mathematical Proof

Use punctuation, it's classy.

2.1 What Constitutes Proof?

In Section 1.1 we spent a fair bit of time convincing one another of the truth or falsity of eight propositions. What followed in chapter one was all the formalism that we will require for the rest of the term, but we mustn't forget those early days of argumentation and justification.

There, without naming our actions, the class standard of proof was born. What we demand of ourselves and our peers is iron-clad reasoning based on religious adherence to agreed-upon definitions, all communicated with cool and unadorned clarity. We are our own harshest critics and we will accept no substitutes.

Consider, for instance, our proof of Proposition 1.11, restated here as

Theorem 2.1. *If the list*

$$\{\ \mathrm{sit}, \mathrm{hut}, \mathrm{sum}, W\ \}$$

is tight and W begins neither with "s" nor "h", then the last letter of W is a "t".

Proof. Suppose that the list $\{\ \mathrm{sit}, \mathrm{hut}, \mathrm{sum}, W\ \}$ is tight and W begins neither with "s" nor "h". If W has a "u" in its second letter position, $d(\mathrm{sit}, W) \leq 2$ implies that W has a "t" in its third letter position. On the other hand, if W does not have a "u" in its second letter position, $d(\mathrm{hut}, W) \leq 2$ implies that W has a "t" in its third letter position. In either case, W has a "t" in its third letter position. $\square$

It is instructive to view the proof of Theorem 2.1 through the lens of formalism provided by chapter one. If we name the constituent propositions

$$
\begin{aligned}
A &: \text{The list } \{ \text{ sit}, \text{hut}, \text{sum}, W \text{ } \} \text{ is tight} \\
B &: W \text{ begins neither with "s" nor "h"} \\
C &: \text{The last letter of } W \text{ is a "t"},
\end{aligned}
$$

then the statement of Theorem 2.1 boils down to

$$[A \wedge B] \Rightarrow C.$$

According to Definition 1.30, the proposition $P \Rightarrow Q$ is automatically true when the antecedent P is false.

The point is that when we set about proving conditional propositions, we need only concern ourselves with demonstrating the truth of the consequent *supposing the antecedent is true.*

Here is a template for direct proof of a conditional proposition:

Proof. Suppose P.
•
•
•
Therefore, Q. □

Table 2.1: Direct Proof of $P \Rightarrow Q$

Consider our proof of Theorem 2.1 and its underlying structure side by side (note here that the antecedent is itself the conjunctive proposition $A \wedge B$):

Proof	*Structure*
Suppose that the list $\{$ sit, hut, sum, W $\}$ is tight and W begins	*Proof.* Suppose $A \wedge B$.
neither with "s" nor "h". If W has a "u" in its second letter	•
position, $d(\text{sit}, W) \leq 2$ implies that W has a "t" in its third	•
letter position. On the other hand, if W does not have a "u"	•
in its second letter position, $d(\text{hut}, W) \leq 2$ implies that	•
W has a "t" in its third letter position. In either case, W has	•
a "t" in its third letter position. □	Therefore, C. □

Table 2.2: Proof of Theorem 2.1 with Corresponding Structure

The devil is in the • • •, of course. Sometimes the details of the logical path will be a straightforward matter of successive application of the definitions, as in Table 2.2. Often, however, your own creativity and ingenuity will be necessary. This is the art of proof and it is what we are learning in this class. Practice well to hone your craft.

Theorem 2.1 is the only theorem in this book where the proof is provided. Henceforth, you will prove every theorem that arises. You may use only the relevant definitions, exercises and theorems that we have already established.

Definition 2.2. Let $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ be the *integers*. We say that the integer a *divides* the integer b if there exists an integer k such that $b = ak$.

Example 2.3. The integer 6 divides the integer 42 because $42 = 6 \cdot 7$. The integer 8 does not divide the integer 34 because there is no integer k such that $34 = 8k$. □

Theorem 2.4. *Let a, b and c be integers. If a divides b, then a divides bc.*

Theorem 2.5. *Let a, b and c be integers. If a divides b and a divides $b + c$, then a divides $3c$.*

Exercise 2.6. Create a definition for what it means for an integer to be *even*.

Exercise 2.7. Create a definition for what it means for an integer to be *odd*.

Theorem 2.8. *If x and y are even integers, then $x + y$ is an even integer.*

Theorem 2.9. *If x and y are odd integers, then $x + y$ is an even integer.*

Theorem 2.10. *If x and y are even integers, then 4 divides xy.*

Theorem 2.11. *If x is an integer, then $x^2 + x + 3$ is an odd integer.*

Theorem 2.12. *The product of consecutive integers is an even integer.*

2.2 Three More Basic Proof Structures

In Section 2.1 we used the direct proof structure of Table 2.1 to discuss what we mean by "proof". Our answer

> "What we demand of ourselves and our peers is iron-clad reasoning based on religious adherence to agreed-upon definitions, all communicated with cool and unadorned clarity. We are our own harshest critics and we will accept no substitutes."

is, however, independent of the method of proof. In this section we take note of three more basic proof structures and put them to use proving some more theorems.

2.2.1 Proof of $P \Rightarrow Q$ by Contraposition

According to Exercise 1.39, the contrapositive $(\sim Q) \Rightarrow (\sim P)$ is equivalent to the conditional proposition $P \Rightarrow Q$. Thus, to prove $P \Rightarrow Q$ it is equivalent to prove $(\sim Q) \Rightarrow (\sim P)$. The resulting proof structure is called "Proof by Contraposition" and is illustrated in Table 2.3.

Proof. Suppose $\sim Q$.
•
•
•
Therefore, $\sim P$.
Thus, $P \Rightarrow Q$. ☐

Table 2.3: Proof of $P \Rightarrow Q$ by Contraposition.

Theorem 2.13. *Let x be an integer. If 4 does not divide x^2, then x is odd.*

Theorem 2.14. *Let x be an integer. If 8 does not divide $x^2 - 1$, then x is even.*

Theorem 2.15. *Let x and y be integers. If xy is even, then either x is even or y is even.*

2.2.2 Proof of $P \Leftrightarrow Q$

According to Exercise 1.42, the biconditional proposition $P \Leftrightarrow Q$ is logically equivalent to $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$. Thus, to prove $P \Leftrightarrow Q$ it is equivalent to prove $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$. The resulting proof structure is a two-part proof and is illustrated in Table 2.4.

Proof.
(i) Show $P \Rightarrow Q$ directly or by contraposition.
• • •
(ii) Show $Q \Rightarrow P$ directly or by contraposition.
• • •
Therefore, $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$.
Thus, $P \Leftrightarrow Q$. ☐

Table 2.4: Two-part Proof of $P \Leftrightarrow Q$.

Theorem 2.16. *Let a, b and c be positive integers. The integer ac divides bc if and only if the integer a divides b.*

Theorem 2.17. *Let a and b be positive integers. The integer $a+1$ divides b and the integer b divides $b+3$ if and only if $a = 2$ and $b = 3$.*

Theorem 2.18. *Let x be a real number. The quadratic $x^2 + 2x + 1 = 0$ if and only if $x = -1$.*

2.2.3 Proof by Contradiction

Imagine we wish to prove some proposition P and we instead prove that

$$(\sim P) \Rightarrow 1 = 2.$$

Because we know that the consequent $1 = 2$ is false, the truth of $(\sim P) \Rightarrow 1 = 2$ implies that the antecedent $\sim P$ is false. We therefore conclude that the original proposition P is true.

The preceding example illustrates "Proof by Contradiction", whereby assuming the negation of what we wish to prove leads logically to absurdity ($1 = 2$ in the present case). The general structure of proof by contradiction is illustrated in Table 2.5.

Proof. Suppose $\sim P$.
•
•
•
Therefore, Q.
But $\sim Q$ is true.
Therefore, P. ☐

Table 2.5: Proof of P by Contradiction.

Again, the role of proposition Q is being played by "$1 = 2$" in our example above. Generally, the key to proof by contradiction lies in deciding what proposition will play the role of Q in the structure of Table 2.5.

Exercise 2.19. Determine what supposition would begin a proof of $P \Rightarrow Q$ by contradiction.

Definition 2.20. A real number r is called *rational* if there exist integers p and q (with $q \neq 0$) such that

$$r = \frac{p}{q}.$$

A real number that is not rational is called *irrational*.

The following is a classic. If you believe in the number $\sqrt{2}$, then this theorem says it's irrational.

Theorem 2.21. *If r is a real number and $r^2 = 2$, then r is irrational.*

The following proposition is not a classic. It's good, though.

Proposition 2.22. *At any Cal Poly football game there are at least two people in attendance with the same number of friends in attendance.*

Google "hardest logic puzzle ever" if you enjoy this next one!

Proposition 2.23. *Suppose Finn and Sloan come from a land where each person either always lies or always tells the truth. If Finn says "Exactly one of us is lying" and Sloan says "Finn is telling the truth", then Finn and Sloan are both lying.*

CAUTION 2.24. Many mathematicians view proofs by contradiction as being less than ideal. One reason for this is that they may provide less insight by their very nature. For instance, a direct proof of $P \Rightarrow Q$ may literally exhibit the *way* that P implies Q, whereas a proof of $P \Rightarrow Q$ by contradiction may only demonstrate that P and $\sim Q$ are incompatible.

Moreover, many proofs by contradiction are in fact nice proofs by contraposition that have been kidnapped and dressed up in ill-fitting clothes. For example, consider a worse version of our proof of Theorem 2.13:

Proof. Suppose that 4 does not divide x^2 and x is even. **Since x is even, there exists an integer j such that $x = 2j$, so $x^2 = (2j)^2 = 4j^2$. Thus, 4 divides x^2.** But this contradicts the supposition that 4 does not divide x^2. Thus, if 4 does not divide x^2, then x is odd. □

The bold portion of the proof is our nice tidy proof by contraposition of Theorem 2.13; the rest is just clumsy and extraneous noise.

In this class, let us strive always to avoid proof by contradiction and to instead employ another method of proof whenever possible.

2.3 Proofs of Quantified Propositions

Many of the most fundamental definitions and theorems in advanced mathematics involve the quantifiers $\forall$ and $\exists$. Facility in proving quantified propositions is critical to future success.

2.3.1 Existence Proofs

Proposition 2.25. *There exists a real number x such that $x^2 = 4$.*

The statement of Proposition 2.25 may be symbolized by

$$(\exists x)(x^2 = 4)$$

in the universe of real numbers. In this instance, the proof consisted of actually producing a specific, concrete value of x that made the open sentence $x^2 = 4$ into a true proposition. Such existence proofs are called *constructive* because the desired object has been constructed and presented to the reader. Table 2.6 illustrates the structure of such existence proofs.

Proof. Consider the object $\star$.
•
•
•
Therefore, $P(\star)$ is true.
Thus, $(\exists x)P(x)$. $\square$

Table 2.6: Constructive Proof of $(\exists x)P(x)$.

CAUTION 2.26. Not all existence proofs are constructive. Sometimes, a valid existence proof leaves us certain that *some* object with particular properties exists, yet leaves us with no idea what *specific* object it is.

Proposition 2.27. *There exists a three-digit number less than 400 with distinct digits that sum to 17 and multiply to 108.*

Proposition 2.28. *There exist irrational numbers x and y such that $x+y$ is rational.*

Proposition 2.29. *There exists an irrational number r such that $r^{\sqrt{2}}$ is rational.*

Proposition 2.30. *There exist integers m and n such that $7m + 2n = 1$.*

Proposition 2.31. *Some two grandmothers of past or present U.S. presidents have birthdays within eleven days of one another.*

2.3.2 Proofs of Universal Propositions

In order to prove a universally quantified proposition $(\forall x)P(x)$, we must show that *every* specific value of x in the universe under consideration yields a true proposition $P(x)$.

Proposition 2.32. *For every odd integer n, $2n^2 + 3n + 4$ is odd.*

Table 2.7 illustrates the typical structure of a proof of $(\forall x)P(x)$. The key thing is to begin by considering an *arbitrary* object x from the relevant universe, resisting all temptation to ascribe any characteristics to x beyond those given by the hypotheses and mere membership in the universe.

Proof. Let x be an arbitrary member of the universe U.
•
•
•
Therefore, $P(x)$ is true.
Thus, $(\forall x)P(x)$. $\square$

Table 2.7: Proof of $(\forall x)P(x)$ in the Universe U.

Theorem 2.33. *For all positive real numbers x and y, $\dfrac{x+y}{2} \geq \sqrt{xy}$.*

Commonly, the statement $P(x)$ in some quantified proposition $(\forall x)P(x)$ is itself a quantified proposition. See Exercises 1.59 and 1.60 to recall what is at stake in such multiply quantified propositions.

Proposition 2.34. *For every real number x there exists a real number y such that $x < y$.*

Proposition 2.35. *There exists a real number y such that for every real number x, $x < y$.*

Proposition 2.36. *For each real number x there exists a real number y such that $x + y = 0$.*

Proposition 2.37. *For every positive real number x there exists a positive real number $y < x$ such that $(\forall z)(z > 0 \Rightarrow yz \geq z)$.*

Proposition 2.38. *For every positive real number ε there exists a positive integer N such that $n \geq N \Rightarrow 1/n < \varepsilon$.*

2.3.3 Unique Existence Proofs

Proposition 2.39. *There exists a unique real number whose square is* 4.

Proposition 2.39 is clearly false. Not because there is no such real number, but because there are too many. The point is that in order to prove a unique existence proposition $(\exists! x)P(x)$, *two* things must be done: (i) an existence proof a la subsection 2.3.1 and (ii) a proof that there is at most one object x such that $P(x)$ is true.

Proof.
(i) Show $(\exists x)P(x)$ by some method.
• • •
(ii) Show $[P(x_1) \wedge P(x_2)] \Rightarrow [x_1 = x_2]$.
• • •
Thus, $(\exists! x)P(x)$. $\square$

Table 2.8: Two-part Proof of $(\exists! x)P(x)$.

Part (ii) of Table 2.8 requires we prove the conditional proposition

$$[P(x_1) \wedge P(x_2)] \Rightarrow [x_1 = x_2].$$

All of the techniques we have encountered already (direct proof, proof by contraposition, proof by contradiction) are potentially viable here and we should treat the proof of this implication as we would any other.

Proposition 2.40. *There exists a unique positive real number whose square is* 4.

Definition 2.41. A *queen* is a chess piece that can attack along rows, columns and diagonals. A *truce* is an arrangement of mutually non-attacking queens.

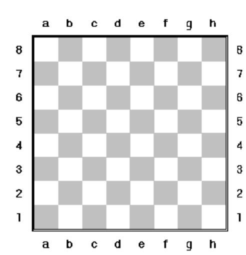


Figure 2.1: A standard chess board.

Proposition 2.42. *There exists a truce of eight queens on the standard chess board.*

Proposition 2.43. *There does not exist a truce of six queens on a 6x6 chess board in which a corner of the board is occupied.*

Proposition 2.44. *There exists a unique truce of six queens on a 6x6 chess board.*

2.4 The Deep Blue Sea

We have done thirty-four proofs so far in this chapter, which is great. But our experience proving things differs from reality in one fundamental way: in each of our thirty-four successes we have known in advance what proof technique to attempt.

In mathematical reality, one encounters a proposition and formulates some feeling for whether it's true or false and then *decides* on an approach. Sometimes things go smoothly and our first inclination bears fruit; often, we choose poorly and have to go back to the drawing board. The very best provers share a certain fearlessness and an ability to greet failure with a smile, confident that with every false step they have added to their unique and priceless personal wisdom.

There is not one shred of mathematical content in this class that can't be recalled or looked up at a later time, but the conditions assembled here that have allowed us to see with new eyes cannot be recreated. Your opportunity to start anew has arrived, and it is singular.

We have the tools. We are fearless. Now into the sea...

Chapter 3

The Theory of Sets

Your proof is not merely a demonstration, it's also a narrative.

3.1 The Stage is Sets

Definition 3.1. A *set* is a collection of objects called its *elements*. If A is a set and x is an element of A, we write $x \in A$. Otherwise, we write $x \notin A$.

Sometimes we describe sets by just listing their elements:

$$\begin{aligned} &A = \{1, 2, 8, 17\} \\ &\mathbb{N} = \{1, 2, 3, \ldots\} && \text{(the \textit{natural numbers})} \\ &\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\} && \text{(the \textit{integers}).} \end{aligned}$$

Other times, we describe sets by abstraction: $B = \{x \in U : x \text{ has a certain property}\}$, which is read "$B$ equals the set of all x in U such that x has a certain property."

For example, according to Definition 2.20 the set of rational numbers may be described by

$$\mathbb{Q} = \left\{ r \in \mathbb{R} : r = \frac{p}{q} \text{ for some } p \in \mathbb{Z} \text{ and } q \in \mathbb{Z} \text{ with } q \neq 0 \right\}.$$

Definition 3.2. The set having no elements is called the *empty set* and is denoted by the Danish letter $\emptyset$.

Example 3.3. Since $x^2 \geq 0$ for every real number x,

$$\{x \in \mathbb{R} : x^2 + 1 = 0\} = \emptyset. \quad \square$$

Definition 3.4. There are certain sets of real numbers that garner special notation (a and b denote real numbers throughout):

$(a,b) = \{x \in \mathbb{R} : a < x < b\}$	(the *open interval* from a to b)
$[a,b] = \{x \in \mathbb{R} : a \leq x \leq b\}$	(the *closed interval* from a to b)
$(a,\infty) = \{x \in \mathbb{R} : a < x\}$	(the *open ray* from a to infinity)
$[a,\infty) = \{x \in \mathbb{R} : a \leq x\}$	(the *closed ray* from a to infinity)
$(-\infty,b) = \{x \in \mathbb{R} : x < b\}$	(the *open ray* from minus infinity to b)
$(-\infty,b] = \{x \in \mathbb{R} : x \leq b\}$	(the *closed ray* from minus infinity to b)

Exercise 3.5. Create set definitions for the following notations and give the sets names as in Definition 3.4:

$(a,b] =$

$[a,b) =$

Definition 3.6. We say that A is a *subset* of B and write $A \subseteq B$ provided each element of the set A is also an element of the set B. That is,

$$A \subseteq B \Leftrightarrow [x \in A \Rightarrow x \in B].$$

We say A *equals* B and write $A = B$ provided $A \subseteq B$ and $B \subseteq A$. That is,

$$A = B \Leftrightarrow [A \subseteq B \wedge B \subseteq A].$$

Proposition 3.7. $\{1, 2, 3, \pi\} \subseteq [1, 4)$.

Proposition 3.8. $\emptyset = \{\emptyset\}$.

Proposition 3.9. $\emptyset \notin \emptyset$.

Proposition 3.10. *For every set A, $\emptyset \subseteq A$.*

Proposition 3.11. $[1/2, 5/2] \subseteq \mathbb{Q}$.

Proposition 3.12. $\{\{\emptyset\}\} \subseteq \{\emptyset, \{\emptyset\}\}$.

Proposition 3.13. $\{\ 1, 2\} \in \{\{1, 2, 3\}, \{2, 3\}, 1, 2\}$.

Proposition 3.14. *If A and B are both sets of real numbers, $A \subseteq B$ or $B \subseteq A$.*

Despite Proposition 3.14, set containment does enjoy other comparative properties. Chief among these is the following theorem that shows that set containment is *transitive.*

Theorem 3.15. *Let A, B and C be sets. If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.*

CAUTION 3.16. There is a big difference between studying *axiomatic set theory*, which is a deep and difficult subject lying at the very foundations of logic and mathematics, and *naive set theory*, which takes some liberties in the interest of brevity and practicality.

For instance, reconsider Definition 3.1. A true set theorist would be aghast as we defined the term "set" with the term "collection."

"What, pray tell, is a collection?" they might inquire.

"Oh, a collection is a, um, you know, aggregate of things taken in unison, I guess," we might respond.

"I'm going to be sick," they would finally lament.

The point is that the divide between axiomatic and naive set theory is not easily bridged and is pretty far from the point of our class. What we develop in our class will take you all the way through your undergraduate math career and would only become insufficient if you became a set theorist.

Be warned, though, there are paradoxes in the world of naive set theory!

Consider **Richard's Paradox**:

> Let
>
> $A = \{x \in \mathbb{N} : x \text{ is describable in fewer than 10,000 English characters } \}.$
>
> The number of distinct strings of fewer than 10,000 English characters is finite. HUGE, but finite. Since there are infinitely many natural numbers, these strings cannot describe every natural number. Let N denote the smallest natural number not in A.
>
> But there are way fewer than 10,000 characters in the preceding paragraph and these describe the number N, so N *is* in A?!? □

Definition 3.17. A set A is called *ordinary* if it does not contain itself as an element, i.e. if $A \notin A$.

Exercise 3.18. Let $X = \{A : A \text{ is an ordinary set } \}$. Is X ordinary? Is X not ordinary?

3.2 New Sets From Old

The three primary ways we combine two sets to form a new set are given in the following definition.

Definition 3.19. Let A and B be sets with elements from some universe U.

(i) The *union* of A and B is the set

$$A \cup B = \{x \in U : x \in A \vee x \in B\}.$$

(ii) The *intersection* of A and B is the set

$$A \cap B = \{x \in U : x \in A \wedge x \in B\}.$$

When $A \cap B = \emptyset$, we say that A and B are *disjoint*.

(iii) The *difference* $A \setminus B$ is the set

$$A \setminus B = \{x \in U : x \in A \wedge x \notin B\}.$$

Exercise 3.20. Draw Venn diagrams illustrating the union, intersection and difference of sets A and B within the universe U.

Exercise 3.21. Let $A = \{1, 3, 5, 7, 9\}$ and $B = \{0, 2, 4, 7, 8\}$. Determine $A \cup B$, $A \cap B$, $A \setminus B$ and $B \setminus A$.

Exercise 3.22. Write the open interval $(1, 3)$ as the union of two disjoint subsets of $\mathbb{R}$.

Proposition 3.23. *Let A, B and C be sets. If $A \subseteq B$, then $A \setminus C \subseteq B \setminus C$.*

Proposition 3.24. *Let A, B, C and D be sets. If $A \cup B \subseteq C \cup D$, $A \cap B = \emptyset$, and $C \subseteq A$, then $B \subseteq D$.*

Proposition 3.25. *If A, B and C are sets, then $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.*

Definition 3.26. Let A be a set with elements in some universe U. The *complement* of A is the set $\widetilde{A}$ given by

$$\widetilde{A} = U \setminus A.$$

Exercise 3.27. Draw a Venn diagram illustrating the complement of the set A within the universe U.

Exercise 3.28. Let the universe be the real numbers $\mathbb{R}$.

(i) Determine the complement of $(2, \infty)$.

(ii) Determine the complement of $[1, 3)$.

(iii) Determine $\widetilde{\emptyset}$.

Proposition 3.29. *For any set A in any universe U, $\widetilde{\widetilde{A}} = A$.*

Proposition 3.30. *Let A and B be sets in some universe. If $\widetilde{B} \subseteq \widetilde{A}$, then $A \subseteq B$.*

The similarity among the symbols "$\vee, \wedge$ and $\sim$" and the symbols "$\cup, \cap$ and $\widetilde{\ }$ " is no coincidence. The following theorem is the "set version" of Exercises 1.23 and 1.25.

Theorem 3.31 (DeMorgan's Laws : Initial Version)**.** *Let A and B be sets in some universe.*

(i) $(\widetilde{A \cup B}) = \widetilde{A} \cap \widetilde{B}$.

(ii) $(\widetilde{A \cap B}) = \widetilde{A} \cup \widetilde{B}$.

3.3 Families of Sets

The phrase "set of sets" sounds a bit awkward, so we often say "*family* of sets" to refer to a set whose elements are themselves sets.

Example 3.32. The family

$$\mathscr{A} = \{\{1, 2\}, \{2, 3, 5\}, \{-\pi, 2\}\}$$

has three elements, each of which is a set of real numbers.

Because $\mathscr{A}$ has only three members, the union and intersection of the elements of the family $\mathscr{A}$ are easy to see:

$$\{1, 2\} \cup \{2, 3, 5\} \cup \{-\pi, 2\} = \{-\pi, 1, 2, 3, 5\} \quad \text{and} \quad \{1, 2\} \cap \{2, 3, 5\} \cap \{-\pi, 2\} = \{2\}.$$

But what if $\mathscr{A}$ had 1437 elements rather than just three elements? It would be highly impractical to write each of these many sets down (and probably harder to determine the union and intersection, too.) Now imagine $\mathscr{A}$ had infinitely many elements; we literally couldn't write each element set down and determining the union and intersection might be harder still. $\square$

The point is that we require a practical way of writing down unions and intersections over all elements of large families of sets. The following definition provides just such notation.

Definition 3.33. Let $\mathscr{A}$ be a family of sets in some universe U. The union and intersection of all sets in $\mathscr{A}$ are given by

$$\bigcup_{A\in\mathscr{A}} A = \{x \in U : x \in A \text{ for at least one set } A \in \mathscr{A}\}$$

and

$$\bigcap_{A\in\mathscr{A}} A = \{x \in U : x \in A \text{ for every set } A \in \mathscr{A}\}.$$

Exercise 3.34. Let $\mathscr{A} = \{[a,\infty) \subseteq \mathbb{R} : a \in \mathbb{R}\}$. Determine $\displaystyle\bigcup_{A\in\mathscr{A}} A$ and $\displaystyle\bigcap_{A\in\mathscr{A}} A$.

Exercise 3.35. Let $\mathscr{A} = \{(-a,a) \subseteq \mathbb{R} : a > 0\}$. Determine $\displaystyle\bigcup_{A\in\mathscr{A}} A$ and $\displaystyle\bigcap_{A\in\mathscr{A}} A$.

Proposition 3.36. *If $\mathscr{A}$ is a family of sets, then for each $B \in \mathscr{A}$*

$$\bigcap_{A\in\mathscr{A}} A \subseteq B.$$

Proposition 3.37. *If $\mathscr{A}$ is a family of sets, then for each $B \in \mathscr{A}$*

$$B \subseteq \bigcup_{A\in\mathscr{A}} A.$$

One natural way a set A can give rise to a family of sets is by considering the set of all subsets of the set A.

Definition 3.38. Let A be a set. The *power set* of A is denoted by $\mathscr{P}(A)$ and consists of every subset of A.

Exercise 3.39. Determine $\mathscr{P}(\{1,2\})$.

Proposition 3.40. *Let B be a set. Then*

$$\bigcup_{A\in\mathscr{P}(B)} A = B \quad \text{and} \quad \bigcap_{A\in\mathscr{P}(B)} A = \emptyset.$$

Example 3.41. Consider the family of sets

$$\mathscr{A} = \{\{1\}, \{1,2\}, \{1,2,3\}, \{1,2,3,4\}, \ldots\}.$$

For each $n \in \mathbb{N}$, let $A_n = \{1, 2, 3, \ldots, n\}$. With the new notation,

$$\mathscr{A} = \{A_1, A_2, A_3, A_4, \ldots\}.$$

Even more compactly, we could denote $\mathscr{A}$ by

$$\mathscr{A} = \{A_n : n \in \mathbb{N}\} = \{A_n\}_{n\in\mathbb{N}} = \{A_n\}_{n=1}^{\infty}. \quad \square$$

The point of the preceding example is that when we "subscript" the sets in a family $\mathscr{A}$ we can often describe $\mathscr{A}$ very succinctly. This act of "subscripting" is called *indexing* and is formalized in the following definition.

Definition 3.42. Let Δ be a nonempty set. Suppose for each $\alpha \in \Delta$ there is a corresponding set A_α. The family of sets

$$\mathscr{A} = \{A_\alpha : \alpha \in \Delta\}$$

is called an *indexed family of sets*. Each $\alpha \in \Delta$ is a particular *index* and the set Δ is called the *indexing set*.

Exercise 3.43. Let $\Delta = \{\clubsuit, \heartsuit, \spadesuit\}$. Let $A_\clubsuit = \{2, 4, 7\}$, $A_\heartsuit = \{3, 4, 5\}$ and $A_\spadesuit = \{4, 5, 7\}$. Let $\mathscr{A} = \{A_\alpha : \alpha \in \Delta\}$.

Determine $\displaystyle\bigcup_{A\in\mathscr{A}} A$ and $\displaystyle\bigcap_{A\in\mathscr{A}} A$.

Exercise 3.44. Suppose $\mathscr{A} = \{A_\alpha : \alpha \in \Delta\}$ is an indexed family of sets. Agree as a class on reasonable interpretations of the symbols

$$\bigcup_{\alpha\in\Delta} A_\alpha \quad \text{and} \quad \bigcap_{\alpha\in\Delta} A_\alpha.$$

Exercise 3.45. Let $\Delta = \mathbb{R}$. For each $x \in \Delta$, let $B_x = [x^2, x^2 + 1]$ be the closed interval from x^2 up to $x^2 + 1$. Determine $\displaystyle\bigcup_{x\in\mathbb{R}} B_x$ and $\displaystyle\bigcap_{x\in\mathbb{R}} B_x$.

Exercise 3.46. Let $\Delta = \mathbb{N}$. For each $n \in \Delta$, let $A_n = (-1/n, 2 + 2/n]$. Determine $\displaystyle\bigcup_{n\in\mathbb{N}} A_n$ and $\displaystyle\bigcap_{n\in\mathbb{N}} A_n$.

Note 3.47. When the indexing set is the natural numbers $\mathbb{N}$, we commonly write

$$\bigcup_{n=1}^{\infty} A_n \quad \text{to mean} \quad \bigcup_{n\in\mathbb{N}} A_n$$

and

$$\bigcap_{n=1}^{\infty} A_n \quad \text{to mean} \quad \bigcap_{n\in\mathbb{N}} A_n.$$

Exercise 3.48. For the indexed family of Exercise 3.46, interpret and determine

$$\bigcup_{n=2}^{3} A_n, \quad \bigcap_{n=1}^{5} A_n, \quad \text{and} \quad \bigcup_{n=4}^{\infty} A_n.$$

Indexed unions and intersections interact in predictable ways with other sets. The following theorems and propositions illustrate these interactions. If one of them is about intersections, it is fruitful to conjecture and assess the analogous statement for unions; if it's about unions, conjecture and assess the analogous statement for intersections.

Theorem 3.49. *If $\mathscr{A} = \{A_\alpha : \alpha \in \Delta\}$ is an indexed family of sets and B is a set, then*

$$B \cup \left(\bigcap_{\alpha\in\Delta} A_\alpha\right) = \bigcap_{\alpha\in\Delta} (B \cup A_\alpha).$$

Proposition 3.50. *If $\mathscr{A} = \{A_\alpha : \alpha \in \Delta\}$ is an indexed family of sets and B is a set, then*

$$B \setminus \left(\bigcap_{\alpha\in\Delta} A_\alpha\right) = \bigcap_{\alpha\in\Delta} (B \setminus A_\alpha).$$

Proposition 3.51. *If $\mathscr{A} = \{A_\alpha : \alpha \in \Delta\}$ is an indexed family of sets and B is a set, then*

$$\left(\bigcup_{\alpha\in\Delta} A_\alpha\right) \setminus B = \bigcup_{\alpha\in\Delta} (A_\alpha \setminus B).$$

Proposition 3.52. *If $\mathscr{A} = \{A_\alpha : \alpha \in \Delta\}$ is an indexed family of sets, then for each $\beta \in \Delta$*

$$\bigcap_{\alpha\in\Delta} A_\alpha \subseteq A_\beta.$$

Proposition 3.53. *If $\mathscr{A} = \{A_\alpha : \alpha \in \Delta\}$ is an indexed family of sets, then for each $\beta \in \Delta$*

$$A_\beta \subseteq \bigcup_{\alpha\in\Delta} A_\alpha.$$

Theorem 3.54 (DeMorgan's Laws : Full Version)**.** *Let* $\mathscr{A} = \{A_\alpha : \alpha \in \Delta\}$ *be an indexed family of sets.*

(i) $\widetilde{\bigcap_{\alpha\in\Delta} A_\alpha} = \bigcup_{\alpha\in\Delta} \widetilde{A_\alpha}$.

(ii) $\widetilde{\bigcup_{\alpha\in\Delta} A_\alpha} = \bigcap_{\alpha\in\Delta} \widetilde{A_\alpha}$.

Chapter 4

The Stuff of Legends

The definitions shall set you free.

This chapter is the primordial soup from which much of modern mathematics springs. Keep a lookout for the vestiges of some of your most familiar and cherished mathematical objects and savor the sensation of seeing with new eyes.

4.1 Products and Relations

Definition 4.1. Let A and B be sets. The *Cartesian product* of A and B is the set

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

Here, (a, b) represents an *ordered pair* and NOT the open interval from a to b.

Exercise 4.2. Let $A = \{\clubsuit, \heartsuit\}$ and $B = \{\square, \triangle, \sharp\}$. List the elements of $A \times B$.

Proposition 4.3. *Given sets A and B, $A \times B = B \times A$.*

It is natural to wonder how the set operation "$\times$" meshes with the set operations "$\cup$" and "$\cap$". The next propositions are a partial inquiry into this question. As always, it would be fruitful to conjecture and assess analogous statements with the roles of the set operations permuted.

Proposition 4.4. *Let A, B and C be sets. Then*

$$A \times (B \cap C) = (A \times B) \cap (A \times C).$$

Proposition 4.5. *Let A, B, C and D be sets. Then*

$$(A \times B) \cup (C \times D) = (A \cup C) \times (B \cup D).$$

Definition 4.6. Let A and B be sets. A *relation from A to B* is simply a subset of $A \times B$. If R is a relation from A to B and $(a, b) \in R$, then we write aRb and say "a is related to b."

Subsets of $A \times A$ are called *relations on A* (rather than "relations from A to A").

Example 4.7. Let $A = \{1, 2, 3\}$ and $B = \{\pi, 0, -1/2, \triangle\}$. The set

$$R = \{(1, \pi), (2, -1/2), (2, \triangle), (3, 0)\}$$

is a relation from A to B. Here $1R\pi$ but 3 is not related to $-1/2$. $\square$

Exercise 4.8. Consider the relation $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} : y - x \in [0, \infty)\}$. How is xRy more commonly written?

Definition 4.9. The *domain* of the relation R from A to B is the set

$$\mathrm{Dom}(R) = \{x \in A : (\exists y)(y \in B \wedge (x, y) \in R)\}$$

consisting of the "first entries" of ordered pairs in R.

The *range* of the relation R from A to B is the set

$$\mathrm{Ran}(R) = \{y \in B : (\exists x)(x \in A \wedge (x, y) \in R)\}$$

consisting of the "second entries" of ordered pairs in R.

Exercise 4.10. Define the relation C on $\mathbb{R}$ by

$$C = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x^2 + y^2 \leq 9\}.$$

(i) Determine $\mathrm{Dom}(C)$.

(ii) Determine $\mathrm{Ran}(C)$.

(iii) Viewing $\mathbb{R} \times \mathbb{R}$ as the good old xy-plane, draw the set C, labeling one specific pair $(x, y) \in C$ and one specific pair $(x, y) \in \widetilde{C}$.

Exercise 4.11. Determine the domain and range of the relation H from $\mathbb{R}$ to $[-5, \infty)$ given by

$$H = \{(x, y) \in \mathbb{R} \times [-5, \infty) : xy = 1\}.$$

Definition 4.12. Let A be a set. The relation $I_A = \{(x, x) \in A \times A : x \in A\}$ is called *the identity relation on* A. Note that by definition $\text{Dom}(I_A) = \text{Ran}(I_A) = A$.

Exercise 4.13. Revisiting the relations C and H of Exercises 4.10 and 4.11, draw each of the following sets in the xy-plane:

(i) $I_{\mathbb{R}}$;

(ii) $I_{\mathbb{R}} \cup C$;

(iii) $C \cap H$.

4.2 New Relations From Old

Definition 4.14. Let R be a relation from A to B. The *inverse* of R is the relation

$$R^{-1} = \{(y, x) \in B \times A : (x, y) \in R\}.$$

Note that R^{-1} is a relation from B to A.

Theorem 4.15. *Let R be a relation from A to B.*

(i) $Dom(R^{-1}) = Ran(R)$.

(ii) $Ran(R^{-1}) = Dom(R)$.

Exercise 4.16. Determine the inverse relation of the relation C of Exercise 4.10. Sketch it as a subset of $\mathbb{R} \times \mathbb{R}$.

Exercise 4.17. Determine the inverse relation of the relation H of Exercise 4.11. Sketch it as a subset of $\mathbb{R} \times \mathbb{R}$.

Exercise 4.18. Determine the inverse relation to the relation S given by

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

Sketch it as a subset of $\mathbb{R} \times \mathbb{R}$.

When their domains and ranges match up appropriately, two relations can yield a third, *composite*, relation. The following definition makes this notion precise.

Definition 4.19. Let R be a relation from A to B and let S be a relation from B to C. The *composition* of R and S is the relation

$$S \circ R = \{(a,c) \in A \times C : (\exists b \in B)((a,b) \in R \wedge (b,c) \in S)\}.$$

Note that $S \circ R$ is a relation from A to C.

Exercise 4.20. Let $R = \{(1,5),(2,2),(3,4),(5,2)\}$ and $S = \{(2,4),(3,4),(3,1),(5,5)\}$ be relations on $\mathbb{N}$. Determine both $S \circ R$ and $R \circ S$.

Proposition 4.21. *If R is a relation from A to B and S is a relation from B to C, then $Dom(S \circ R) \subseteq Dom(R)$.*

Exercise 4.22. Construct a concrete example of relations R and S such that $\mathrm{Dom}(S \circ R) \neq \mathrm{Dom}(R)$.

It is natural to consider how inverse and composition relations interact with one another. The following theorem addresses this question.

Theorem 4.23. *Let A, B, C and D be sets. Let R be a relation from A to B, S a relation from B to C and T a relation from C to D.*

(a) $(R^{-1})^{-1} = R$.

(b) $T \circ (S \circ R) = (T \circ S) \circ R$.

(c) $I_B \circ R = R$ *and* $R \circ I_A = R$.

(d) $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$.

4.3 Equivalence Relations

There are two types of relations that stand head and shoulders above the rest both in their importance and their ubiquity. The first is the topic of this section; the second will occupy all of Chapter 5.

Definition 4.24. Let R be a relation on the set A. We call R an *equivalence relation* on A if R has the following three properties:

(i) If $a \in A$, then $(a,a) \in R$.	(Reflexivity)
(ii) If $(x,y) \in R$, then $(y,x) \in R$.	(Symmetry))
(iii) If $(x,y) \in R$ and $(y,z) \in R$, then $(x,z) \in R$.	(Transitivity)

Exercise 4.25. Check the following relations on $A = \{1, 2, 3\}$ for reflexivity, symmetry and transitivity.

(a) $R_1 = \{(1, 1), (1, 2), (2, 1)\}$.

(b) $R_2 = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3)\}$.

(c) $R_3 = \{(1, 2)\}$.

Exercise 4.26. Construct a relation R on $\{1, 2, 3\}$ that is reflexive and transitive, but not symmetric.

Proposition 4.27. *The relation R on $\mathbb{Z}$ defined by*

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

is an equivalence relation.

Proposition 4.28. *The relation S on $\mathscr{P}(\mathbb{R})$ defined by*

$$S = \{(A, B) \in \mathscr{P}(\mathbb{R}) \times \mathscr{P}(\mathbb{R}) : A \subseteq B\}$$

is an equivalence relation.

CAUTION 4.29. Out in the world of mathematics, we often use convenient shorthand to define relations. For example, one could succinctly define the relations R and S of the previous two exercises by

$$xRy \text{ iff } x^2 = y^2$$

and

$$ASB \text{ iff } A \subseteq B.$$

If you encounter this notation, feel free to translate it back into the more formal set notation. Probably you will come to appreciate the efficiency of the shorthand, but you'll always know what lurks beneath! $\square$

Given an equivalence relation on a set A, the elements of A can be "clumped together" according to mutual relation. For instance, if we define R on the set of all living people by xRy iff x and y have the same surname and then group all related people together, then the view from space would be quite something. We would see gigantic hoards of Smiths and Lees and Hernandezes alongside little tiny clumps of Retseks, McGillicuddys and Obamas.

This act of "clumping" by mutual relation is formalized in the following definition.

Definition 4.30. Let R be an equivalence relation on the set A. For each $x \in A$, the *equivalence class* of x determined by R is the set

$$x/R = \{y \in A : (x, y) \in R\}.$$

The symbol x/R is read "the equivalence class of x modulo R" or, more concisely, "x mod R". The set of all the different equivalence classes is called A *modulo* R and is written

$$A/R = \{x/R : x \in A\}.$$

Note that A/R is a set of sets.

To illustrate the idea of equivalence classes, we take an important example that you will encounter again in your future number theory and/or abstract algebra classes.

Example 4.31. Let $m \in \mathbb{Z}$ with $m \neq 0$. Define the relation $\equiv_m$ on $\mathbb{Z}$ by

$$\equiv_m = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : m \text{ divides } (x - y)\}.$$

In our shorthand, we might write

$$x \equiv_m y \text{ iff } m \text{ divides } (x - y).$$

Another common notation for $x \equiv_m y$ is

$$x \equiv y \pmod{m}.$$

Either way, the statement $x \equiv_m y$ is read "x is congruent to y modulo m."

Theorem 4.32. *For each $m \in \mathbb{Z} \setminus \{0\}$, the relation $\equiv_m$ is an equivalence relation.*

Exercise 4.33. Determine the set $3/\equiv_4$.

Exercise 4.34. Determine the set $\mathbb{Z}/\equiv_7$. What does this set of "clumps" look like from space?

Proposition 4.35. *Let $m \in \mathbb{Z} \setminus \{0\}$. If $a \equiv_m b$ and $c \equiv_m d$, then $(a+c) \equiv_m (b+d)$.*

Exercise 4.36. Conjecture and assess a statement for modular multiplication analogous to the preceding proposition.

The "clumping" into disjoint equivalence classes that we have observed in specific examples is a general principle that is the very essence of equivalence relations. This idea is summarized in the following theorem.

Theorem 4.37. *Let R be an equivalence relation on the set A.*

(a) For each $x \in A$, $x \in x/R$.

(b) $A = \bigcup_{x \in A} x/R$.

(c) $(x, y) \in R$ iff $x/R = y/R$.

(d) $(x, y) \notin R$ iff $x/R \cap y/R = \emptyset$.

The content of Theorem 4.37 is summarized in Figure 4.1. Every equivalence relation R on a set A breaks A into disjoint equivalence classes of mutually related elements in A.

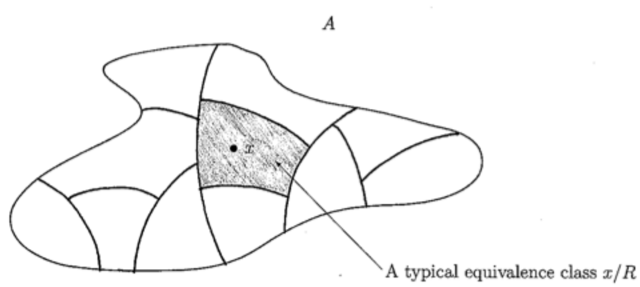


Figure 4.1: The set A broken into disjoint equivalence classes.

It turns out that Theorem 4.37 is actually a two way street: not only does every equivalence relation on a set A break A into a number of disjoint pieces, but every breaking of A into disjoint pieces gives rise to an equivalence relation. We need some terminology in order to lend precision to this assertion.

Definition 4.38. Let A be a set and $\mathscr{A}$ a family of subsets of A. We call $\mathscr{A}$ a *partition* of A if

(a) Every member of $\mathscr{A}$ is nonempty.

(b) If X and Y in $\mathscr{A}$ are distinct, then $X \cap Y = \emptyset$.

(c) $A = \bigcup_{X \in \mathscr{A}} X$.

Example 4.39. The family $\mathscr{A} = \{(-\infty, 0], (0, \infty)\}$ is a partition of $\mathbb{R}$ into two infinite rays.

Exercise 4.40. Construct a partition $\mathscr{A}$ of the real numbers $\mathbb{R}$ into infinitely many disjoint sets.

We are now able to prove the companion result to Theorem 4.37. Namely, every partition of a set A gives rise to an equivalence relation having exactly that partition as its equivalence classes.

Theorem 4.41. *Let $\mathscr{A}$ be a partition of the nonempty set A. Define the relation Q on A by*

$$Q = \{(x, y) \in A \times A : (\exists C \in \mathscr{A})(x \in C \wedge y \in C)\}.$$

Then

(a) Q is an equivalence relation on A.

(b) $A/Q = \mathscr{A}$.

Chapter 5

The Promised Land

I am the master of my fate: I am the captain of my soul.

From Invictus*, by William Ernest Henley*

This chapter is devoted to the concept of function, king of all relations. The fact that you have experience with functions can be a double-edged sword. Certainly there is comfort in familiarity, but comfort has a way of morphing into complacency. Let us maintain the formal stance that has taken us this far, allowing the theory to enhance our understanding without replacing it.

5.1 Functions

Functions are a particular type of relation.

Definition 5.1. Let f be a relation from A to B. We call f a *function from A to B* and write $f : A \to B$ if f has the following two properties:

(i) $\mathrm{Dom}(f) = A$.

(ii) $[\ (x, y) \in f \wedge (x, z) \in f\ ] \Rightarrow y = z$.

The set B is called the *codomain* of the function.

Exercise 5.2. Let $A = \{1, 2, 3\}$ and $B = \{6, \pi, -1, 13\}$. Determine which of the following relations are functions from A to B.

(i) $f_1 = \{(1, \pi), (2, 6), (3, 6), (2, -1)\}$

(ii) $f_2 = \{(1, -1), (2, \pi), (3, \pi)\}$

(iii) $f_3 = \{(1, 6), (3, -1)\}$

Exercise 5.3. Recall the relation $C = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x^2 + y^2 \leq 9\}$ of Exercise 4.10. Is C a function from $[-3, 3]$ to $\mathbb{R}$?

Exercise 5.4. Is the relation $D = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x^2 + y^2 = 9\}$ a function from $[-3, 3]$ to $\mathbb{R}$?

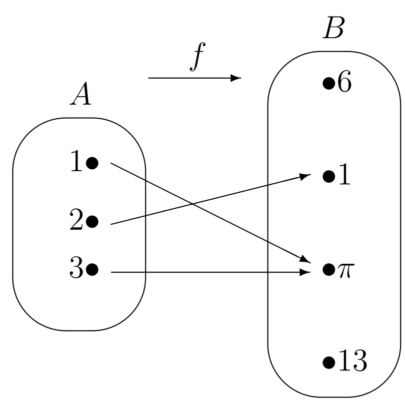
Exercise 5.5. Is the relation $E = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x^2 + y^2 = 9 \text{ and } y \geq 0\}$ a function from $[-3, 3]$ to $\mathbb{R}$?

Exercise 5.6. In light of the preceding three exercises, what graphical "rule of thumb" from your past is condition (ii) in Definition 5.1 the formal version of?

Example 5.7. It is sometimes helpful to think of a function as a dynamic object, as something that *happens to* each element in the domain. For instance, we could depict the function

$$f = \{(1, \pi), (2, 1), (3, \pi)\}$$

from $A = \{1, 2, 3\}$ to $B = \{6, \pi, 1, 13\}$ as the following "mapping" that shows where each element of the domain $A = \{1, 2, 3\}$ gets "sent":



$\square$

The dynamic view of functions motivates the following terminology.

Definition 5.8. Let $f : A \to B$. If $(a, b) \in f$, we write $f(a) = b$ and say that "b is the *image* of a under f" or that "b is the *value* of f at a."

Exercise 5.9. Referring to Example 5.7, address the following questions.

(i) What is the image of 1 under f?

(ii) What is the value of f at 3?

(iii) What is 13 the image of under f?

(iv) What is the range of f?

Proposition 5.10. *Let A be a set. The identity relation I_A is a function from A to A.*

Exercise 5.11. Let $f : \mathbb{R} \to \mathbb{R}$ be the function $f = \{(x, 3) \in \mathbb{R} \times \mathbb{R} : x \in \mathbb{R}\}$. Every element in the domain has the same image: $f(x) = 3$. This is an example of a *constant function*.

Give a representation of this function f both as a mapping diagram like in Example 5.7 and in the old fashioned precalculus way by drawing its graph in the xy-plane.

Exercise 5.12. Let U be some universe and $A \subseteq U$. Let $\chi_A : U \to \{0, 1\}$ be the function

$$\chi_A(x) = \begin{cases} 1 & \text{if } x \in A, \\ 0 & \text{if } x \in U \setminus A. \end{cases}$$

The function χ_A is called the *characteristic function* of the set A

(i) Give a representation of this function f as a mapping diagram.

(ii) If $U = \mathbb{R}$ and $A = (1, 3]$, give a representation of χ_A by drawing its graph in the xy-plane.

The first big theorem of the chapter says that two functions are equal if and only if they have the same domain and do the same thing to each element in that common domain. In our former lives, we might have accepted this as self-evident. But we are no longer innocent, we have lifted the veil; these words have precise meaning and we have no recourse but to adhere to our own definitions.

Theorem 5.13. *Two functions f and g are equal if and only if*

(i) Dom(f) = Dom(g), and

(ii) For each $x \in$ Dom(f), $f(x) = g(x)$.

5.2 New Functions From Old

In Section 4.2 we examined two important ways new relations arise from old: through composition and inverse. Since functions are just special types of relations, both constructions apply here as well.

Example 5.14. Let $f : \mathbb{R} \to \mathbb{R}$ be given by $f(x) = e^x$ and $g : \mathbb{R} \to \mathbb{R}$ be given by $g(x) = x^2$. In the formal sense of these functions as sets of ordered pairs,

$$f = \{(x, y) \in \mathbb{R} \times \mathbb{R} : y = e^x\}$$

and

$$g = \{(u, v) \in \mathbb{R} \times \mathbb{R} : v = u^2\}.$$

So by Definition 4.19, the composition $g \circ f$ is the relation

$$\begin{aligned} g \circ f &= \{(a, c) \in \mathbb{R} \times \mathbb{R} : (\exists b \in \mathbb{R})((a, b) \in f \wedge (b, c) \in g)\} \\ &= \{(a, c) \in \mathbb{R} \times \mathbb{R} : (\exists b \in \mathbb{R})(b = e^a \wedge c = b^2)\} \\ &= \{(a, c) \in \mathbb{R} \times \mathbb{R} : c = (e^a)^2\} \\ &= \{(a, c) \in \mathbb{R} \times \mathbb{R} : c = e^{2a}\} \end{aligned}$$

That is, $(g \circ f)(x) = e^{2x}$. □

Exercise 5.15. Mimic Example 5.14 and compute $f \circ g$ for those same two functions.

In the preceding example and exercise, both $g \circ f$ and $f \circ g$ turned out to be themselves functions. The following theorem indicates that this is a general phenomenon. That $g \circ f$ is itself a *relation* follows from Definition 4.19 and is not at issue here; the strength of the theorem is the assertion that $g \circ f$ is itself a *function* from A to C.

Theorem 5.16. *If $f : A \to B$ and $g : B \to C$, then $g \circ f : A \to C$.*

Function composition has well-behaved algebraic properties too.

Theorem 5.17. *If $f : A \to B$, $g : B \to C$ and $h : C \to D$, then $h \circ (g \circ f) = (h \circ g) \circ f$.*

Theorem 5.18. *If $f : A \to B$, then $f \circ I_A = f$ and $I_B \circ f = f$.*

As with composition, we are free to form the inverse relation f^{-1} any time we encounter a function $f : A \to B$.

Exercise 5.19. Show that the inverse relation f^{-1} to the function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = 2x^2 + 1$ is not itself a function.

CAUTION 5.20. As Exercise 5.19 illustrates, a function's inverse relation need not be itself a function. To repeat:

> Writing the symbol f^{-1} DOES NOT imply that the function f is "invertible" or that the relation f^{-1} is a function.

This is a common mistake that is to be vigilantly avoided.

5.3 1-1 and Onto Functions

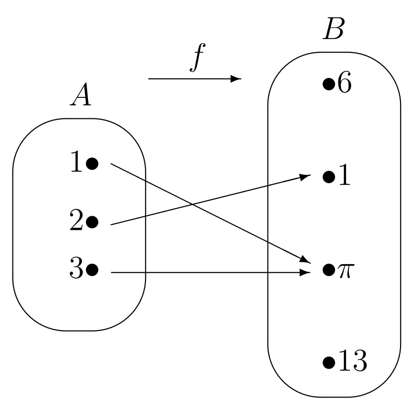
In light of Exercise 5.19 and the subsequent vigorous caution, it is natural to ask "Okay, fine, so when *is* f^{-1} a function?" To fully address this question we first need some terminology.

Definition 5.21. Let $f : A \to B$. The function f is called *one-to-one* if

$$(\dagger) \qquad [\ f(x) = y \text{ and } f(z) = y\ ] \Rightarrow x = z.$$

The phrase "one-to-one" is often shortened to "1-1". One-to-one functions are also called *injections.*

Example 5.22. Recall the function $f : \{1, 2, 3\} \to \{6, \pi, 1, 13\}$ from Example 5.7 given by



Note that both $f(1) = \pi$ and $f(3) = \pi$ despite $1 \neq 3$, violating the definition of one-to-one.

Our mapping diagrams give a nice dynamic sense of what it means to be one-to-one: the function $f : A \to B$ is 1-1 if and only if each element of the domain A "gets sent" to a different element in the codomain B. Since, in this example, 1 and 3 on the left both get sent to π on the right, this function f is not 1-1. $\square$

Exercise 5.23. Show that $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = \sin(x)$ is not 1-1.

Exercise 5.24. Find a domain $A \subset \mathbb{R}$ such that the function $f : A \to \mathbb{R}$ given by $f(x) = \sin(x)$ is 1-1.

Exercise 5.25. What graphical "rule of thumb" from your past is condition $(\dagger)$ in Definition 5.21 the formal version of?

Proposition 5.26. *If $f : A \to B$ and $g : B \to C$ are both 1-1, then $g \circ f : A \to C$ is 1-1.*

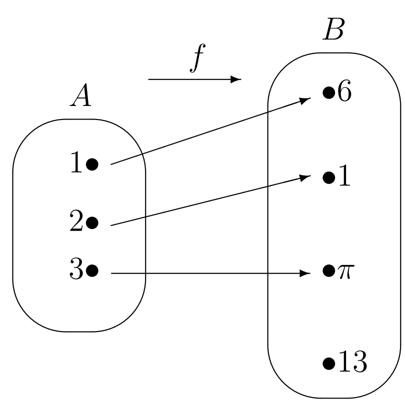
Proposition 5.27. *If $g \circ f : A \to C$ is 1-1, $f : A \to B$ and $g : B \to C$, then $g : B \to C$ is 1-1.*

Proposition 5.28. *If $g \circ f : A \to C$ is 1-1, $f : A \to B$ and $g : B \to C$, then $f : A \to B$ is 1-1.*

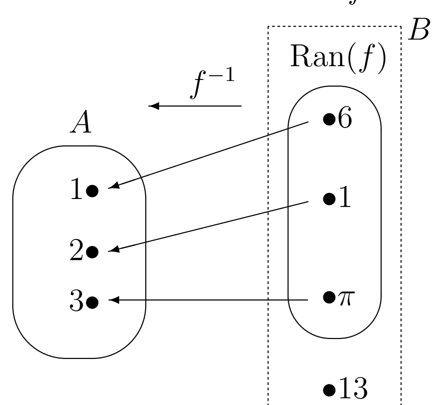
Given $f : A \to B$, we can now characterize exactly when the inverse relation f^{-1} is itself a function.

Theorem 5.29. *Let $f : A \to B$. Then $f^{-1} : Ran(f) \to A$ if and only if f is 1-1.*

Example 5.30. Theorem 4.15 guaranteed that $\mathrm{Dom}(f^{-1}) = \mathrm{Ran}(f)$ long before we ever discussed 1-1 functions. The big deal about a function f being one-to-one is that the inverse f^{-1} is not merely a relation, but a function in its own right. As always, our mapping diagrams give a nice visual. If $f : A \to B$ is given by



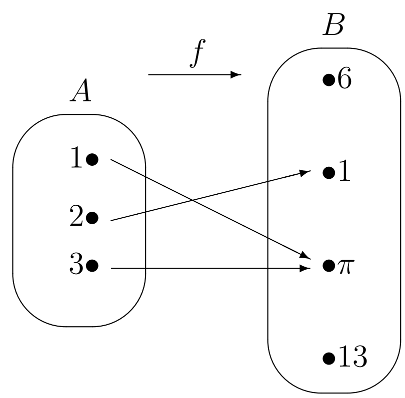
then $f^{-1} : \mathrm{Ran}(f) \to A$ "reverses" the action of f



$\square$

Definition 5.31. Let $f : A \to B$. The function f is called *onto* if $\operatorname{Ran}(f) = B$. Onto functions are also called *surjections*.

Example 5.32. Again recall the function $f : \{1, 2, 3\} \to \{6, \pi, 1, 13\}$ from Example 5.7 given by



Now revisit our answer to Exercise 5.9(iii). The value $13 \in B$ is not the image of anything in A, i.e. $13 \notin \operatorname{Ran}(f)$ and therefore f is not onto.

Our mapping diagrams give a nice informal and intuitive feeling for what it means for a function to be onto: the function $f : A \to B$ is onto if and only if everything in B "gets hit" by something from A. $\square$

Exercise 5.33. Show that $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = \cos(x)$ is not onto.

Exercise 5.34. Find a codomain $B \subset \mathbb{R}$ such that the function $f : \mathbb{R} \to B$ given by $f(x) = \cos(x)$ is onto.

Proposition 5.35. *If $f : A \to B$ and $g : B \to C$ are both onto, then $g \circ f : A \to C$ is onto.*

Proposition 5.36. *If $g \circ f : A \to C$ is onto, $f : A \to B$ and $g : B \to C$, then $g : B \to C$ is onto.*

Proposition 5.37. *If $g \circ f : A \to C$ is onto, $f : A \to B$ and $g : B \to C$, then $f : A \to B$ is onto.*

Exercise 5.38. Exhibit a specific function $f : \mathbb{R} \to \mathbb{R}$ that is 1-1, but not onto.

Exercise 5.39. Exhibit a specific function $f : \mathbb{R} \to \mathbb{R}$ that is onto, but not 1-1.

Exercise 5.40. Exhibit a specific function $f : \mathbb{R} \to \mathbb{R}$ that is neither 1-1 nor onto.

Exercise 5.41. Exhibit a specific function $f : \mathbb{R} \to \mathbb{R}$ that is both 1-1 and onto.

Functions that are both 1-1 and onto are prized for their nice properties, and we have a special name for them.

Definition 5.42. A function $f : A \to B$ is called a *bijection* if it is 1-1 and onto.

A bijection and its inverse function interact naturally.

Theorem 5.43. *If $f : A \to B$ is a bijection, then $f^{-1} : B \to A$ is a bijection.*

Theorem 5.44. *Let $f : A \to B$ and $g : B \to A$. Then $g = f^{-1}$ if and only if $g \circ f = I_A$ and $f \circ g = I_B$.*

The essence of Theorems 5.43 and 5.44 is that a bijection and its inverse are two sides of the same coin: each undoes what the other does. Figure 5.1 is a representation of this symbiosis.

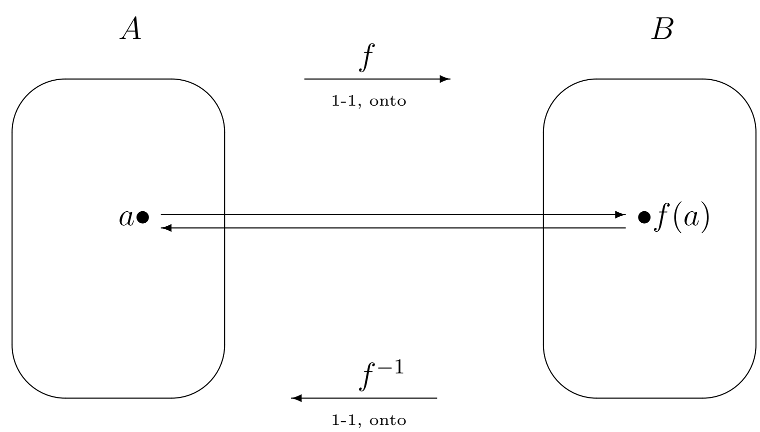


Figure 5.1: The dynamics of a bijection $f : A \to B$ and its inverse.

5.4 Set Images

Given $f : A \to B$, we already know what we mean when we say "What is the image of the element $a \in A$ under the function f?" We would like to extend this question to ask for the image of an entire subset of the domain A under the function f.

Definition 5.45. Let $f : A \to B$ and $X \subseteq A$. The *image* of the subset X is the set

$$f(X) = \{f(x) \in B : x \in X\}.$$

Figure 5.2 illustrates the set image $f(X)$. It is literally the set of all images of elements of X.

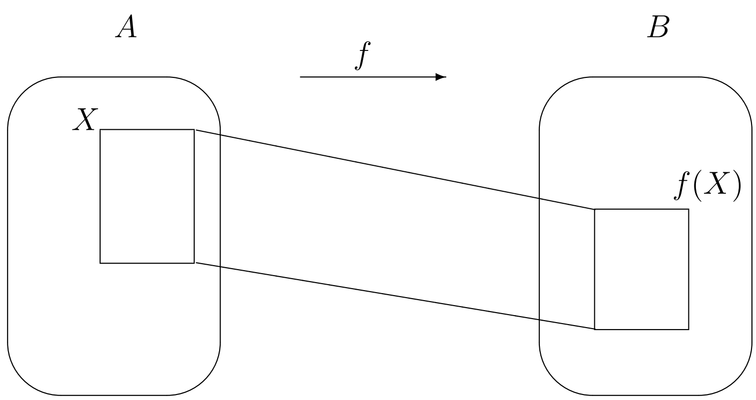


Figure 5.2: The set image $f(X)$ under $f : A \to B$.

Exercise 5.46. Let $f : \mathbb{R} \to \mathbb{R}$ be given by $f(x) = -2x + 7$. Determine each of the following set images:

(i) $f((-1, 3])$

(ii) $f(\mathbb{R})$

(iii) $f(\mathbb{Z})$

The set image $f(X)$ is part of the range of f. There is a natural companion idea on the domain side of things. Namely, given $f : A \to B$ and a subset $Y \subseteq B$, why not ask "What elements in A have their images in Y?"

Definition 5.47. Let $f : A \to B$ and $Y \subseteq B$. The *preimage* of the subset Y is the set

$$f^{-1}(Y) = \{x \in A : f(x) \in Y\}.$$

Figure 5.3 illustrates the preimage $f^{-1}(Y)$. It is literally the set of all domain elements whose images end up in Y.

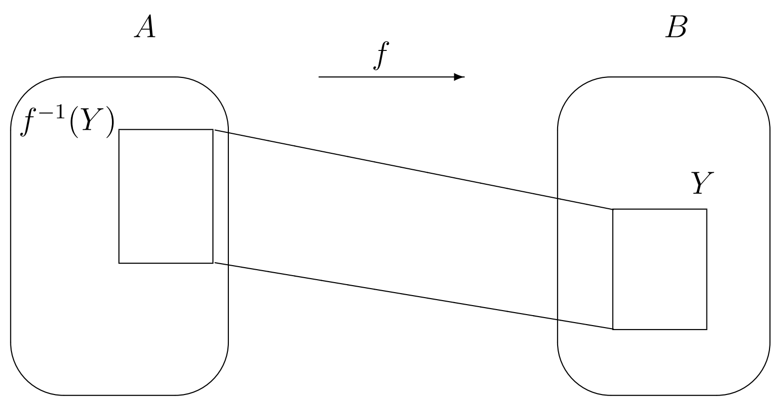


Figure 5.3: The preimage $f^{-1}(Y)$ under $f : A \to B$.

CAUTION 5.48. Figures 5.2 and 5.3 look awfully similar, but they come from vastly different perspectives.

(i) $f(X)$ answers the question "Where do things in X end up?"

(ii) $f^{-1}(Y)$ answers the question "What things end up in Y?"

CAUTION 5.49. In the definition of preimage $f^{-1}(Y)$, there is no requirement whatsoever that the function f be 1-1. We therefore must not interpret the symbol f^{-1} as suggesting that f has an inverse function. It's just notation, ink on a page, nothing more and nothing less. Adhere to Definition 5.47 for best results!

Exercise 5.50. Let $f : \mathbb{R} \to \mathbb{R}$ be given by $f(x) = x^2$. Determine the following set images and preimages.

(a) $f(\{1, 2, 3\})$

(b) $f([0, 2])$

(c) $f^{-1}(\{4\})$

(d) $f^{-1}([0, 4))$

(e) $f((-3, -2])$

(f) $f^{-1}(f((-3, -2]))$

(g) $f^{-1}((-4, 1]))$

(h) $f(f^{-1}((-4, 1])))$

What we have just observed in Exercise 5.50 can be stated in some generality.

Theorem 5.51. *If $f : A \to B$ and $E \subseteq B$, then $f(f^{-1}(E)) \subseteq E$.*

Exercise 5.52. Discover and prove a theorem characterizing when $f(f^{-1}(E)) = E$. It should read something like:

> **Theorem.** Let $f : A \to B$ and $E \subseteq B$. The equality $f(f^{-1}(E)) = E$ holds if and only if "something about E."

Theorem 5.53. *If $f : A \to B$ and $D \subseteq A$, then $D \subseteq f^{-1}(f(D))$.*

Exercise 5.54. Discover and prove a sufficient condition for $D = f^{-1}(f(D))$.

Now that we have made the leap from images and primages of particular elements to images and preimages of entire sets, it is natural to go one step further and consider images and preimages of unions and intersections of entire families of sets.

This is a culminating moment for us. As you prove the following theorem, imagine confronting it weeks ago; proving it would have been out of the question and even reading it might have been a challenge. We have come some way in these weeks and you should relish in your achievement.

Theorem 5.55. *Let $f : A \to B$. Let $\{D_\alpha : \alpha \in \Delta\}$ be a family of subsets of A and let $\{E_\beta : \beta \in \Gamma\}$ be a family of subsets of B.*

(i) $$f\left(\bigcap_{\alpha\in\Delta} D_\alpha\right) \subseteq \bigcap_{\alpha\in\Delta} f(D_\alpha).$$

(ii) $$f\left(\bigcup_{\alpha\in\Delta} D_\alpha\right) = \bigcup_{\alpha\in\Delta} f(D_\alpha).$$

(iii) $$f^{-1}\left(\bigcap_{\beta\in\Gamma} E_\beta\right) = \bigcap_{\beta\in\Gamma} f^{-1}(E_\beta).$$

(iv) $$f^{-1}\left(\bigcup_{\beta\in\Gamma} E_\beta\right) = \bigcup_{\beta\in\Gamma} f^{-1}(E_\beta).$$

Appendix A

Induction

Recall that $\mathbb{N} = \{1, 2, 3, \ldots\}$ is the set of natural numbers. The natural numbers enjoy the following essential properties:

(1) $1 \in \mathbb{N}$.
(2) If $x \in \mathbb{N}$, then x has a unique *successor* $x + 1 \in \mathbb{N}$.
(3) 1 is not the successor of any natural number.
(4) If x and y have the same successor, then $x = y$.
(5) If $S \subseteq \mathbb{N}$ satisfies
  (i) $1 \in S$;
  (ii) $\forall k \in \mathbb{N}$, $k \in S \Rightarrow k + 1 \in S$,
 then $S = \mathbb{N}$.

Properties (1)-(5) above are axioms. They are independent of one another and cannot be proven. They are essential in the sense that any other set N' having these properties is equivalent to $\mathbb{N}$. As Shakespeare might say, "An $\mathbb{N}$ by any other name would smell as sweet."

Using these properties of $\mathbb{N}$ and the tools in this book, one can build much of the whole rich structure of mathematics from scratch. Of present interest, however, is property (5), which is called The Principle of Mathematical Induction (PMI).

<u>The Principle of Mathematical Induction (PMI)</u>

If $S \subseteq \mathbb{N}$ satisfies
  (i) $1 \in S$;
  (ii) $\forall k \in \mathbb{N}$, $k \in S \Rightarrow k + 1 \in S$,
then $S = \mathbb{N}$.

Exercise A.1. Write the PMI without employing a single mathematical symbol.

Exercise A.2. Write the PMI employing only mathematical symbols.

Suppose $P(n)$ is some open sentence involving $n \in \mathbb{N}$ and we wish to prove the quantified proposition $\forall\, n \in \mathbb{N}, P(n)$. One option is to attempt a direct proof along the lines of Table 2.7: consider an arbitrary element $n \in \mathbb{N}$ and show $P(n)$ holds.

The PMI affords a second option. Rather than directly proving $P(n)$ for an arbitrary $n \in \mathbb{N}$, we let

$$S = \{n \in \mathbb{N} : P(n) \text{ is true}\}$$

be the set of natural numbers for which $P(n)$ is true, show that S meets conditions (i) and (ii) of the PMI, and conclude that $S = \mathbb{N}$, i.e. $P(n)$ is true for *all* natural numbers. Table A.1 illustrates the structure of such a proof by induction.

Proof. Let $S = \{n \in \mathbb{N} : P(n) \text{ is true}\}$.
•
•
•
Therefore S meets condition (i) of the PMI.
•
•
•
Therefore S meets condition (ii) of the PMI.
Thus, $S = \mathbb{N}$ by the PMI. $\square$

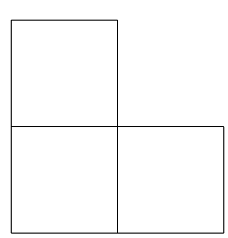
Table A.1: Proof of $\forall\, n \in \mathbb{N}, P(n)$ by Induction.

Proposition A.3. *For each* $n \in \mathbb{N}$,

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

Proposition A.4. *For each* $n \in \mathbb{N}$, $3^n \geq 1 + 2^n$.

Definition A.5. A *triomino* is the L-shape obtained by removing a square from a 2×2 square grid:



Proposition A.6. *For each $n \in \mathbb{N}$, a $2^n \times 2^n$ chess board with one square missing can be covered exactly with non-overlapping triominos.*

Proposition A.7. *For each $n \in \mathbb{N}$, $2^n > n^2$.*

Exercise A.8. Develop a "Generalized PMI" suitable for use on a salvaged Proposition A.7.

Exercise A.9. Determine the set of natural numbers for which $(n+1)! > 2^{n+3}$ and prove your result.

The Principle of Complete Induction allows a stronger inductive hypothesis to obtain the same result.

> The Principle of Complete Induction (PCI)
>
> If $S \subseteq \mathbb{N}$ satisfies
> $(\star)$ $\forall n \in \mathbb{N}$, $[\,\{k \in \mathbb{N} : k < n\} \subseteq S\,] \Rightarrow n \in S$,
> then $S = \mathbb{N}$.

Exercise A.10. Write the PCI without employing a single mathematical symbol.

Exercise A.11. Write the PCI employing only mathematical symbols.

The use of the PCI is often called *strong induction* because the induction hypothesis that *all* naturals less than n are in S is much stronger than the PCI induction hypothesis that the natural *immediately preceding* n is in S.

Exercise A.12. Let $a_1 = 2$, $a_2 = 4$ and $a_n = 5a_{n-1} - 6a_{n-2}$ for $n \geq 3$. Determine an explicit formula depending on n for the nth term a_n and prove that your formula holds for all $n \in \mathbb{N}$.

Exercise A.13. Develop a "Generalized PCI" analogous to your development in Exercise A.8.

One classic instantiation of strong induction deals with the idea of *prime factorization.*

Definition A.14. An integer $p > 1$ is called *prime* if the only positive integers that divide p are 1 and p itself.

Theorem A.15. *Every integer $p > 1$ can be expressed as a product of prime numbers.*

We conclude with a discussion bordering on meta-mathematics.

Exercise A.16. Suppose we have two propositions whose truth values are unknown to us:

Proposition 1. If P, then Q.

Proposition 2. If R, then S.

Write an outline of how we would prove the following

Theorem. If Proposition 1 is true, then Proposition 2 is true.

The PMI and the PCI are interchangeable in the sense that we could replace property (5) of the natural numbers, the PMI, with property (5′), the PCI, and the whole of mathematics would go unchanged. In other words, the PMI and the PCI are logically equivalent. That neither of them can be proven from properties (1)-(4) is immaterial; property (5′) follows from properties (1)-(5) and property (5) follows from properties (1)-(5′).

Let PMI* stand for axioms (1)-(5) and PCI* stand for axioms (1)-(4),(5′).

Theorem A.17. $PMI^* \Leftrightarrow PCI^*$.

There is a third utterly believable, but equally unprovable, property of the natural numbers that makes a triumvirate set of candidates for property (5). This one asserts that every nonempty set of naturals has a least member.

The Well Ordering Principle (WOP)
Every nonempty subset $S \subseteq \mathbb{N}$ has a least element.

Theorem A.18. $PMI^* \Leftrightarrow WOP$.

Note A.19. Rest assured that 99.9999% of mathematics is done in the world of PMI*. You should use the axioms without hesitation and expect to never meet anyone in earnest opposition.

Appendix B

Cardinality

Exercise B.1. Demonstrate to someone who can't count that you have the same number of fingers on each hand.

Despite its simplicity, Exercise B.1 is the kernel of one of the great ideas in modern mathematics. Namely, two sets are the "same size" precisely if we can pair all of their elements in one-to-one correspondence:

Definition B.2. Sets A and B have the *same cardinality*, written $|A| = |B|$, if there exists a bijection $f : A \to B$.

Exercise B.3. Show that $\{\clubsuit, \diamondsuit, \spadesuit, \heartsuit\}$ and $\{9, -\sqrt{2}, \pi, e\}$ have the same cardinality.

Exercise B.4. Show that $|(2, 3)| = |(-1, 4)|$.

Exercise B.5. Show that $|(0, 1]| = |[1, 3)|$.

Exercise B.6. Show that $|(0, 1)| = |\mathbb{R}|$.

Proposition B.7. *Every nonempty open interval in* $\mathbb{R}$ *has the same cardinality.*

Proposition B.8. *Let* $E = \{x \in \mathbb{Z} : x \text{ is even } \}$. *Then* $|E| = |\mathbb{Z}|$.

We are mainly interested in "infinite" sets.

Definition B.9. The set A is *infinite* if there exists a one-to-one function $f : \mathbb{N} \to A$. Otherwise, A is called *finite*.

Proposition B.10. *The set* A *is infinite if and only if* A *has a subset of the same cardinality as* $\mathbb{N}$.

Loosely, Proposition B.10 says that a set is infinite if and only if it is big enough to house a copy of $\mathbb{N}$ inside it. The flip side of this idea is that some sets are "small enough" to have a copy inside $\mathbb{N}$.

Definition B.11. The set A is called *countable* if there exists a one-to-one function $f : A \to \mathbb{N}$.

Proposition B.12. *The set* $A = \{9, -\sqrt{2}, \pi, e\}$ *is countable.*

Proposition B.13. *The set* $\mathbb{N}$ *is countable.*

Proposition B.14. *The set* $\mathbb{Z}$ *is countable.*

Proposition B.15. *If* A *is countable and* $B \subseteq A$*, then* B *is countable.*

Sets like $\mathbb{N}$ and $\mathbb{Z}$ that are both countable and infinite are called *countably infinite*. The next theorem asserts that all countably infinite sets have the same cardinality as $\mathbb{N}$.

Theorem B.16. *If* A *is countable, then* A *is finite or* $|A| = |\mathbb{N}|$.

Theorem B.16 says that there is only one "countable infinity", that of the natural numbers. Put another way, a set A is countably infinite if and only if it can be "listed":

$$A = \{a_1, a_2, a_3, \ldots\}.$$

This is most mathematicians' working sense of countably infinite sets. They're the ones that can be listed.

Exercise B.17. Draw a mapping diagram illustrating a natural bijection between $A = \{a_1, a_2, a_3, \ldots\}$ and $\mathbb{N}$.

As usual, we next consider how the set property of being countable interacts with intersections and unions.

Proposition B.18. *If* A *and* B *are countable, then* $A \cap B$ *is countable.*

Proposition B.19. *If* A *and* B *are countable, then* $A \cup B$ *is countable.*

Propositions B.18 and B.19 concern intersections and unions of two countable sets, but why stop there? What about three countable sets? Ten? Ten million? Countably infinitely many? The language of families of sets allows precise formulation of these questions.

Proposition B.20. *If $\{A_k : k \in \mathbb{N}\}$ is a countable family of countable sets, then $\bigcap_{k\in\mathbb{N}} A_k$ is countable.*

The analogous statement for countable unions requires a bit more care. We start with the following lemma, which reads as a slightly weaker statement than our ultimate goal (though they are in fact equivalent).

Lemma B.21. *If $\{A_k : k \in \mathbb{N}\}$ is a countable family of pairwise disjoint countable sets, then $\bigcup_{k\in\mathbb{N}} A_k$ is countable.*

Theorem B.22. *If $\{A_k : k \in \mathbb{N}\}$ is a countable family of countable sets, then $\bigcup_{k\in\mathbb{N}} A_k$ is countable.*

Remark B.23. Theorem B.22 may be paraphrased by "A countable union of countable sets is countable." When we run into each other ten years from now in the cereal aisle at the grocery store, this is something you will remember. □

Let us attempt to develop a line of inquiry for Cartesian products akin to that already developed for unions and intersections.

Proposition B.24. *If A and B are countable, then $A \times B$ is countable.*

What about larger products of finitely many countable sets?

Exercise B.25. Create a definition for the Cartesian product $A_1 \times A_2 \times \cdots \times A_N$ of finitely many sets that agrees with Definition 4.1 in the case $N = 2$.

Proposition B.26. *If $A_1, A_2, \ldots, A_N$ are finitely many countable sets, then the product $A_1 \times A_2 \times \cdots \times A_N$ is countable.*

The sets $\mathbb{Q}$ and $\mathbb{R}$ are both infinite by Proposition B.10. We are now in a position to decide whether or not they are countably infinite.

Theorem B.27. *The set $\mathbb{Q}$ of rational numbers is countably infinite.*

Considering that between any two natural numbers there are infinitely many rational numbers (can you prove this?), it is remarkable that $|\mathbb{Q}| = |\mathbb{N}|$. In fact, we are yet to establish that there are any *uncountable* sets at all!

In point of fact, examples of uncountable sets abound and there are several ways one can see this. We shall pursue two of these avenues, the first being a classic line of reasoning attributed to the father of modern set theory, Georg Cantor (1845-1918).

Exercise B.28. Determine a real number in the interval $(0,1)$ that is not on the following list:

$$\begin{aligned}
y_1 &= 0.y_{11}y_{12}y_{13}y_{14}y_{15}y_{16}y_{17}y_{18}y_{19}\cdots \\
y_2 &= 0.y_{21}y_{22}y_{23}y_{24}y_{25}y_{26}y_{27}y_{28}y_{29}\cdots \\
y_3 &= 0.y_{31}y_{32}y_{33}y_{34}y_{35}y_{36}y_{37}y_{38}y_{39}\cdots \\
y_4 &= 0.y_{41}y_{42}y_{43}y_{44}y_{45}y_{46}y_{47}y_{48}y_{49}\cdots \\
y_5 &= 0.y_{51}y_{52}y_{53}y_{54}y_{55}y_{56}y_{57}y_{58}y_{59}\cdots \\
y_6 &= 0.y_{61}y_{62}y_{63}y_{64}y_{65}y_{66}y_{67}y_{68}y_{69}\cdots \\
y_7 &= 0.y_{71}y_{72}y_{73}y_{74}y_{75}y_{76}y_{77}y_{78}y_{79}\cdots \\
y_8 &= 0.y_{81}y_{82}y_{83}y_{84}y_{85}y_{86}y_{87}y_{88}y_{89}\cdots \\
y_9 &= 0.y_{91}y_{92}y_{93}y_{94}y_{95}y_{96}y_{97}y_{98}y_{99}\cdots
\end{aligned}$$

Theorem B.29 (Cantor, 1874)**.** *The open interval* $(0,1)$ *is uncountable.*

Corollary B.30. *The set* $\mathbb{R}$ *of real numbers is uncountable.*

Corollary B.31. *The set* $\mathbb{I}$ *of irrational numbers is uncountable.*

In the sense of Corollary B.31, then, "most" real numbers are irrational. Naming them, however, is often hard to do; the proofs that π and e are irrational are modern and not so easy. You may encounter these in a class on real analysis.

Any urge to conclude that the infinitude of $\mathbb{R}$ is somehow the "biggest" infinity is squashed by the following theorem, due also to Cantor, comparing the size of a set to the size of its power set.

Theorem B.32. *No set has the same cardinality as its power set.*

Thus, in a spectacular abuse of notation, we have ultimately shown

$$|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| < |\mathbb{R}| < |\mathscr{P}(\mathbb{R})| < |\mathscr{P}(\mathscr{P}(\mathbb{R}))| < |\mathscr{P}(\mathscr{P}(\mathscr{P}(\mathbb{R})))| < \cdots$$

and must therefore conclude that there is no "biggest" infinity.

Bibliography

[1] Burger, E.B.. **Extending the Frontiers of Mathematics *Inquiries into Proof and Argumentation*** Key College Publishing, California 2007.

[2] Eggen, M., Smith, D., and St. Andre, R.. **A Transition to Advanced Mathematics** Thomson Brooks/Cole, California 2006.

[3] Freiwald, R.. **Point-Set Topology** Unpublished Course Notes, St. Louis, Missouri 1997.

[4] Solow, D.. **How to Read and Do Proofs *An Introduction to Mathematical Thought Processes*** John Wiley & Sons, New York 2002.