DANIEL GONZALEZ CEDRE

DISCRETE MATHEMATICS

UNIVERSITY OF NOTRE DAME

January 31, 2024

These notes are intended for students of CSE 20110 Discrete Mathematics at the University of Notre Dame.

https://daniel-gonzalez-cedre.github.io

Contents

Notation

SYNTAX		SEMANTICS
$\top$	*"True."*	A *true* sentence; a tautology.
$\bot$	*"False."*	A *false* sentence; a contradiction.
$x \coloneqq y$	*"x is, by definition, y."*	The name x has been assigned to the object referenced by y.
$x = y$	*"p equals q."*	p and q refer to the same object.
$p \equiv q$ $p \Leftrightarrow q$	*"p is equivalent to q."* *"p if, and only if, q."*	The sentence p is logically equivalent to the sentence q.
$p \vdash q$ $p \Rightarrow q$	*"p proves q."* *"p implies q."*	By assuming the sentence p, we can prove the sentence q.
$\varnothing$	*"The empty set."*	The set containing no elements.
$\{a, b, c\}$	*"The set containing a, b, and c."*	The object whose elements are a, b, c.
$\{x \mid \varphi(x)\}$	*"The set of all x such that $\varphi(x)$."*	The object whose elements consist of all possible objects x for which the sentence $\varphi(x)$ is *true*.
$\{x \in \mathcal{A} \mid \varphi(x)\}$	*"The set of all x in $\mathcal{A}$ such that $\varphi(x)$."*	The object consisting of all x from $\mathcal{A}$ for which the sentence $\varphi(x)$ is *true*.
$f : \mathcal{A} \to \mathcal{B}$	*"f is a function from $\mathcal{A}$ to $\mathcal{B}$."*	A function named f with domain $\mathcal{A}$ and codomain $\mathcal{B}$.
$f(x)$	*"f of x."*	The output of f on the input x, where $x \in \mathcal{A}$ and $f(x) \in \mathcal{B}$.
$\mathbb{N}$	*"enn"*	The set of natural numbers.
$\mathbb{Z}$	*"zee"*	The set of integers.
$\mathbb{Q}$	*"queue"*	The set of rational numbers.
$\mathbb{R}$	*"arr"*	The set of real numbers.

Table 1: An overview of some important notation. Note that some expressions, like $p \equiv q$ and $p \vdash q$, have more than one equivalent notation. The middle column gives some common ways of *reading* each notation in English. The last column provides the *meaning* of each expression.

COLOR	INTERPRETATION
	Emphasis
	Pronunciation
	Definition
	External link
	Internal link

Table 2: Color legend.

MARK	MEANING
定義	***definition***
直覺	***idea***
公理	***axiom***
引理	***lemma***
定理	***theorem***
推論	***corollary***
演算法	***algorithm***

Table 3: Notation for organizing topics.

GLYPH	NAME	IPA	GLYPH	NAME	IPA
$A\ \alpha$	*alpha*	[a]	$N\ \nu$	*nu*	[n]
$B\ \beta$	*beta*	[v]	$\Xi\ \xi$	*xi*	[ks]
$\Gamma\ \gamma$	*gamma*	[ɣ]	$O\ o$	*omicron*	[o]
$\Delta\ \delta$	*delta*	[ð]	$\Pi\ \pi$	*pi*	[p]
$E\ \varepsilon$	*epsilon*	[e]	$P\ \rho$	*rho*	[r]
$Z\ \zeta$	*zeta*	[z]	$\Sigma\ \sigma$	*sigma*	[s]
$H\ \eta$	*eta*	[ɛː]	$T\ \tau$	*tau*	[t]
$\Theta\ \theta$	*theta*	[θ]	$\Upsilon\ \upsilon$	*upsilon*	[yː]
$I\ \iota$	*iota*	[iː]	$\Phi\ \varphi$	*phi*	[f]
$K\ \kappa$	*kappa*	[k]	$X\ \chi$	*chi*	[k^h]
$\Lambda\ \lambda$	*lambda*	[l]	$\Psi\ \psi$	*psi*	[ps]
$M\ \mu$	*mu*	[m]	$\Omega\ \omega$	*omega*	[ɔː]

Table 4: The Greek alphabet.

Logic

0

Language

> *"No language is justly studied merely as an aid to other purposes. It will in fact better serve other purposes, philological or historical, when it is studied for love, for itself."*
>
> – J. R. R. Tolkien

We communicate our thoughts to others with the use of language. This is worth reflecting on. You are probably reading this because you have some interest in computation, mathematics, logic, or are incurably bored; the goal of these notes is—in part—to provide the mathematical background necessary to study these fields at a higher level. This is particularly true for aspiring *computer scientists,* who may have some misconceptions about their field because of its misleading name,[1] and who may not be aware that the field properly and historically falls under the grand umbrella of *mathematics.*

This ambitious undertaking must therefore involve engaging with the tumultuous and violent history of mathematics. Although modern computer science is now richly interdisciplinary, the field was born during a particularly turbulent period in the late 19th and early 20th centuries AD[2] agitated by an existential crisis in mathematics: a crisis caused by our flagrant use of language. Here's a short summary.

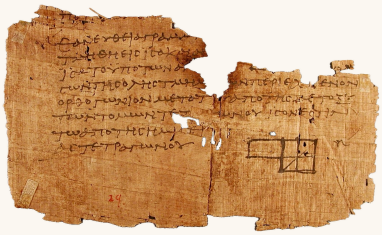

Figure 1: A fragment of book 2 from Euclid's *Elements* taken from the Oxyrhynchus papyri, dated ca. 100 AD.

[1] It's *not* about computers *nor* is it science.

[2] We will see later that its roots span at least to the time of Euclid in 300 BC.

0.1 A Brief History of...

The serious study of rhetoric—the art of argumentation and persuasion—as a subject in its own right dates back to at least the 5th century BC.[3] Around the 3rd century BC, Euclid's 13 books of the *Elements* heralded the birth of geometry, algorithmic computation, and the first theory of numbers,[4] where he *proved* certain statements followed from a list of *axiomatic* assumptions. This was a great achievement, establishing mathematical *proof* as a form of *argumentation* that logically deduces conclusions from a list of common assumptions. The contemporaneous Greek philosopher Theophrastus further pushed the envelope by describing the *form* of these arguments and establishing their validity.

[3] The time of the ancient Greek sophists, who were notably opposed by Socrates, Plato, and Aristotle.

[4] The only evidence of algorithms before this time—for multiplying, factoring, and finding square roots—dates back to Egypt and Babylon before 1600 BC.

The ancient Greeks laid the foundation for the two instrumental aspects of mathematical thought: *abstraction* and *argumentation*. Euclid abstracted what were thought to be the fundamental truths of geometry into a list of 12 *axioms*[1] so that, instead of thinking about *that* particular wall or *that* particular stick or *that* particular roof, he could make statements and observations about *quadrilaterals*, and *lines*, and *triangles* in general. These axioms were meant to encode the *universal truths* of geometry: the nature of what it fundamentally means to construct and measure distances, angles, and (simple) shapes. The last of these axioms would quickly become infamous.

axiom

[1] An *axiom* is a statement that we assume is true without justification nor proof.

Axiom (Parallel Postulate).
If two straight lines meet a third straight line making two interior angles that are each less than right angles, then the two lines—if they were to be extended—must intersect on that side where the interior angles are.
公理

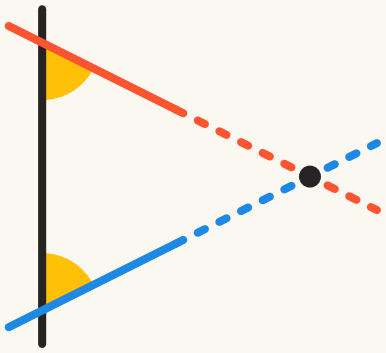

Figure 2: The parallel postulate says that any two lines and that make acute interior angles and with a third line must intersect at a point.

If you stop to think for a moment, this postulate says something very obvious. Assuming all of Euclid's other axioms, there are a few *equivalent* ways to restate the parallel postulate:

1. For any line L and point P not on L, there is exactly one line parallel to L passing through P.
2. The sum of interior angles in any triangle is 180 degrees.
3. A right triangle with side lengths A, B, C satisfies $A^2 + B^2 = C^2$.

You'll recognize this third statement as the Pythagorean *theorem*,[2] which is not merely an assumption![3] For the next 2000 years, the mathematical community was haunted by the thought that it was possible to *prove* the parallel postulate using the other axioms. It seemed like the rest of the axioms did such a perfectly good job of characterizing geometry that the parallel postulate *must necessarily* follow from the other axioms.

[2] A *theorem* is a statement that has a proof.

[3] The first two are called Playfair's axiom and the triangle postulate respectively.

However, between 1810–1832 AD, no less than *three* papers on *hyperbolic* geometry were published, and by 1854 Bernhardt Riemann had developed a theory of *Riemannian* geometry on manifolds. These were all different examples of consistent models of geometry that *denied* the parallel postulate! These ideas were intensely contested: many mathematicians and natural philosophers of the time refused to accept the notion that geometry could be non-Euclidean because *it went against their intuitive notion of how geometry should behave.*

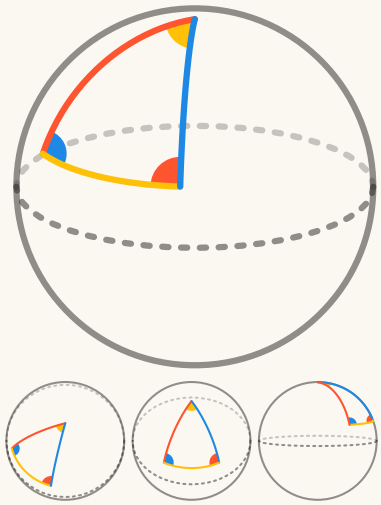

Figure 3: Four views of the same triangle whose angles sum to 270 degrees. Notice how the notions of *straight* and *parallel* differ on the surface of a sphere.

This whole ordeal was only foreshadowing what would come at the turn of the century. In 1874, Georg Cantor would make a series of discoveries[4] surrounding the nature of infinity so fundamentally opposed to common mathematical thought that he would be antagonized and

[4] We will study these later.

ostracized for decades, causing him to suffer serious depressive crises. Once again, mathematicians' *intuitive notions of how infinity should behave* were shown to be wrong. Cantor's discoveries sparked not only a civil war within the mathematical community but also a concerted effort by many mathematicians and logicians in the early 20th century to *fix* mathematics by establishing it on a firm *foundation*.

The cause of all this turmoil was, fundamentally, a *lack of precision and rigor* in the way people would communicate mathematical ideas and arguments. What does it *mean* for a line to be straight, or for two straight lines to be parallel? What does it *mean* to have two lines, or to have infinitely many lines? What *is* infinity? Is infinity a number? What *are* numbers? How do we *know* we are saying anything *true* at all?

If we hope to answer any of these questions, we must first develop a language for *precise* mathematical communication. This necessarily begins with a systematic deconstruction and analysis of *language* itself.

0.2 Syntax and Semantics

Languages encode ideas into sequences of symbols.[1] These symbols represent objects, ideas, actions, and concepts. The *meaning* behind a particular cluster of symbols is called its *semantics*. The *form* the language takes, dictated by its *grammatical rules* for composing symbols into valid sentences, is called its *syntax*. We refer to objects by giving them names. A *variable* is a symbol[2] that stands in place for an object that has not been determined yet.[3] We can assign name to a *particular* object with the $:=$ symbol. We call these the *terms* of an expression.

semantics

syntax

variable

term

[1] For our purposes, we will focus only on written—as opposed to spoken or signed—languages.

[2] We typically denote variables using single Latin or Greek letters, though there are no strict universal rules. Some common examples are listed below.

- $a, b, c, i, j, k, \ell, m, n, p, q, u, v, w, x, y, z$
- $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}, \mathcal{G}, \mathcal{H}, \mathcal{M}, \mathcal{N}, \mathcal{R}, \mathcal{X}, \mathcal{Y}, \mathcal{Z}$
- $\alpha, \beta, \gamma, \delta, \epsilon, \eta, \theta, \lambda, \mu, \pi, \sigma, \tau, \varphi, \psi, \omega$

[3] A variable does not *necessarily* refer one particular object, or even any object at all.

Definition* 0.1 *(Sentences).

sentence

atomic

A *sentence* is the expression of a complete thought or idea in accordance with the syntactic and grammatical rules of a given language. A statement is called *atomic* if it can't be broken down into smaller semantic components in any way that obeys the language's syntax and grammar.

1. A *declarative* sentence is one that describes something. They typically consist of a *subject* being described and a *predicate* property it has.
2. An *interrogative* sentence asks a non-rhetorical question.
3. An *imperative* sentence heralds a command or request.

"Oft hope is born when all is forlorn."

"What has it got in its pocketses?"

"Keep your forked tongue behind your teeth."

Mathematical practice principally involves *making and justifying observations about mathematical objects*.[4] As such, we are only really interested in crafting *declarative* sentences—sentences that describe *terms*. We will systematically deconstruct and analyse these kinds of sentences, extract their *logical essence*, and build up a new language.

[4] We leave the problem of *what* a mathematical object actually *is* for later.

0.3 A Recurring Theme

Before going any further, we should make a brief detour to discuss a topic that lies at the *heart* of computing, logic, and the 20th century foundational crisis in mathematics: *recursion*. In a very strong sense, what we *mean* when we say that some *thing* is *computable* is that there is a *recursive procedure* that produces that *thing*.

Idea (Church-Turing Thesis).
We say something is *computable* if it is expressible as a *general recursive process*, is a *term in the λ-calculus*, or could described by a *Turing machine*.

範例

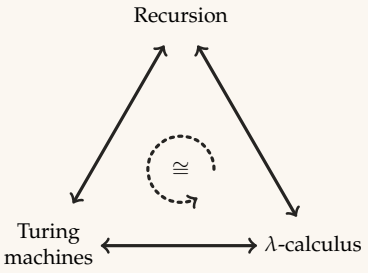

Figure 4: The Church-Turing thesis states that these three concepts—which are all *formally* equivalent—correspond with our *informal* notion of computability. In modern times, many people now take this as a definition for computability.

[1] We leave Turing machines and the λ-calculus for a future time.

Actually, the three concepts described above are all *equivalent* to each other. It should then be no surprise that *recursion* (and its twin *induction*) will play a central role in our studies, so we will take this brief moment to quickly describe the fundamental idea at behind recursion.[1]

First, an example: how do we *compute* the sum of a list of n numbers?

$$3+5+9+2$$

With some hard work and determination access to the internet, we can see that $3+5+9+2=19$, but *how* did we get that answer? At the most basic level, we started by taking two of the numbers, 3 and 5 say, computing their sum $3+5=8$, and adding this intermediate result to another number from the list, 9 say, to get $8+9=17$, and adding that again to yet another element of the list—in this case, only 2 remains—to finally arrive at $17+2=19$.

$$\begin{aligned} 3+5+9+2 &= 3+5+9+2 && (1)\\ &= 8+9+2 && (2)\\ &= 8+9+2 && (3)\\ &= 17+2 && (4)\\ &= 17+2 && (5)\\ &= 19 && (6) \end{aligned}$$

This might seem so obvious it physically hurts, but let's analyse what we just did more closely. Suppose we have a list of n arbitrary numbers.[2]

$$x_0 + x_1 + x_2 + \cdots + x_{n-2} + x_{n-1}$$

Once again, we begin by taking the first two numbers and computing $x_0 + x_1$, then adding *this* result to x_2, then adding *that* result to x_3, then adding *that* result to x_4, and so on until we reach the end of the list. So, in order to compute $x_0 + x_1 + x_2 + \ldots x_{n-2} + x_{n-1}$, we *first* need to compute $x_0 + x_1 + x_2 + \ldots x_{n-2}$ and then add that result to x_{n-1}.

[2] Notice that, being the sophisticates we are, we start counting at 0, so that a list of n numbers will be indexed starting at 0 and ending at $n-1$.

But wait, isn't $x_0 + x_1 + x_2 + \ldots x_{n-2}$ also the sum of a list? It is, it's just that the list has one less element! So *how do we compute the sum of elements in a list*? We first *compute the sum of elements in a list*, and then add one more element to that result. So, it seems like in order to do what we want, we need to already know how to do what we want; the key here is that we only need to know how to sum the elements of a *smaller* list in order to get the result we want for the *larger* list. As long as we can *eventually* get a result for one of these *"smaller"* sums, we will be able to build up a solution to our original problem by passing this result *"back up"* the chain of computation. Back to our first example.

$$
\begin{aligned}
3+5+9+2 &= 3+5+9+2 && (1)\\
&= 3+5+9+2 && (2)\\
&= 3+5+9+2 && (3)\\
&= 8+9+2 && (4)\\
&= 17+2 && (5)\\
&= 19 && (6)
\end{aligned}
$$

This paragraph describes the *recurrence.*

Steps (1) through (3) continually decompose the given list into sublists on the left until we have no more lists we can break up. Each one of these lists is a smaller version of the original problem, and we compute the sums of these smaller lists by breaking them down and computing *their* sublists' sums, recombining these results at the end.

This paragraph encounters the *basis.*

This now brings us to an important point: *we can't decompose* 3 *any further,* because this list only has one element in it. Do we know what the sum of all numbers in a list with one element is? Of course we do: it's just *that* number. Now we can return this result *back up* to the 5 that was waiting to be added to it, and when we add them together, we can return *that* result back to the 9 that was waiting, and then return *that* result to the 2 that was waiting, finally letting us conclude that the sum over the whole list is 19. The *recurrence relation* below summarizes this.[1]

recurrence relation

$$
\texttt{sum}(x_0, x_1, \ldots x_{n-1}) = \begin{cases} 0 & \text{if } n = 0 \\ \texttt{sum}(x_0, x_1, \ldots x_{n-2}) + x_{n-1} & \text{if } n \geqslant 1 \end{cases}
$$

[1] Notice that this is actually written slightly differently than the procedure we've just described; think about *how* this is different and whether or not it actually computes the same result as the procedure we were just analysing.

We've exposed here a *recurrence* and a *basis*—the two key components underlying recursion (and, later, induction). The *recurrent* part of this procedure explains how to express a problem in terms of *"smaller"* instances of the *same problem,* describing how to combine the solutions to those subproblems into a solution for the original problem. Obviously, though, if you just keep decomposing problem into subproblems forever, you'll never be able to actually generate an answer to anything. Eventually, you need to *stop* and actually say what the answer to something is. The *basis*, does exactly this by providing explicit answers to the *smallest* versions of the problem.[2]

recurrence

basis

[2] This is sometimes called the *base case.*

1

Zeroth-Order Logic

"The limits of my language means the limits of my world."
– Ludwig Wittgenstein

Figure 1.1: Illustration by Rockwell Kent from "Moby Dick: or, The Whale."

As we saw in the previous chapter, sentences can be broadly classified based on the kind of information they convey—their *functional role* in language. How do we begin deconstructing the descriptive fragment of our language? Naturally, we can think to classify the descriptive sentences by asking the fundamental question: *is this description true?*

1.1 *Truth Values*

Let's consider the following declarative sentence.

"Ahab is a captain." (1.1)

Here we have a descriptive sentence about the term *Ahab*—a man and thus an object of our discourse—asserting he *is a captain.* In the context of Herman Melville's *Moby Dick,* this is an accurate description. Referring to the above sentence as $\sigma_{1.1}$, we would then say $\sigma_{1.1}$ is *true*. We introduce the symbol $\top$ to denote these kinds of sentences.

true
$\top$

"Ishmael is a whale." (1.2)

The above sentence, however, which we will name $\sigma_{1.2}$, immediately furrows the brow and strikes at the heart of our conscience. We know from the story that Ishmael is a sailor, and thus human, and therefore *not* a whale! We should then want to say that $\sigma_{1.2}$ is *false*, reserving the symbol $\bot$ for sentences of this kind.

false
$\bot$

The symbols $\top$ and $\bot$ are also sometimes called *"top"* and *"bot"* respectively.

The attributes *true* and *false* that we are attaching to these sentences are what we call *truth values*, and they are *the* essential component of the kinds of sentences we want to express. Sentences that are *true* all exhibit a quality that makes them similar to each other but dissimilar to *false* sentences, regardless what the actual sentences themselves *mean*

truth value

semantically. What we've just done is *abstract* the fundamental concept of truth value from descriptive sentences. This abstraction allows us to notice that *all true sentences are essentially the same as each other,* at least from the perspective of their truth values, with the same applying to *false* sentences. On the other hand, *true* and *false* sentences are complete opposites. This relationship inspires our first definition below.

Definition 1.1 (Propositional Equivalence).
equivalence
$\equiv$
We say that two sentences φ and ψ are *equivalent* when they have the same truth value. We denote this by writing $\varphi \equiv \psi$.[1]

[1] *"φ is (logically) equivalent to ψ."*

Axiom (Equivalence is an Equivalence Relation).
We will take the following three properties to be *true* for any sentences φ, ψ, and ξ that are carriers of truth values.

1. $\varphi \equiv \varphi$. *reflexivity*
2. *If* $\varphi \equiv \psi$, *then* $\psi \equiv \varphi$. *symmetry*
3. *If* $\varphi \equiv \psi$ *and* $\psi \equiv \xi$, *then* $\varphi \equiv \xi$. *transitivity*

公理

With this new definition, we can formalize our observations from the preceding paragraph as $\sigma_{1.1} \equiv \top$ and $\sigma_{1.2} \equiv \bot$ as well as $\sigma_{1.1} \not\equiv \sigma_{1.2}$. Notice that each of these three expressions is a complete sentence describing properties[2] held by some objects.[3] In fact, these statements were themselves *true* declarative sentences. Now, let's ponder the following sentence, which we will call $\sigma_{1.3}$.

[2] being (or not) logically equivalent

[3] the sentences $\sigma_{1.1}$ and $\sigma_{1.2}$

"Colorless green ideas sleep furiously." (1.3)

Like the previous examples, this is a grammatically correct, declarative sentence, but what does this sentence *mean?* Is it *true?* Is it *false?* Taking the normal English definitions for each of the words in this sentence, it doesn't seem to make any sense. We then clearly can't call it an accurate description of anything, so it can't possibly be *true.* Does that mean it must be *false?* Well, if we assume it is *false,* then what about the following sentence?

"Colorless green ideas *do not* sleep furiously." (1.4)

This one, which we will call $\sigma_{1.4}$, seems to be saying the opposite of whatever $\sigma_{1.3}$ was saying, so if the other one is *false,* then this one must be *true.* The question then becomes: what is $\sigma_{1.4}$ accurately describing? *This* sentence seems to make just as little sense as the original! This should lead us to conclude that $\sigma_{1.3}$ could not have been *false* either, so that sentence *has no truth value!* We call expressions like this *nonsensical* because they *carry no semantic meaning.*
nonsense

Let's now analyse the following statement, which we will call $\sigma_{1.5}$.

"This sentence is *false*." (1.5)

Expressed a little more *formally*, this is the sentence—named $\sigma_{1.5}$—that says $\sigma_{1.5} \equiv \bot$. This certainly doesn't seem like nonsense; it says something clear about a well-understood object. So, what is the truth value of this sentence? We can try reasoning about this like we did before by examining the two possible truth values the $\sigma_{1.5}$ can take.

First, let's assume $\sigma_{1.5}$ is *true*, which we write formally as $\sigma_{1.5} \equiv \top$. By definition, this would imply $\sigma_{1.5}$ is an accurate description of some object, so we should believe what the sentence says about that object. In this case, the object is $\sigma_{1.5}$ and the description is that $\sigma_{1.5} \equiv \bot$. This *contradicts* our initial assumption! ↯ Therefore, $\sigma_{1.5}$ is *not true!*[1]

[1] We conclude this because this is the opposite of our initial assumption, which lead us to a contradiction.

That rules out one truth value. What happens then if we assume $\sigma_{1.5}$ is *false?* Again, we can write this formally as $\sigma_{1.5} \equiv \bot$. By definition, this implies we should *reject* what $\sigma_{1.5}$ is asserting, leaving us with $\sigma_{1.5} \not\equiv \bot$. As before, a *contradiction* emerges! ↯ Therefore, $\sigma_{1.5}$ is *not false* either!

From this simple analysis, we can see that $\sigma_{1.5}$ *does not have a truth value!* Sentences that *contradict themselves* like this are called *paradoxes*.[2] In the preceding analysis, we relied on the idea that $\top$ and $\bot$ are opposed to each other, so that the same sentence can't meaningfully be both $\top$ and $\bot$ at the same time. This should be intuitive based on our natural understanding and usage of the words *true* and *false*, but we will make it a point to *formally* introduce this idea now.

paradox

[2] The word *paradox* is unfortunately overload and context-dependent. When referring to specific sentences, we will use it to specifically mean a self-contradictory sentence such as $\sigma_{1.5}$, but it is also commonly used in some contexts to refer to situations that are simply *unintuitive* rather than outright contradictory.

Axiom (Principle of Bivalence).
Sentences expressing truth values are either *true* or *false* but not both.
公理

What this analysis has hopefully shown us is that *not every* well-formed, declarative sentence expresses a truth value. In order for a sentence to express a truth value, it must satisfy the following three properties.

1. The sentence must be grammatically well-formed.
2. The sentence must be declarative.
3. The sentence must be semantically meaningful.

These are the kinds of statements are *eligible to carry a truth value*—the ones for which *it would make sense* to say they are either *true* or *false*—so they will form the foundation of our new language. We will eventually call these *propositions*, but beware that this is not (yet) a *formal* definition of what a proposition is. First, we need to get a better sense of *what* propositions are linguistically and *how* they are formed.

1.2 *Logical Connectives*

The examples of sentences we've seen so far have all been *atomic*—meaning they can't be broken down into simpler sentences that themselves are complete thoughts—but we can obviously express thoughts that are more than merely atomic. These *compounded* propositions are formed by taking smaller propositional sentences and *connecting* them together based on what our intended meaning is.

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \to q$	$p \leftrightarrow q$
$\top$	$\top$	$\bot$	$\top$	$\top$	$\top$	$\top$
$\top$	$\bot$	$\bot$	$\bot$	$\top$	$\bot$	$\bot$
$\bot$	$\top$	$\top$	$\bot$	$\top$	$\top$	$\bot$
$\bot$	$\bot$	$\top$	$\bot$	$\bot$	$\top$	$\top$

Table 1.1: A truth table summarizing the basic connectives of classical logic. The two left-most columns represent the *input* values of the propositions p and q. The remaining columns describe the *output* of each expression given the corresponding inputs on each row.

Each of these different ways of connecting sentences together suggests a different way of *transforming* between truth values by combining the truth values of the component propositions into a truth value for the compound expression.

logical connective

In this section, we will uncover these different transformations—which we will call *logical connectives*—and encode them using *truth tables*, which specify the output truth values for every combination of inputs.

Negations

Suppose we encountered the following sentence, which we call $\sigma_{1.6}$.

"Espresso is not delicious." (1.6)

Immediately, the moral observer will realize the offensive absurdity of this sentence, compelled by the force of conscience to declare $\sigma_{1.6} \equiv \bot$! With this, we could simply carry on with our day; however, pausing to think for a moment, we can see that $\sigma_{1.6}$ is intimately related to the following (much more pleasant) sentence, which we call $\sigma_{1.7}$.

"Espresso is delicious." (1.7)

This sentence is *clearly true,* letting us sigh $\sigma_{1.7} \equiv \top$ in relief. Not only that, it is the saying exactly the opposite of what $\sigma_{1.6}$ asserted! We call propositions like these *negations* of each other. This is our first example of a *transformation* of truth value: the negation of a proposition is another proposition with the opposite truth value. To denote this formally, we introduce the $\neg$ symbol, allowing us to write $\sigma_{1.6} \equiv \neg\sigma_{1.7}$.

negation

$\neg$

Table 1.2: Truth table for negations.

p	$\neg p$
$\top$	$\bot$
$\bot$	$\top$

We can now think of $\neg$ formally as a *unary function* that operates on truth values.[1] This function works by mapping $\neg\top$ to $\bot$ and by

[1] A function is *unary* if it takes only one input argument. We will study functions in more detail later.

mapping $\neg\bot$ to $\top$. This gives us a way of abstracting negations at the level of truth values, so that we can formally define what it means to *negate* a proposition. We provide this definition now in table 1.2, where the left-most column represents the inputs[1] to $\neg$ and the right-most column shows the truth values of the resulting output expression.[2]

[1] ... shown with white backgrounds ...

[2] ... shown with colored backgrounds ...

Conjunctions and Disjunctions

But we can obviously connect two (and sometimes more) sentences together to create larger sentences in English. For example,

"Espresso is delicious, and it nourishes the soul." (1.8)

This sentence is composed of two smaller atomic sentences, namely *"espresso is delicious"* and *"espresso nourishes the soul,"* which we know are both independently *true.* Connecting them together with the word *"and"* should then, based on the way this word works in English, produce another *true* sentence. Conversely, if either of the subexpressions had been *false,* the compound result should also be *false.* This *binary* connective is called the logical *conjunction*, and we denote it using the $\wedge$ symbol. It is defined in table 1.3.

conjunction

$\wedge$

Table 1.3: Truth table for logical conjunctions and disjunctions.

p	q	$p \wedge q$	$p \vee q$
$\top$	$\top$	$\top$	$\top$
$\top$	$\bot$	$\bot$	$\top$
$\bot$	$\top$	$\bot$	$\top$
$\bot$	$\bot$	$\bot$	$\bot$

There are several distinct ways this connective can appear in English that are nonetheless equivalent. Some examples are listed below.

"Espresso is delicious, *and* it nourishes the soul."
"Espresso is delicious *and* soul-nourishing."
"Espresso is delicious, *but* it nourishes the soul."
"Espresso is delicious, *yet* nourishing to the soul."
"Espresso is delicious; *further*, it nourishes the soul."
"*Although* espresso is delicious, it *also* nourishes the soul."

Table 1.4: These sentences are all logically equivalent to $\sigma_{1.8}$, though this list is obviously not exhaustive.

disjunction

$\vee$

The conjunction has a *logical dual* called the *disjunction*, defined in table 1.3 using the $\vee$ symbol and exemplified by the following sentence.

"Espresso is delicious, or it nourishes the soul." (1.9)

We all these two connectives *dual* to each other because negating all of the inputs to one of them is equivalent to negating the output of the other. Specifically, the expression $\neg p \vee \neg q$ is equivalent to $\neg(p \wedge q)$ whenever p and q are propositions.

Definition 1.2 (Logical Duality).

logical duality

We say two logical connectives f and g are *logically dual* if negating the inputs of f is always logically equivalent to negating the output of g. Equivalently, we can say f is *logically dual* to g if applying f after $\neg$ always gives the same result as applying $\neg$ after g on any given inputs.

Conjunctions and disjunctions are just one example of a dual connective pair. In fact, every logical connective is dual to some other connective![1] For now, we present this result about $\wedge$ and $\vee$ *without proof;* we will *prove* this statement when we discuss theorem 1.5 in a short while.

[1] Why might this be? Think about this.

Conditional Statements

We turn our attention now to sentence $\sigma_{1.10}$ below.

"If espresso nourishes the soul, then I will drink it." (1.10)

This is a *conditional* sentence, composed of two subclauses called the *antecedent* and the *consequent*.[2] When we use this sort of linguistic construction, we mean to say that *if* the premise happens, *then* the conclusion must also happen. Said another way: the conclusion must occur *whenever* the premise is satisfied. Notice *we are not asserting anything* about the antecedent or consequent individually! We are only establishing a *relationship* where the consequent occurs *every time* that the premise is satisfied. We call this the *material implication*, denoted by the $\to$ symbol and defined in table 1.5.

implication
$\to$

Table 1.5: Truth table for conditionals.

p	q	$p \to q$	$p \leftrightarrow q$
$\top$	$\top$	$\top$	$\top$
$\top$	$\bot$	$\bot$	$\bot$
$\bot$	$\top$	$\top$	$\bot$
$\bot$	$\bot$	$\top$	$\top$

[2] Synonyms for *antecedent* & *consequent*.

protasis	apodosis
sufficient	necessary
premise	inference
assumption	conclusion
supposition	deduction
implicant	implicand
hypothesis	thesis

$$p_{1.10} := \text{"Espresso nourishes the soul."}$$
$$q_{1.10} := \text{"I will drink espresso."}$$

The antecedent and consequent for $\sigma_{1.10}$ are defined above. With these definitions, we can now write $\sigma_{1.10} \equiv p_{1.10} \to q_{1.10}$ and observe that $\sigma_{1.10}$ simply says: *if* $p_{1.10} \equiv \top$, *then* $q_{1.10} \equiv \top$. Importantly, this is *the only thing* that $\sigma_{1.10}$ is asserting! This sentence *is not saying* that if $p_{1.10} \equiv \bot$, then $q_{1.10} \equiv \bot$. In fact, if the premise is *false,* then $\sigma_{1.10}$ says *nothing* about whether or not $q_{1.10}$ is *true* or *false.*

To make this concrete, suppose I told you the following.

"If you make an $\mathcal{A}$ in this class, then I will eat my shoe." (1.11)

If you do happen to make an $\mathcal{A}$ in this class, then I'll be forced to physically eat my shoe in order to keep up my end of the bargain; in that case, the sentence was *true.*[3] On the other hand, if you make an $\mathcal{B}$ instead, then I can go home with both shoes and conscience intact; in this case, the sentence was also *true.*[4] However, what if you make the $\mathcal{B}$ but I decide to eat my shoe anyways? Did I lie? No; just because you failed to make an $\mathcal{A}$ doesn't mean I *can't* eat my shoe! All I said was that I definitely would if you made an $\mathcal{A}$.[5] That sentence is only a lie when you *do* make an $\mathcal{A}$ in the class, but I refuse to eat my shoe, since I really am breaking my promise then.[6]

[3] $\top \to \top \equiv \top$

[4] $\bot \to \bot \equiv \top$

[5] $\bot \to \top \equiv \top$

[6] $\top \to \bot \equiv \bot$

In table 1.6, we list several ways of verbalising $p \to q$ in English. Since this connective can be worded in so many unintuitive ways; careful attention must be paid to phrases involving conditionals.

"I will drink espresso *if* it nourishes the soul."
"Espresso nourishes the soul *only if* I drink it."
"It is *sufficient* that espresso nourish the soul for me to drink it."
"It is *necessary* that I drink espresso for it to nourish the soul."
"I will drink espresso *unless* it doesn't nourish the soul."

Table 1.6: These sentences are *all* logically equivalent to $\sigma_{1.10}$. Pay close attention to *grammar* of each sentence, and make special note of *where* the connectives appear.

biconditional ↔

Finally, the *material equivalence*,[1] also called the *biconditional* and written $p \leftrightarrow q$, is *true* exactly when p and q have the same truth value and is *false* otherwise. With these connectives all defined, we are now ready to formally introduce the *recursive definition* of a proposition.

[1] This is often written *"if and only if"* in English, abbreviated *iff* .

A Formal Proposition

Definition* 1.3 *(Proposition).

proposition

We say that λ is a *proposition iff* λ satisfies the following recurrence.

1. $\lambda = \top$ or $\lambda = \bot$.
2. $\lambda = \neg(\varphi)$, where φ is a proposition.
3. $\lambda = (\varphi) \wedge (\psi)$ where φ and ψ are propositions.
4. $\lambda = (\varphi) \vee (\psi)$, where φ and ψ are propositions.
5. $\lambda = (\varphi) \to (\psi)$ where φ and ψ are propositions.
6. $\lambda = (\varphi) \leftrightarrow (\psi)$, where φ and ψ are propositions.

Notice the use of *equality* $=$ rather than *equivalence* $\equiv$ throughout this definition. In each statement here, we are saying that the statement λ is *equal* to the expression on the right-hand side of the $=$ symbol, meaning *they are the same sentence written in the same way.* This gives a *syntactic* definition of what a proposition is.

The use of parentheses in this definition is to avoid issues with order of operations; in situations where the meaning is clear, we can *carefully* drop parentheses.

This definition works by first establishing as our *basis* that $\top$ and $\bot$ are propositions in (1). We then, in (2) through (6), specify larger propositions *recursively* by composing together smaller, already-existing propositions using logical connectives. This then lets us verify that statements like $((\neg\top) \wedge (\bot \wedge \top)) \to \top$ are indeed propositions.

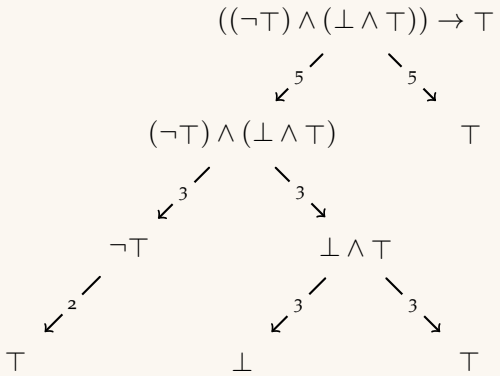

Figure 1.2: In this example, we have dropped some unambiguous parentheses for clarity. Notice, however, that some parentheses *cannot* be dropped: for example, those around the premise of the $\to$ conditional, and those separating the arguments of the two $\wedge$ conjunctions. If those parentheses had been placed like $((\neg\top) \wedge \bot) \wedge \top$ instead, we would have parsed $\not\curlywedge$ instead of $\not\curlyvee$ as in the figure.

Alternatively, think of this as *inductive bootstrapping*.[2] Beginning with $\top$ and $\bot$ from (1) as our initial instances of propositions, we then

[2] *"Pulling itself up by the bootstraps."*

build larger propositions like $\neg\bot$ and $\top \wedge \bot$, which fall into (2) and (3) respectively. We can then take those expressions, conjunct them again using (2), and place an implication between that result and $\top$ using (5) to arrive at our final expression $((\neg\top) \wedge (\bot)) \to \top$. By taking basis expressions and connecting them together according to the rules laid out in the definition, we *computed* a way of building the final expression in a way that satisfies the definition, verifying that it is a proposition.

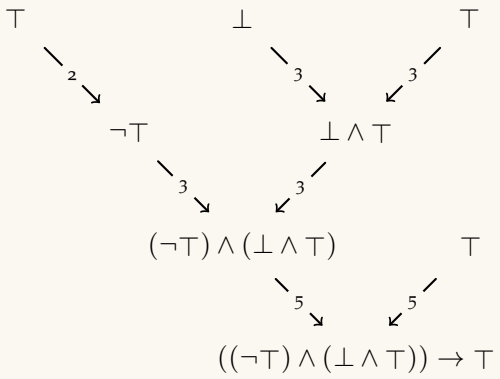

Figure 1.3: The inductive way of building up the expression, as contrasted with the recursive way of tearing down the expression in the previous figure.

Definition 1.4 (Propositional Formula).

propositional formula

A *propositional formula* is an expression that evaluates as a proposition when all of its *variables* are themselves replaced by propositions.

Logical Equivalence

The astute reader may have noticed that some expressions are logically equivalent to each other even if they look different when written out.

p	q	$\neg(p \wedge q)$	$\neg p \vee \neg q$	$p \to q$	$\neg q \to \neg p$
$\top$	$\top$	$\bot$	$\bot$	$\top$	$\top$
$\top$	$\bot$	$\top$	$\top$	$\bot$	$\bot$
$\bot$	$\top$	$\top$	$\top$	$\top$	$\top$
$\bot$	$\bot$	$\top$	$\top$	$\top$	$\top$

Table 1.7: A truth table verifying two equivalences. First, that $\neg(p \wedge q)$ and $\neg p \vee \neg q$ are equivalent as predicted by DeMorgan. Second, that $p \to q$ is equivalent to its *contrapositive* $\neg q \to \neg p$.

For example, it's clear that $p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$, as the name *"if and only if"* would suggest. We saw another example of an equivalence when we examined the duality of $\wedge$ and $\vee$, illustrated in table 1.7. We can see that statements like these are logically equivalent because the output truth values are always the same whenever we assign the same input truth values to the variables in these expressions. In their joint truth table, the output columns for the two expressions are identical. *Equivalent propositions are essentially the same when we view them through the lens of truth values.*[1]

[1] The idea of blurring the lines between objects that are *essentially the same* according to some salient characteristics is a fundamental idea in mathematics that shows up basically everywhere. This is, fundamentally, *why* abstractions are useful and interesting: we abstract in order to draw equivalences between things we previously thought of as distinct.

Following this idea means having to construct a joint truth table whenever we want to check whether or not two formulæ are equivalent. Although it would be a straightforward to automate, doing all of our work by hand would be *extremely* tedious. If we are given two propositions $\varphi(p_1, p_2, \ldots p_n)$ and $\psi(p_1, p_2, \ldots p_n)$ consisting of the same variables, then answering $\varphi(p_1, p_2, \ldots p_n) \stackrel{?}{\equiv} \psi(p_1, p_2, \ldots p_n)$ requires computing truth values for φ and ψ with *all possible combinations* of truth assignments to $p_1, p_2, \ldots p_n$ and checking that they match.

Now, p_1 can either be $\top$ or $\bot$. For each of these truth values, we then have check both truth values p_2 can take. Then, for each of those, we need to check the two truth values for p_3, and so on until we reach p_n. Each particular assignment of truth values to all of the propositional variables corresponds to one row in our truth table.

If $n = 1$, so our propositions each involve one variable, this means we only need two rows in our truth table to exhaust the entire search space: one row if the variable is $\top$, and one row if it's $\bot$. However, with each new variable we introduce, we *double* the size of our search space because this new variable comes with *two new possible truth values* that we need to check *for each* of the rows we've already computed. We summarize this phenomenon with the following *recurrence relation.*[1]

$$\texttt{rows}(n) = \begin{cases} 1 & \text{if } n = 0 \\ 2 & \text{if } n = 1 \\ 2 \cdot \texttt{rows}(n-1) & \text{if } n \geqslant 2 \end{cases} \tag{1.12}$$

[1] The degenerate case of $n = 0$, when neither expression has any propositional variables, would just require one row in our truth table since each proposition only has one, unchanging truth value.

This shows us that answering the equivalence question for propositional formulæ of n variables involves computing a truth table with 2^n rows. Obviously, *this doesn't scale;* it quickly becomes infeasible to even *allocate enough space* for our output columns, much less actually compute and check these outputs. The thinking man's alternative is to instead *prove* that the two expressions are equivalent, constructing a formal, logical argument that derives $\varphi(p_1, p_2, \ldots p_n) \equiv \psi(p_1, p_2, \ldots p_n)$ from assumptions—called *axioms*—using *rules of inference.*

proof

axiom

Logical Nonequivalence

Showing that two propositional expressions are *not* equivalent is computationally easier than showing that they *are*. Checking that two propositional formulæ are equivalent involves either writing proof or computing *every row* of an exponentially sized truth table. However, checking that two formulæ are *not* equivalent requires *just one example* of a truth assignment on which the propositions disagree. Instead of an entire truth table, all we need is a *single row*.

p	q	$\neg(p \wedge q)$	$\neg p \wedge \neg q$
$\top$	$\top$	$\bot$	$\bot$
$\top$	$\bot$	$\top$	$\bot$
$\bot$	$\top$	$\top$	$\bot$
$\bot$	$\bot$	$\top$	$\top$

Table 1.8: A truth table showing negations do not distribute over conjunctions.

For example, to show that $p \to q \not\equiv q \to p$, all we have to do is let $p := \top$ and $q := \bot$. We can then observe that $p \to q \equiv \top \to \bot \equiv \bot$. Meanwhile, $q \to p \equiv \bot \to \top \equiv \top$. Thus, we conclude $p \to q \not\equiv q \to p$.

Definition 1.5 (Logical Equivalence & Nonequivalence).
Let φ and ψ be propositional formulæ both consisting of the *same* variables $p_1, \ldots p_n$. We say that φ is *equivalent* to ψ if *every* assignment of truth values to the variables of φ and ψ produces the same truth value. In this case, we write $\varphi \equiv \psi$.

logical equivalence

$\equiv$

We say that φ is *not equivalent* to ψ if *there is* an assignment of truth values to the formulæ's variables that makes the truth values of φ and ψ different. In this case, we write $\varphi \not\equiv \psi$.

logical non equivalence

$\not\equiv$

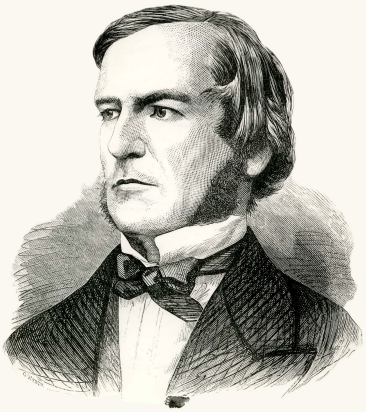

Figure 1.4: George Boole, a largely self-taught mathematician, logician, and philosopher, first described the eponymous *Boolean algebra* in his 1854 monograph *The Laws of Thought.*

1.3 *The Propositional Logic*

Axioms and Proofs

The axioms of propositional logic encode the *foundational assumptions* we are making about the nature of truth-value-based reasoning. We take these truths to be self-evident *without justification.*

IDENTITY	$\top \wedge p \equiv p$	$\bot \vee p \equiv p$
COMPLEMENT	$\neg p \wedge p \equiv \bot$	$\neg p \vee p \equiv \top$
COMMUTATIVITY	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$
ASSOCIATIVITY	$p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$	$p \vee (q \vee r) \equiv (p \vee q) \vee r$
DISTRIBUTIVITY	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
CONDITIONAL DISINTEGRATION		$p \to q \equiv \neg p \vee q$
BICONDITIONAL DISINTEGRATION	$p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$	

Table 1.9: The axioms of classical logic. The first five specify a *Boolean algebra*; notice that each of these first five axioms has a conjunctive fragment (left) and a *dual* disjunctive fragment (right).

Each of the statements in this table is a logical equivalence establishing that the two expressions are *interchangeable in all contexts.* We could verify each of these by constructing the appropriate truth table; however, the attitude we will take is that each statement in the table simply *is true a priori,* without any need for verification. Instead, they will form the *basis* upon which we build proofs of *other* statements.

The *complement* axiom in the second row of table 1.9 shows us two important facts about the negation of any proposition. If we take a proposition p and conjunct it with its negation $\neg p$, that axiom tells us that we get $\bot$; dually, disjuncting p with its negation gives us $\top$. Is this behavior *characteristic* of $\neg p$? The following theorem tells us *yes,* that any proposition that *behaves like* the negation of p must be *indistinguishable* from $\neg p$ through the lens of truth values! With that said, let's try to prove our first *theorem*.[1]

theorem

[1] A *theorem* is a provable proposition.

Theorem 1.1 (Uniqueness of Complements).
For any propositions p and q, if $p \wedge q \equiv \bot$ and $p \vee q \equiv \top$, then $\neg p \equiv q$.

定理

Proof. Let p and q be arbitrary propositions.[2] Assume $p \wedge q \equiv \bot$ and $p \vee q \equiv \top$.[3] We will prove $\neg p \equiv q$ by showing that $\neg p$ and q are both equivalent to the same expression. First, observe the following.

[2] Since we need to prove this statement *for any two propositions* p and q, we introduce two *arbitrary* propositions at the beginning of our proof.

[3] These assumptions are warranted because they are the *premise* of the *conditional* statement we are proving.

$$
\begin{aligned}
\neg p &\equiv \top \wedge \neg p && \text{by } \textit{identity} \\
&\equiv \neg p \wedge \top && \text{by } \textit{commutativity} \\
&\equiv \neg p \wedge (p \vee q) && \text{because we assumed } p \vee q \equiv \top \\
&\equiv (\neg p \wedge p) \vee (\neg p \wedge q) && \text{by } \textit{distributivity} \\
&\equiv \bot \vee (\neg p \wedge q) && \text{by } \textit{complement} \\
&\equiv \neg p \wedge q && \text{by } \textit{identity}
\end{aligned}
$$

As a result, $\neg p \equiv \neg p \wedge q$. Similarly, we can now observe the following.

$$
\begin{aligned}
q &\equiv \top \wedge q && \text{by } \textit{identity} \\
&\equiv q \wedge \top && \text{by } \textit{commutativity} \\
&\equiv q \wedge (p \vee \neg p) && \text{by } \textit{complement} \\
&\equiv (q \wedge p) \vee (q \wedge \neg p) && \text{by } \textit{distributivity} \\
&\equiv (p \wedge q) \vee (\neg p \wedge q) && \text{by } \textit{commutativity} \\
&\equiv \bot \vee (\neg p \wedge q) && \text{because we assumed } p \wedge q \equiv \bot \\
&\equiv \neg p \wedge q && \text{by } \textit{identity}
\end{aligned}
$$

This gives us $q \equiv \neg p \wedge q$. Therefore, we conclude $\neg p \equiv \neg p \wedge q \equiv q$.

Q.E.D.

Q.E.D. stands for *Quod Erat Demonstrandum,* which is Latin for "what was to be shown has been demonstrated," after the Greek Ὅπερ ἔδει δεῖξαι. This is called a *tombstone,* and it is a traditional way of denoting the end of a proof. Modern authors might use □ or ■ instead.

Notice how *every* statement in the proof above is written with *purpose,* and much of the proof is inspired by *the form of the theorem* we are trying to prove. Let's analyze what just happened. Before we begin writing the proof, we first read the theorem focussing on two things: the *form* of the statement, and *what* the statement says.

First and foremost, this theorem says something about *any propositions.* We have two options for proving something is true about every single

proposition: we can check all of them individually, or we can show that the thing we are trying to prove is an *inherent quality of being a proposition.* The former approach is clearly unworkable whenever we have infinitely many—or even just a large amount of—things to check, as we do here. Instead, we will take the later approach: by taking an *arbitrary* proposition and *making no assumptions, imposing no constraints,* then any argument we make about this particular proposition will also apply to any other proposition we encounter.[1] The first sentence of the proof introduces these two arbitrary propositions.

Now that we know we are proving something *universal* about propositions, we keep reading the theorem and see that it's a statement of the form *"if ___, then ___."* This is a *conditional* statement, and the most straight-forward way to show a conditional statement is *true* is to *demonstrate the conclusion is fulfilled whenever the premise is true.* Thus, we can *assume* the premise of the conditional is *true,* and our task them is to derive the conclusion. The second sentence of our proof assumes the premise, which happens to be a conjunction of two statements.

Up to this point, everything we've done has been determined solely by the *form* of the theorem we are trying to prove. Now, our task is to take what we have and show the conclusion.[2] What follows next is a sequence of logical statements, each of which is *justified,*[3] which ends at the conclusion we wanted. *How* you decide to craft this sequence of statements—what statements to make in what order, what proof techniques to use, what intuition inspired your approach—is entirely dependent on *your style* as long as all of the logic is clear, all of the logical rules are followed, and all of the justification is correct.

Proof-writing is an art form in much the same way building a musical instrument is. When a luthier makes a guitar, the process is guided by the particular luthier's traditions, experiences, style, and tastes; so long as the final product is truly a guitar that sounds and plays like a guitar should, the luthier has complete liberty. While two master luthiers might take radically different approaches that lead to guitars with unique aesthetic qualities, they will nonetheless produce two functioning guitars and preference of one over the other will be a matter of judgement and taste. This is much the same when it comes to writing proofs; the analogue to programming should be clear.

Since we proved theorem 1.1, we can now use this result in the future when proving more complicated statements. For example, it should be easy to see intuitively that $\top \equiv \neg\bot$ and $\bot \equiv \neg\top$, based on the way we use the words *true* and *false* in natural language and how $\top$ and $\bot$ are meant to correspond to those truth values. We can now prove this as a *corollary*—a simple consequence—of theorem 1.1.

[1] As an example, suppose we wanted to prove that the square of any positive number is also positive. We obviously can't check all of the positive numbers one-by-one. Instead, we can take an *arbitrary* number x such that $x > 0$, and then argue that $x^2 > 0$. If we do this successfully, then we can take *any* particular number, such as 5, substitute it for x in our argument, and obtain a proof that $5^2 > 0$. However, if we couldn't have written our *original argument* in terms of 5; this would have meant imposing the *additional constraint* that $x = 5$, preventing our argument from generalizing to *all* positive numbers.

[2] If our conclusion were a longer, compound statement, we would continue breaking the problem down *recursively* until we were left with something *atomic*.

[3] ...either by a *definition*, an *axiom*, an *assumption* we've made, or a prior *theorem* we've proven ...

Figure 1.5: Examples of three distinct bracing styles for the classical guitar.

***Corollary* 1.1.**
$\top \equiv \neg\bot$ and $\bot \equiv \neg\top$.

推論

Proof. Observe that $\bot \wedge \top \equiv \bot$ by the *identity* axiom. Similarly, we have that $\bot \vee \top \equiv \top \vee \bot \equiv \top$ by *commutativity* and the *identity* axiom again. So, we can apply theorem 1.1[1] and conclude $\top \equiv \neg\bot$. Similarly, we can observe that $\top \wedge \bot \equiv \bot \wedge \top \equiv \bot$ by *commutativity* and *identity*, and $\top \vee \bot \equiv \bot$ by the *identity* axiom. Thus, $\bot \equiv \neg\top$ by theorem 1.1.

Q.E.D.

[1] We can invoke the theorem here because we have just *proven* the premises of the theorem are *true* for the particular propositions we are looking at (in this case, $p \coloneqq \bot$ and $q \coloneqq \top$). That means, having satisfied the premises, we get to assert the conclusion, justified by that theorem.

A proof gives us more than just a formal verification of a statement. It tells us that the statement is a *necessary consequence* of the axioms we assumed in setting up our logical system, and every instance of a proof gives us insight into *why* that's the case. These past two proofs show us that we didn't have to explicitly *define* or *assume* $\top$ to be the opposite of $\bot$ because this is a face satisfied by *any* instance of a Boolean algebra.

Let's prove another simple, but useful, theorem.

***Corollary* 1.2.**
For any propositions p and q, if $p \equiv q$, then $\neg p \equiv \neg q$.

推論

Proof. Let p and q be propositions such that $p \equiv q$ and observe.

$$\begin{aligned} q \wedge \neg p &\equiv p \wedge \neg p && \text{because we assumed } p \equiv q \\ &\equiv \bot && \text{by } \textit{commutativity} \text{ and } \textit{complement} \end{aligned}$$

We can do a very similar thing in the disjunctive case.

$$\begin{aligned} q \vee \neg p &\equiv p \vee \neg p && \text{because we assumed } p \equiv q \\ &\equiv \top && \text{by } \textit{commutativity} \text{ and } \textit{complement} \end{aligned}$$

Therefore, applying theorem 1.1, we conclude that $\neg p \equiv \neg q$.

Q.E.D.

***Corollary* 1.3.**
For any propositions p, q, r, s such that $p \equiv q$ and $r \equiv s$, the following.

$$\begin{aligned} p \wedge r &\equiv q \wedge s \\ p \vee r &\equiv q \vee s \\ p \to r &\equiv q \to s \\ p \leftrightarrow r &\equiv q \leftrightarrow s \end{aligned}$$

推論

We include corollary 1.3 above just for completeness, so that some of the basic properties of $\equiv$ are codified somewhere; their proofs are not particularly interesting. We are now ready to tackle the proof of a claim you probably find so obvious as to not even be worth mentioning—but it *is* worth mentioning how much groundwork we had to lay in order to prove this simple fact!

Theorem 1.2 (Double Negation).
For any proposition p, we have that $p \equiv \neg\neg p$.

定理

Proof. Let p be a proposition. We will show that $p \equiv \neg\neg p$ by showing that p acts like the negation of $\neg p$. Observe that $\neg p \wedge p \equiv p \wedge \neg p \equiv \bot$ by *communtativity* and the *complement* axiom. We can similarly see $\neg p \vee p \equiv p \vee \neg p \equiv \top$ by *commutativity* and *complement.* Therefore, we can conclude that $p \equiv \neg(\neg p)$ by theorem 1.1.

Q.E.D.

Our goal for the rest of this section will be to prove *De Morgan's laws*. This will finally establish the establish dual relationship between conjunctions and disjunctions. For this, we first need a few more tools.

Theorem 1.3 (Idempotence).
For any proposition p, we have $p \wedge p \equiv p$ and $p \vee p \equiv p$.

定理

Proof. Let p be a proposition. For the conjunctive statement, observe.

$$\begin{aligned}
p \wedge p &\equiv \bot \vee (p \wedge p) && \text{by } \textit{identity} \\
&\equiv (p \wedge p) \vee \bot && \text{by } \textit{commutativity} \\
&\equiv (p \wedge p) \vee (p \wedge \neg p) && \text{by } \textit{complement} \\
&\equiv p \wedge (p \vee \neg p) && \text{by } \textit{distributivity} \\
&\equiv p \wedge \top && \text{by } \textit{complement} \\
&\equiv \top \wedge p && \text{by } \textit{commutativity} \\
&\equiv p && \text{by } \textit{identity}
\end{aligned}$$

An analogous chain of reasoning takes us through the disjunctive case.[1]

$$\begin{aligned}
p \vee p &\equiv (p \vee p) \wedge \top && \text{by } \textit{identity} \text{ and } \textit{commutativity} \\
&\equiv (p \vee p) \wedge (p \vee \neg p) && \text{by } \textit{complement} \\
&\equiv p \vee (p \wedge \neg p) && \text{by } \textit{distributivity} \\
&\equiv p \vee \bot && \text{by } \textit{complement} \\
&\equiv p && \text{by } \textit{commutativity} \text{ and } \textit{identity}
\end{aligned}$$

Therefore, we have $p \wedge p \equiv p$ and $p \vee p \equiv p$ as desired.

Q.E.D.

[1] Notice that we have combined some steps here involving *commutativity;* when it is clear, we can save some space by combining *commutativity* with the step directly proceeding it. We *do not* yet have the maturity to combine any other steps.

Theorem 1.4 (Domination).
For any proposition p, we have $\top \vee p \equiv \top$ and $\bot \wedge p \equiv \bot$.

定理

Proof. Let p be a proposition and observe.

$$\begin{aligned}
\top \vee p &\equiv p \vee \top && \text{by } \textit{commutativity} \\
&\equiv p \vee (p \vee \neg p) && \text{by } \textit{complement} \\
&\equiv (p \vee p) \vee \neg p && \text{by } \textit{associativity} \\
&\equiv p \vee \neg p && \text{by } \textit{idempotence} \\
&\equiv \top && \text{by } \textit{complement}
\end{aligned}$$

The dual case works out in nearly the same manner.

$$\begin{aligned}
\bot \wedge p &\equiv p \wedge \bot && \text{by } \textit{commutativity} \\
&\equiv p \wedge (p \wedge \neg p) && \text{by } \textit{complement} \\
&\equiv (p \wedge p) \wedge \neg p && \text{by } \textit{associativity} \\
&\equiv p \wedge \neg p && \text{by } \textit{idempotence} \\
&\equiv \bot && \text{by } \textit{complement}
\end{aligned}$$

We therefore conclude $p \vee \top \equiv \top$ and $p \wedge \bot \equiv \bot$.

Q.E.D.

We are now ready to prove *De Morgan's laws.*

Theorem 1.5 (De Morgan's Laws).
If p, q are propositions, $\neg(p \wedge q) \equiv \neg p \vee \neg q$ and $\neg(p \vee q) \equiv \neg p \wedge \neg q$.

定理

Proof. Let p and q be propositions. We will prove the first half of this theorem by showing $\neg p \vee \neg q$ acts like the negation of $p \wedge q$, satisfying the premise of *uniqueness of negations.* We then apply the theorem to obtain $\neg(p \wedge q) \equiv \neg p \vee \neg q$. We will leave the other half—proving $\neg(p \vee q) \equiv \neg p \wedge \neg q$—as an exercise to the reader.

First, the conjunctive branch.

$$\begin{aligned}
(p \wedge q) \wedge (\neg p \vee \neg q) &\equiv p \wedge (q \wedge (\neg p \vee \neg q)) && \text{by } \textit{associativity} \\
&\equiv p \wedge ((q \wedge \neg p) \vee (q \wedge \neg q)) && \text{by } \textit{distributivity} \\
&\equiv p \wedge ((q \wedge \neg p) \vee \bot) && \text{by } \textit{complement} \\
&\equiv p \wedge (\bot \vee (\neg p \wedge q)) && \text{by } \textit{commutativity} \\
&\equiv p \wedge (\neg p \wedge q) && \text{by } \textit{identity} \\
&\equiv (p \wedge \neg p) \wedge q && \text{by } \textit{associativity} \\
&\equiv \bot \wedge q && \text{by } \textit{complement} \\
&\equiv \bot && \text{by } \textit{domination}
\end{aligned}$$

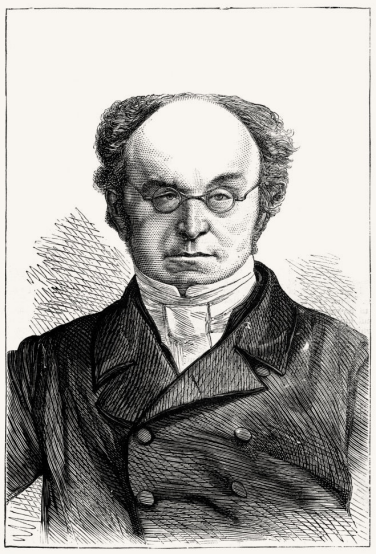

Figure 1.6: Augustus De Morgan, after whom these laws are named, is also notable for his work on logical quantification and mathematical induction.

We have now worked out that $(p \wedge q) \wedge (\neg p \vee \neg q) \equiv \bot$. We will show $(p \wedge q) \vee (\neg p \vee \neg q) \equiv \top$ in the disjunctive branch below analogously.

$$
\begin{aligned}
(p \wedge q) \vee (\neg p \vee \neg q) &\equiv ((p \wedge q) \vee \neg p) \vee \neg q && \text{by } \textit{associativity} \\
&\equiv (\neg p \vee (p \wedge q)) \vee \neg q && \text{by } \textit{commutativity} \\
&\equiv ((\neg p \vee p) \wedge (\neg p \vee q)) \vee \neg q && \text{by } \textit{distributivity} \\
&\equiv ((p \vee \neg p) \wedge (\neg p \vee q)) \vee \neg q && \text{by } \textit{commutativity} \\
&\equiv (\top \wedge (\neg p \vee q)) \vee \neg q && \text{by } \textit{complement} \\
&\equiv (\neg p \vee q) \vee \neg q && \text{by } \textit{identity} \\
&\equiv \neg p \vee (q \vee \neg q) && \text{by } \textit{associativity} \\
&\equiv \neg p \vee \top && \text{by } \textit{complement} \\
&\equiv \top \vee \neg p && \text{by } \textit{commutativity} \\
&\equiv \top && \text{by } \textit{domination}
\end{aligned}
$$

Therefore, by theorem 1.1, we conclude $\neg(p \wedge q) \equiv \neg p \vee \neg q$ as desired.

Q.E.D.

Rules of Inference

THE DEDUCTION RULE	$(p \vdash q) \vdash (p \to q)$	If, by assuming p, we can prove q, then we can write $p \to q$.
MODUS PONENS	$p, (p \to q) \vdash q$	If we have $p \to q$ and we know p, then we can deduce q.
MODUS TOLLENS	$\neg q, (p \to q) \vdash \neg p$	If we have $p \to q$ but also $\neg q$, then we can infer $\neg p$.
REDUCTIO AD ABSURDUM	$(\neg p \vdash q), (\neg p \vdash \neg q) \vdash p$	If $\neg p$ leads to a contradiction, then $\neg p$ is absurd; we conclude p.

Table 1.10: The rules of inference.

So far, we've developed a modestly-powerful formal language—capable of expressing some basic logical ideas—founded on *axioms*. This gives us a formal syntactic framework for expressing logical ideas, along with a basic semantics that relates these formal symbols to our natural language. The axioms in table 1.9 are all *equivalences*—substitution rules between propositions that preserve truth values—and we've now seen several examples of their use in proving some basic theorems.

Yet, you may have noticed that *some* of our reasoning in those proofs *was not based on equivalences*. This is most apparent in the proof of theorem 1.1, our very first theorem. We began that proof by introducing two arbitrary propositions and then *immediately assuming* that their conjunction was $\bot$ and their disjunction as $\top$. Making those assumptions was not justified on any of the equivalence axioms we'd introduced, so why were we allowed to say that in our proof? By a similar token, in

the proof of corollary 1.1, we apply theorem 1.1 by saying that, since we'd satisfied the premises of that theorem, we were allowed to write down the conclusion of that theorem. Why were we allowed to say that? In short: *because it makes sense!* The problem, of course, is that nothing yet in our system *formally* gives us the right or power to do these things, even though they make logical sense.

This then calls for the introduction of more axioms—ones that will allow us to construct these kinds of *one-way*, *inferential* arguments alongside our equivalence-based reasoning. We call these the *rules of inference*.

The rules in table 1.10 each take the form $\Gamma \vdash \varphi$,[1] where Γ represents a set of assumptions and φ is the conclusion that follows from them. The $\vdash$ symbol, sometimes called a turnstile, signifies that we can *prove* φ by assuming the statements in Γ and using the equivalence axioms, the rules of inference, and any theorems we've already proven. If there is nothing written to the left of the $\vdash$ symbol, this simply means that the conclusion φ can be derived *without* any additional assumptions.

prove

[1] *"Γ proves φ"* or *"φ follows from Γ."*

The most important of the rules of inference is *modus ponens*, enabling us to *follow through* on chains of conditional reasoning.[2] *Modus ponens* is, in a sense, the essence of classical rhetoric. Without it, the conclusion of a conditional statement's conclusion would not be meaningfully *conditioned* on its premise. There would be no point in establishing hypothetical arguments because the conditional chains of reasoning would never actually have any point to work towards. This rule has a sister—*modus tollens*—which conversely allows *breaking down* arguments counterfactually, denying antecedents with false consequents.[3]

[2] *Modus ponens* is short for the Latin phrase *modus ponendo ponens,* literally *"the method of putting by placing."*

[3] *Modus tollens* is short for the Latin phrase *modus tollendo tollens,* literally *"the method of removing by taking away."*

The next rule, named *reductio ad absurdum*,[4] gives us the ability to construct proofs by contradiction. Suppose we are interested in proving some proposition p. One way to reason about the validity of p is to think about what would happen if p were not the case. Hypothetically, assuming $\neg p$, if we were able to derive both q and also $\neg q$, then we would have derived a falsity ($q \wedge \neg q \equiv \bot$). If we were starting from *true* premises, this would be impossible since all of our axioms and rules of inference are *truth-preserving*. Clearly, this must mean that our assumption $\neg p$ was *not true,* leaving p as the only logical conclusion. This form of argumentation is like *"is like arguing with a hammer,"* according to a dear professor of mine from undergrad. It is incredibly powerful and has been in use since at least the year 400 BC.[5]

[4] *Reductio ad absurdum* is a Latin phrase meaning to *"reduce to absurdity."* This has also been called *argumentum ad absurdum*.

[5] In Plato's dialogues, Socrates frequently engages in this sort of reasoning by showing his opponents' seemingly-sensible statements can be systematically dismantled to absurdity.

Finally, the *deduction rule* is a technical rule of inference that ties together the meta-symbol $\vdash$ with the logical $\rightarrow$ symbol. It enshrines the parallel between a deductive *"q follows from p"* statement and a formal *"if p then q"* statement. If this distinction is confusing, just keep in mind that

we are constructing a formal language to express mathematical ideas with; the *propositions* we express are written in our language, but we write our *proofs* of these propositions in our natural language, and our natural language is what we use to write down the rules and axioms that our language must obey. The *deduction rule* tells us that the result of our *proofs* can be converted into statements *within the formal language.*

Although this is a rather small collection of rules, it is capable of representing any kind of expressible propositional rhetoric. Despite that, it's not a *minimal* set of rules for the zeroth-order logic. In fact, it's possible to have an even smaller set of rules without sacrificing the rhetorical strength of our language. *Modus tollens,* for instance, could actually be shown to follow from the other rules of inference as a *theorem,* reducing our total number of assumptions. Let's prove it now.

Theorem 1.6 (Modus Tollens).
We have $\neg q, (p \to q) \vdash \neg p$ for any propositions p and q.

定理

Proof. Let p and q be arbitrary propositions, and suppose $\neg q$ and also $p \to q$. We know that $p \to q \equiv \neg q \to \neg p$,[1] so we have $\neg q \to \neg p$. Then, by *modus ponens,* we can conclude $\neg p$.

Q.E.D.

[1] This result—that a conditional statement is equivalent to its *contrapositive*—is left as an exercise to the reader.

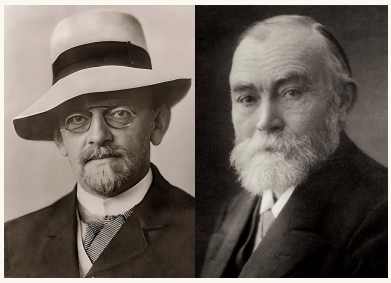

Figure 1.7: David Hilbert and Gottlob Frege were two of the most influential figures in the *logicist program* that was attempting to reduce mathematics to pure logic. Outside of logic, Hilbert was an extremely accomplished algebraist (maybe you've heard of Hilbert spaces in the context of linear algebra). Frege, while underappreciated during his life, is now recognized as one of the greatest and most profound mathematicians and philosophers of language of human history.

The interested reader might be excited to learn that *all* of propositional logic can be encoded using *just two connectives* ($\neg$ and $\to$) and *just three axioms* along with *modus ponens*. There are several classical *syllogisms* that have been studied since the time of the ancient Greeks. Before discussing these, we will first prove three important theorems.

Hilbert's System

The logical system we've set up so far—the axioms that establish the propositional calculus as a Boolean algebra, and our comprehensive rules of inference—is very user-friendly, but for this reason it is not *minimal.* We could have made our logical system more *"elegant"*—in some eyes—by choosing a shorter list of axioms and relying on only one rule of inference, at the consequence of having *much uglier* theorems and substantially more tedious proofs. Nonetheless, there is still benefit to be had by studying one of these *more minimal* axiomatizations, as it will provide us invaluable insight into proving a very important theorem: *conjunction elimination.* This alternative axiomatization for the propositional calculus is attributed to Hilbert and Frege. A modern, more condensed version of their system can be written using only two axioms without losing any expressive power. We now prove their axioms as *theorems of our system* below.

Theorem 1.7 (Hilbert's First Axiom).
$\vdash \varphi \to (\psi \to \varphi)$ for any propositions φ and ψ.

定理

Proof. Let φ and ψ be arbitrary propositions and assume φ.

Suppose ψ. We have φ by assumption. Thus, we have $\psi \vdash \varphi$ since we derived φ from ψ. By the *deduction rule*, we then obtain $\psi \to \varphi$.

We now have $\varphi \vdash (\psi \to \varphi)$, since we derived $\psi \to \varphi$ from φ. Therefore, we conclude $\varphi \to (\psi \to \varphi)$ by the *deduction rule.*

Q.E.D.

Theorem 1.8 (Hilbert's Second Axiom).
$\vdash (\varphi \to (\psi \to \xi)) \to ((\varphi \to \psi) \to (\varphi \to \xi))$ for any φ, ψ, and ξ.

定理

Proof. Let φ, ψ, and ξ be propositions and assume $\varphi \to (\psi \to \xi)$. We want to show $(\varphi \to \psi) \to (\varphi \to \xi)$. Towards that goal, assume $\varphi \to \psi$. We now want to show $\varphi \to \xi$; so, towards this goal, assume φ. Now,

$$\varphi, (\varphi \to (\psi \to \xi)) \vdash \psi \to \xi$$

by *modus ponens* using our earlier assumption, so we obtain $\psi \to \xi$. Again, by applying *modus ponens* to our prior assumption, we see that

$$\varphi, (\varphi \to \psi) \vdash \psi$$

leaves us with ψ. We now take these two intermediate results to deduce

$$\psi, (\psi \to \xi) \vdash \xi$$

using *modus ponens.* Therefore, we have derived ξ from our initial assumption φ, letting us conclude $\varphi \vdash \xi$.

We now apply the *deduction rule* several times to arrive at the conclusion. From $(\varphi \vdash \xi)$, we deduce $(\varphi \to \xi)$. Next, from $((\varphi \to \psi) \vdash (\varphi \to \xi))$, we deduce $((\varphi \to \psi) \to (\varphi \to \xi))$. Lastly, we take our expression $((\varphi \to (\psi \to \xi)) \vdash ((\varphi \to \psi) \to (\varphi \to \xi)))$ and finally derive $((\varphi \to (\psi \to \xi)) \to ((\varphi \to \psi) \to (\varphi \to \xi)))$.

Q.E.D.

Classical Syllogisms

We now follow in the footsteps of classical students of rhetoric, who in antiquity would ponder over these (and other) *syllogisms*—a traditional term referring to an argument where a conclusion is drawn from some collection of premises—as a way to hone our skills in the sister arts of proof-writing and deductive reasoning.

The following theorem allows us to construct and follow extended chains of conditional reasoning. Combined with *modus ponens,* this fundamentally forms the basis for any nontrivial argument.

Theorem 1.9 (Hypothetical Syllogism).
We have $(p \to q), (q \to r) \vdash p \to r$ for any propositions p, q, and r.

定理

Proof. Let p, q, and r be arbitrary propositions, and suppose $p \to q$ and $q \to r$. We will first show that $p \vdash r$. Assume p. Since $p \to q$, we have q by *modus ponens.* Further, since we have $q \to r$, we get r by *modus ponens.* Thus, $p \vdash r$. Therefore, by applying the *deduction rule,* we can conclude $p \to r$.

Q.E.D.

The next theorem is the converse of the *deduction rule.* When these two are taken together, they establish the formal, syntactic equivalence between the $\to$ and $\vdash$ symbols, which are semantically distinct.

Theorem 1.10 (Conditional Elimination).
We have $(p \to q) \vdash (p \vdash q)$ for any propositions p and q.

定理

Proof. Let p and q be arbitrary propositions, and suppose $p \to q$. We will now show that $p \vdash q$. Assume p. Then, since we have $p \to q$, we can derive q by *modus ponens.* Thus, $p \vdash q$.

Q.E.D.

Theorem 1.11 (Conjunction Introduction).
We have $p, q \vdash p \wedge q$ for any propositions p and q.

定理

Proof. Let p and q be arbitrary propositions. Assume p, and also separately assume q. Towards a contradiction, suppose $\neg(p \wedge q)$. [1] We can plainly see

$$\begin{aligned} \neg(p \wedge q) &\equiv \neg p \vee \neg q \quad \text{by } \textit{De Morgan's laws} \\ &\equiv p \to \neg q \quad \text{by } \textit{conditional disintegration}. \end{aligned}$$

So, we have $p \to \neg q$, from which we can derive $\neg q$ by *modus ponens.* This shows us that $\neg(p \wedge q) \to \neg q$ by the *deduction rule.* However, since we also had q by assumption, we can derive $\neg(p \wedge q) \to q$ using the *deduction rule* again. ↯ [2]

Therefore, we can conclude $p \wedge q$ by *reductio ad absurdum*.

Q.E.D.

[1] When beginning a *proof by contradiction,* it is good form to explicitly alert the reader to this fact with a phrase like *"towards a contradiction."*

[2] The symbol ↯ is useful in *proofs by contradiction* to highlight to the reader where the *contradiction* is and when it is reached.

In table 1.11, we summarize these results and some other theorems. We leave the proofs of these as an important list of exercises to the reader.

MODUS TOLLENS	$\neg q, (p \to q) \vdash \neg p$	
HYPOTHETICAL SYLLOGISM	$(p \to q), (q \to r) \vdash p \to r$	
CONDITIONAL ELIM.	$(p \to q) \vdash (p \vdash q)$	*a.k.a. the consolidation rule*
CONJUNCTION INTRO.	$p, q \vdash p \wedge q$	*a.k.a. adjunction*
CONJUNCTION ELIM.	$p \wedge q \vdash p$	*a.k.a. simplification*
DISJUNCTION INTRO.	$p \vdash p \vee q$	*a.k.a. addition*
DISJUNCTION ELIM.	$(p \to r), (q \to r), (p \vee q) \vdash r$	*a.k.a. proof by cases*
EX FALSO QUODLIBET	$p, \neg p \vdash q$	*a.k.a. explosion*
CONSTRUCTIVE DILEMMA	$(\alpha \to \gamma), (\beta \to \delta), (\alpha \vee \beta) \vdash \gamma \vee \delta$	

Table 1.11: Some useful theorems.

2

First-Order Logic

"I am in a charming state of confusion."

– Ada Lovelace

The language we have described so far is often called the *classical logic*—since this is a modern development on Aristotelian logic—or the *propositional logic* because its basic syntactic unit is the proposition. Having the proposition as the most granular accessible referent helps keep this language manageable, but it will hold us back from being as expressive as we'd like to be. For example, suppose we are hungry, and in the course of our ruminations we discover that shepherd's pie is irresistibly delicious. We also happen to know the same thing about paella. Having recognized these facts, no simple substitute will do: we *must* have one of these two meals if we are to be satisfied at all. How might we express this logically? Let's introduce some definitions.

$$s := \text{"We eat } \textit{shepherd's pie.}\text{"}$$
$$p := \text{"We eat } \textit{paella.}\text{"}$$
$$n := \text{"We do not eat } \textit{anything.}\text{"}$$

The claim we are trying to express would formally look as follows.

$$(\neg s \wedge \neg p) \rightarrow n \tag{2.1}$$

From the syntax above, it doesn't seem like there is any relationship between the premise of that conditional statement and its conclusion. In fact, there doesn't even appear to be a relationship between s and p, even though they are both saying something really similar, because *syntactically* they just look like two distinct propositions! Suppose our friend felt the same way as we do about food, but he additionally knew about a *secret third food:* the tostada. Our friend might then resolve to have *that* meal as a fall-back if he can't get his hands on shepherd's pie or paella. He would let $t :=$ "We eat *a tostada.*" and say the following.

$$(\neg s \wedge \neg p) \rightarrow t \tag{2.2}$$

English *shepherd's pie,* as God intended.


The humble *paella,* national dish of Spain.


Tostada & café, a classic Cuban breakfast.

Now, despite our two claims having the *exact same syntactic form*, they express remarkably different ideas. To realize this, think about what it would take to prove (2.1): after verifying $\neg s$ and $\neg p$, we would then need to show we did not eat *any other food!* This is a *universal claim* we are making about *all* possible meals. However, our friend is not making this kind of claim: his conclusion is simply that *there exists* a particular meal he eats if $\neg s$ and $\neg p$ are satisfied. To prove himself right, he simply has to show that he ate that particular meal.

2.1 A More Expressive Language

It will quickly become frustrating for our language to limit our expressivity like this. The missing component in our language is the ability to distinguish the *object* of our speech from the *predicate* description we make about it when we declare a proposition.

Every man is mortal.
Socrates is a man.
$\therefore$ Socrates is mortal.

The argument above seems like a clear, sensible argument; it in fact looks like a simple application of *modus ponens*. Yet, we realize that a proof of this argument in the propositional logic could not actually invoke *modus ponens*. There is no way to symbolize the first sentence in such a way that we obtain a conditional $x \to y$ where the premise is *"Socrates is a man,"* and if we can't do that then we can't apply *modus ponens*. We fix this issue by augmenting our language with the ability to *syntactically* distinguish between *predicates* and the *terms* they describe.

Definition 2.1 (Term).

term

A *term* is a symbol denoting an object. Specific terms—*e.g.*, the natural number 5, Socrates, shepherd's pie—are called *constants*. Placeholder terms denoting objects that have not been specifically determined are called *variables*. Notice that *terms, on their own, do not form complete sentences! A term does not have a truth value!*

Definition 2.2 (Predicate).

predicate

universe of discourse

Let $x_1, \dots x_n$ be variable symbols. We say $\varphi(x_1, \dots x_n)$ is an *n-ary predicate* if replacing each of the n variables $x_1, \dots x_n$ by terms $t_1, \dots t_n$ from our results in a *proposition* $\varphi(t_1, t_2, \dots t_n)$, carrying a truth value. The collection of all terms that our language has referential access to is our *universe of discourse*.

We've now introduced a new problem into our language though. Suppose we have define the predicates $\mu(x) :=$ "x is a man" and

$\theta(x) :=$ "x is mortal" in an attempt to translate the previous argument. We can now translate the second premise and conclusion as $\mu(\text{Socrates})$ and $\theta(\text{Socrates})$ respectively. But we still can't translate the first line. For this, we need the ability to express *quantities*.

universal
$\forall$

Let $\varphi(x_1, \dots x_i, \dots x_n)$ be an n-ary predicate containing a variable x_i. The *universal quantification* of the variable x_i appearing in φ is denoted $\forall x\big(\varphi(x_1, \dots x, \dots x_n)\big)$ and says *any constant* replacing x will satisfy φ.

```
def forall(universe: Iterable, phi: callable) -> bool:
  for x in universe:
    if not phi(x):
      return False
  return True
```

Figure 2.1: A hypothetical implementation of $\forall x\big(\varphi(x)\big)$. If `False` is returned, then there is at least one `x` in `universe` such that `phi(x) == False`, which is equivalent to $\forall x\big(\varphi(x)\big) \equiv \bot$. Otherwise, every `x` in `universe` will satisfy `phi(x) == True`, which means exactly that $\forall x\big(\varphi(x)\big) \equiv \top$.

existential
$\exists$

The *existential quantification* of x_i is denoted $\exists x\big(\varphi(x_1, \dots x, \dots x_n)\big)$ and claims that *there is at least one* constant that, in place of x, satisfies φ. The *scope* of a quantifier is denoted by parentheses specifying its variable's lifetime; that variable is *bound* to that quantifier within that scope. A

free variable

variable that is not bound to any quantifier is called *free*. Statements with free variables *cannot have truth values*, they do not carry *meaning*. If a statement has free variables, those variables need to either be replaced by *terms*, or be bound to a *quantifier*.

```
def exists(universe: Iterable, phi: callable) -> bool:
  for x in universe:
    if phi(x):
      return True
  raise False
```

Figure 2.2: A hypothetical implementation of $\exists x\big(\varphi(x)\big)$. If `True` is returned, then there must be an `x` in `universe` such that `phi(x) == True`, which is equivalent to $\exists x\big(\varphi(x)\big) \equiv \top$. Otherwise, every `x` in `universe` will satisfy `phi(x) == False`, so that $\exists x\big(\varphi(x)\big) \equiv \bot$.

unique existential
$\exists!$

We also introduce the *unique existential quantification* of x_i as a way of saying that *there is exactly one* constant satisfying φ in place for x. We use the notation $\exists! x\big(\varphi(x_1, \dots x, \dots x_n)\big)$, to denote this, which is read as *"there exists a unique x such that $\varphi(x)$"* in English.[1]

[1] This will be useful in future chapters.

$$\exists! x\big(\varphi(x)\big) \;:\Leftrightarrow\; \exists x\Big(\varphi(x) \wedge \forall y\Big(\varphi(y) \;\Rightarrow\; (y = x)\Big)\Big).$$

This is a special case of existential quantification; using the unique existential quantifier means making an existential claim *and additionally* asserting that only one such example exists. So, we define the $\exists!$ quantifier *in terms of* the $\exists$ quantifier. Be careful to note that the ! symbol in $\exists!$ *does not correspond with negating anything!* Do not make the mistake of confusing ! with $\neg$ if you have experience with a programming language where the ! syntax corresponds to logical negation.

Forming Formulæ Well

Definition 2.3 (Atomic Formula).

atomic formula

We say a formula φ is *atomic* if it satisfies the following recurrence.

1. $\varphi = \top$ or $\varphi = \bot$.
2. $\varphi = \psi(t_1, \dots t_n)$, where ψ is an n-ary predicate, $t_1, \dots t_n$ are terms.

Definition 2.4 (Well-Formed Formula).

well-formed formula

We say λ is a *well-formed formula*—often abbreviated *wff*—if it satisfies the following recurrence.

1. λ is an atomic formula.
2. $\lambda = \neg(\varphi)$, where φ is a *wff*.
3. $\lambda = (\varphi) \wedge (\psi)$, where φ and ψ are *wff*.
4. $\lambda = (\varphi) \vee (\psi)$, where φ and ψ are *wff*.
5. $\lambda = (\varphi) \to (\psi)$, where φ and ψ are *wff*.
6. $\lambda = (\varphi) \leftrightarrow (\psi)$, where φ and ψ are *wff*.
7. $\lambda = \forall x(\varphi)$, where φ is a *wff*.
8. $\lambda = \exists x(\varphi)$, where φ is a *wff*.

sentence

A well-formed formula with no free variables is called a *sentence in the first-order logic.* Looking at the above definitions, a *wff* that has no free variables will boil down to a *proposition,* meaning it will have a definite, unambiguous truth value. Sentences will be our primary mode for expressing conjectures, theorems, and proofs.

2.2 *Rules of Inference*

UNIVERSAL INTRODUCTION	$\varphi(t)$ for an *arbitrary* $t \vdash \forall x(\varphi(x))$	If we know $\varphi(t)$ and t is *arbitrary*, then we can say $\forall x(\varphi(x))$.
UNIVERSAL ELIMINATION	$\forall x(\varphi(x)) \vdash \varphi(t)$ for *any term* t	If we have $\forall x(\varphi(x))$, then we can pick *any* t and say $\varphi(t)$.
EXISTENTIAL INTRODUCTION	$\varphi(t)$ for a *particular* $t \vdash \exists x(\varphi(x))$	If we know $\varphi(t)$ for a *specific* term t, then we can say $\exists x(\varphi(x))$.
EXISTENTIAL ELIMINATION	$\exists x(\varphi(x)) \vdash \varphi(t)$ for a *new term* t	If we have $\exists x(\varphi(x))$, then we have $\varphi(t)$ for some t *that has not yet appeared.*

Table 2.1: The rules of inference for quantified expressions involving predicates. Note that the *"new term"* referred to by *existential elimination* must be a symbol that has not yet appeared in your proof.

When we were building the propositional logic, we first defined a *syntax* for our logic by introducing the logical connectives and some other special symbols; we then gave it an *algebraic semantics* when we introduced the equivalence axioms and the rules of inference. Now that we are augmenting our language with *terms, predicates, and quantifiers,*

we have a similar need to establish semantics for interpreting our new symbols. We introduce these rules in table 2.1. In addition, we have three important theorems involving quantified expressions, each containing a *universal* fragment and an *existential* fragment. This first theorem establishes a form of *De Morgan duality* between the $\forall$ and $\exists$ quantifiers: *negating* a quantified sentence is equivalent to quantifying the *negated* sentence using the *other* quantifier.

Theorem 2.1 (Negation of Quantifiers).
If φ is a predicate of at most one free variable, these equivalences hold.

$$\neg\forall x\big(\varphi(x)\big) \equiv \exists x\big(\neg\varphi(x)\big) \qquad \neg\exists x\big(\varphi(x)\big) \equiv \forall x\big(\neg\varphi(x)\big)$$

定理

The next theorem illustrates a sort of *distributive law* for quantifiers. Be sure to *pay careful attention to the parentheses* in the following theorem.

Theorem 2.2 (Distribution of Quantifiers).
Let φ be a predicate of at most one free variable and p be a proposition. The four equivalences below are then satisfied; mind the parentheses.

$$\forall x\big(\varphi(x)\big) \wedge p \equiv \forall x\big(\varphi(x) \wedge p\big) \qquad \exists x\big(\varphi(x)\big) \wedge p \equiv \exists x\big(\varphi(x) \wedge p\big)$$
$$\forall x\big(\varphi(x)\big) \vee p \equiv \forall x\big(\varphi(x) \vee p\big) \qquad \exists x\big(\varphi(x)\big) \vee p \equiv \exists x\big(\varphi(x) \vee p\big)$$

Further, if ψ is also a predicate with at most one free variable and t is a term, then the following four one-way inferences hold.

$$\forall x\big(\varphi(x) \wedge \psi(x)\big) \vdash \forall x\big(\varphi(x)\big) \wedge \psi(t) \qquad \exists x\big(\varphi(x)\big) \wedge \psi(t) \vdash \exists x\big(\varphi(x) \wedge \psi(x)\big)$$
$$\forall x\big(\varphi(x) \vee \psi(x)\big) \vdash \forall x\big(\varphi(x)\big) \vee \psi(t) \qquad \exists x\big(\varphi(x)\big) \vee \psi(t) \vdash \exists x\big(\varphi(x) \vee \psi(x)\big)$$

However, those inferences above are *not* equivalences, as shown below.

$$\forall x\big(\varphi(x)\big) \wedge \psi(t) \nvdash \forall x\big(\varphi(x) \wedge \psi(x)\big) \qquad \exists x\big(\varphi(x) \wedge \psi(x)\big) \nvdash \exists x\big(\varphi(x)\big) \wedge \psi(t)$$
$$\forall x\big(\varphi(x)\big) \vee \psi(t) \nvdash \forall x\big(\varphi(x) \vee \psi(x)\big) \qquad \exists x\big(\varphi(x) \vee \psi(x)\big) \nvdash \exists x\big(\varphi(x)\big) \vee \psi(t)$$

Finally, the following four equivalences hold for conditional statements.

$$\forall x\big(\varphi(x) \to p\big) \equiv \exists x\big(\varphi(x)\big) \to p \qquad \forall x\big(p \to \varphi(x)\big) \equiv p \to \forall x\big(\varphi(x)\big)$$
$$\exists x\big(\varphi(x) \to p\big) \equiv \forall x\big(\varphi(x)\big) \to p \qquad \exists x\big(p \to \varphi(x)\big) \equiv p \to \exists x\big(\varphi(x)\big)$$

定理

The third and final theorem concerns the *order of quantifiers*, importantly pointing out that *quantifiers don't necessarily commute with each other*.

Theorem 2.3 (Quantifier Shift).
If φ is a predicate of at most two free variables, then the following hold.

$$\forall x\forall y\big(\varphi(x,y)\big) \equiv \forall y\forall x\big(\varphi(x,y)\big) \qquad \exists x\exists y\big(\varphi(x,y)\big) \equiv \exists y\exists x\big(\varphi(x,y)\big)$$
$$\forall x\exists y\big(\varphi(x,y)\big) \nvdash \exists x\forall y\big(\varphi(x,y)\big) \qquad \exists x\forall y\big(\varphi(x,y)\big) \vdash \forall x\exists y\big(\varphi(x,y)\big)$$

定理

2.3 *The Art of Writing Proofs*

The way approach a proof of a statement principally depends on the *form* of the what we're trying to prove. Depending on what the statement *looks* like, a valid proof may be allowed to take certain liberties or be required to satisfy certain constraints. We will end this chapter with some words of advice for writing proofs based on the rules of inference we have established and the semantic interpretation we have attached to our various logical symbols. Since propositions and sentences in the first-order logic are *recursive* constructions, the first thing we should do when presented a statement to prove is to *recursively* analyze its *form.*

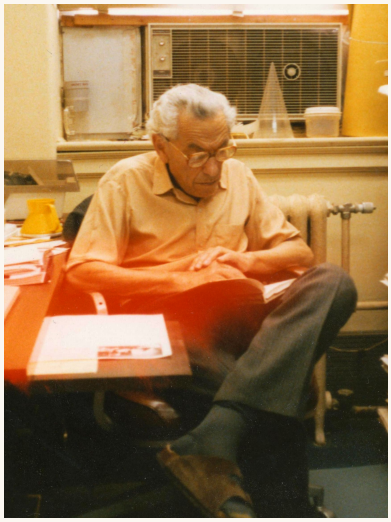

Figure 2.3: *"The purpose of life is to prove and to conjecture."* – Paul Erdős

Quantified Formulæ

If we are trying to prove a statement like $\forall x(\varphi(x))$, we can *check* $\varphi(t)$ *for all possible values of* t. This is usually not possible, as our universe of discourse often contains infinitely many objects. The natural alternative is to *introduce an arbitrary term* t and, without making any assumptions about t, to show that t satisfies φ. If we manage to do this without relying on any details pertaining to t specifically, then our argument *will generalize universally.* On the other hand, to prove a statement of the form $\exists x(\varphi(x))$, the task is to *find a specific object* t that we can prove satisfies φ. Existential claims are often the *most difficult* kind to prove because there is, generally, no clear strategy for *how* t should be found.

Figure 2.4: *"Another roof, another proof."* – Paul Erdős

Conditional Statements

Suppose we have a statement we want to prove that takes the form of a conditional $p \to q$. These are *by far the most common* kinds of statements we will be interested in proving. This involves showing we can derive q from p, so we first *assume* p in order to get to q. After assuming p is the case, we can think of how to derive q based on its *form* by again going through this analysis. Alternatively, instead of showing $p \to q$ directly, we can always think to prove $\neg q \to \neg p$ and apply our knowledge that a conditional statement is always equivalent to its contrapositive.

Junctions

Statements that look like $p \wedge q$ are relatively straight-forward: we have to show that *both* p *and* q are true. Similarly, showing $p \vee q$ requires deriving *one of either* p *or* q, but we are free to choose which one to pursue. Naturally, this will depend on what forms p and q take.

Nonconstructive Proofs

When, in the course of human events, it becomes necessary for one people to encounter a *contradiction*, a decent respect to the opinions of mankind requires that they should *reject the assumptions* that impelled them there. What we mean by this is: if you are ever stuck and feeling like a proposition p that you feel is insurmountable—for which you can see no way to make progress—try *assuming* $\neg p$ and seeing what happens. If this leads you to a *contradiction,* then you can invoke *reductio ad absurdum* and conclude p, washing your hands of the situation.

Ex falso quodlibet can be treated as a cousin to *reductio ad absurdum.* It is nowhere near as commonly used as a mode of reasoning, and to many it is far less intuitive than a simple proof by contradiction would be, but there are situations when it can be used to shortcut a proof in only a couple of lines. Keep an eye out for situations in which you are asked to prove a conditional statement $\bot \to q$ with a *false premise* because this rule will let you immediately reach your conclusion.

Mathematics

3

Foundations

"Finally I am becoming stupider no more."

– Paul Erdős

With the development of the first-order logic, we finally have a formal language for rigorous communication. This language has several incredibly nice properties: it's sufficiently expressive to prove any *universal* truth, while not being so unwieldy as to admit falsehoods or contradictions. The development of the first-order logic—along with Gödel's completeness and incompleteness theorems—marks one of humanity's greatest intellectual achievements, which would have ramifications throughout nearly every field of philosophy and natural science. With this language in hand, we are now ready to embark on our studies of *mathematics* proper. The natural first question we have to answer is: *what is our universe of discourse?* What *are* mathematical objects?

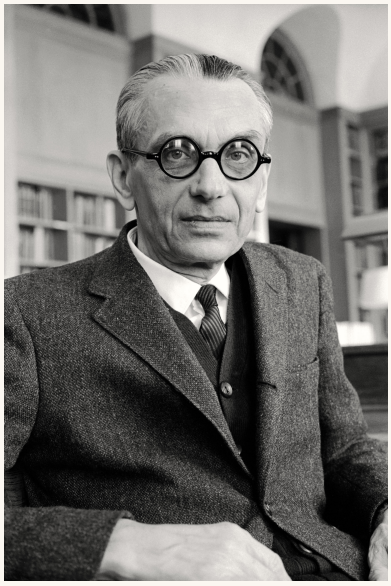

Figure 3.1: Kurt Gödel was an absolutely monumental figure in mathematical logic. He famously showed all universal truths in the first-order logic are provable (a property known as *completeness*). Despite that, he then infamously demonstrated there are mathematical truths that can *not* be proven (the *incompleteness* theorems).

3.1 *Informal Notions*

Thanks to insights made throughout the 20^{th} and 21^{st} centuries, there are actually several competing ways to answer this question (though the most *modern* and *"computer science"* of these formalisms would have required us to take a different logical foundation than the one we did). We will be taking a mainstream perspective that is fundamentally based on the concept of a *set*, but we will introduce two other useful kinds of objects in this section for convenience. *Technically* speaking, *every* object in our universe of discourse will be, or can be, *implemented as a set*, but it's often distracting to think of things like numbers as sets. As an analogy, think about the files on your computer. The PDF file you're reading these notes from is, fundamentally, a long binary number stored somewhere in your computer's memory. That number *represents* this PDF in the same way a set can represent a function, or the number 15, but if all you want to do is read these notes then it wouldn't be useful to interact with the binary *implementation* of the PDF.

Numbers

number

The most natural kinds of objects we should feel impelled to discuss are the *numbers*, and the most fundamental kind of number is, naturally, the *natural number*. Informally, these correspond precisely with the *non-negative whole numbers*. We can elegantly characterize these kinds of numbers with the following recurrence.

1. 0 is a natural number.
2. If n is a natural number, then $\mathcal{S}(n)$ is a natural number.

In the above recurrence, the notation $\mathcal{S}(n)$—read *"the successor of n"*—is referring to the *"next (whole) number after n."* This is the defining characteristic of the natural numbers, from which every other arithmetical property springs forth: begin somewhere (*i.e.*, at zero), and proceed by taking steps (*i.e.*, if n is a natural number, then so its the *next* one).

Figure 3.2: An initial segment of the natural number line, which begins at zero.

These will be a very important class of object for us to talk about, so we introduce them into our universe of discourse here. For now, we will be philosophical Platonists in the sense that we will simply believe the natural numbers exist *"out there, somewhere, in the ideal platonic realm of forms."* After we develop a bit more theory, we will be able to be more concrete about *what* precisely a number *is* formally-speaking.

Functions

function

A crucial part of the description of the natural numbers we just made is this notion of the *successor* of a natural number n. This idea is usually expressed in terms of the *successor function*, which begs us to define what a *function* is. For our purposes right now, a *function* is an object that *maps inputs from a domain* to *outputs in a codomain* in a *predictable way*. Specifically, a function *must produce exactly one output* for each of its valid inputs—the output will not change unless the input changes.[1] If we have a function named f and a valid input x, then the notation we will use to denote the output value f realizes on the input x is $f(x)$.[2]

$$\forall x \forall y \big(x = y \;\Rightarrow\; f(x) = f(y) \big)$$

With this notation, we express this idea more formally above, taking note that the quantifiers range over the collection of valid inputs for f. We throw function into our universe for now and revisit this later.

[1] Think about this informal definition and see if it agrees with the kinds of things you have been calling *"functions"* throughout your life so far.

[2] *"f of x,"* or *"f at x."*

Sets

Since functions are maps that transform inputs into outputs, we are finally driven to ask *"inputs from where?"* In the study of mathematics, all roads eventually lead to the idea of *a collection of things*. For a function, the collection of all valid inputs is usually called the *domain*, and the collection of all possible outputs is accordingly called the *codomain*. Numbers are typically used to measure quantities, which are collections of things. I could spend all day coming up with more examples, but I think you get the picture.

A notion of such *fundamental* importance to mathematics should therefore have a solid place in our universe of discourse. In fact, like the binary numbers that form the foundation for the files in your computer, these kinds of objects will form the basis upon which we build our mathematics. We will call these *sets*. In the following section, we will introduce sets *formally* by encoding their behavior in the form of a list of axioms, called the *Zermelo-Fraenkel axioms* of set theory.

set

	ENTAILMENT	EQUIVALENCE
Language	$\rightarrow$	$\leftrightarrow$
Metalanguage	$\vdash$	$\equiv$
Mathematics	$\Rightarrow$	$\Leftrightarrow$

Table 3.1: With the rules of inference and the theorems in table 1.11, we recognize the equivalence between $\rightarrow, \leftrightarrow$ syntactically and $\vdash, \equiv$ semantically. To simplify our notation, we replace these symbols with $\Rightarrow$, $\Leftrightarrow$ respectively.

As a final note, *we will be simplifying our notation from this section forward*. We had previously been introduced to the symbols $\rightarrow$ and $\leftrightarrow$ for expressing conditional statements *within* the language of the first-order logic. In the *metalanguage*—the language we are using right now to *talk about* the formal system we built—we used the $\vdash$ symbol to denote that some conclusions are derivable from some premises, and we used $\equiv$ to denote that two statements were logically indistinguishable. Given the theorems we proved in the last few chapters, the line between these two classes of symbols has been made blurrier, and it's typical in mainstream mathematical practice to ignore this distinction entirely. So, we now introduce the symbol $\Rightarrow$ to denote entailment as a replacement for the $\rightarrow$ and $\vdash$ symbols. Similarly, we introduce $\Leftrightarrow$ as a replacement for $\leftrightarrow$ and $\equiv$, denoting logical equivalence in all contexts.

$\Rightarrow$

$\Leftrightarrow$

Figure 3.3: Ernst Zermelo (left) produced one of the first axiomatizations of set theory in 1908, which was augmented in 1922 by Abraham Fraenkel (right) and also, independently, by Thoralf Skolem.

3.2 *Set Theory*

Intuitively, a *set* is a collection of objects. In this section, we will be *formally* developing the theory of sets by establishing the fundamental rules that sets must obey. These will be the *axioms of set theory*. From now on, our *universe of discourse* will be the *collection of all possible sets*,

and we will describe precisely *what* a set *is* by specifying the conditions that sets must satisfy in order to *provably exist*.

Definition 3.1 (The Predicates of Set Theory).

$\in$ The first predicate of set theory is $\in$, which stands for *elementhood*. When we write $x \in y$,[1] we mean to say that x is an element of y.

[1] "x is an element of y."

$=$ Our second predicate is $=$, which we use to denote *equality*. We will assume equality has the following straight-forward properties.

1. $\forall x(x = x)$ *reflexivity*
2. $\forall x \forall y\big((x = y) \Rightarrow (y = x)\big)$ *symmetry*
3. $\forall x \forall y \forall z\Big(\big((x = y \wedge y = z)\big) \Rightarrow (x = z)\Big)$ *transitivity*

These properties make equality an example of an *equivalence relation*.

Everything and anything we want to *formally* say about mathematical objects will be written in the first-order logic and expressed in terms of the $\in$ and $=$ predicates. As an example, suppose that A is a set, and that we know A contains the numbers 0 and 1 as elements. Then, we would simply say $(0 \in A) \wedge (1 \in A)$. Now, what if A could *only possibly* contain 0 and 1 as elements? That would then mean that, for any x, we have $x \in A \Rightarrow (x = 0) \vee (x = 1)$. Now, what if A contains *only* the numbers 0 and 1? Combining the two previous ideas, we would express this in the first-order logic by writing $\forall x\big(x \in A \Leftrightarrow (x = 0) \vee (x = 1)\big)$.

The concept that should begin to take shape from here on is that sets are abstractions of what it means to be a *a collection of objects*. Throughout the rest of this chapter, we will introduce *seven axioms* that will codify the rules for set theory, and each one of these axioms is an *intuitive consequence* of this concept. If we reflect deeply on the notion of *an arbitrary collection of objects*, then there are several properties that sets *must* have in order to properly capture that notion. Each of these axioms encodes one of these properties; as you read through the rest of the chapter, make sure you've extracted from each axiom the intuitive property underlying it.

Extensionality

Sets are entirely determined by their elements. If sets are nothing more than just abstract collections, we should be able to figure out any fact we need to know about a set just by looking at its elements. This naturally begs the question: what does it mean for two sets to be *equal?* Are the any of the sets in Figure 3.4 *equal* to each other despite looking so different? To answer this question, we need to look *inside* the sets and figure out whether or not they have the same elements. In this case,

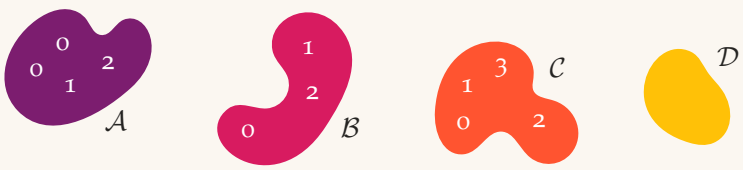

Figure 3.4: A visual representation of two sets. The *purple* set has the same elements as the *red* set, the figures refer to the same set, letting us infer $\mathcal{A} = \mathcal{B}$. The *orange* set contains an element not present in the other two sets, so $\mathcal{C} \neq \mathcal{A}$ and $\mathcal{C} \neq \mathcal{B}$. The *yellow* set has no elements, so it is empty.

we can see that $0 \in \mathcal{A}$, $1 \in \mathcal{A}$, and $2 \in \mathcal{A}$, and we also have that $0 \in \mathcal{B}$, $1 \in \mathcal{B}$, and $2 \in \mathcal{B}$. Even though the elements appear with different frequencies and in different positions between the two sets, it must be that $\mathcal{A} = \mathcal{B}$ because they have all the same elements. However, we can see that $3 \in \mathcal{C}$ while $3 \notin \mathcal{A}$, implying that $\mathcal{A} \neq \mathcal{C}$. In general, we should then expect sets to be equal precisely when they have the same elements, and that sets with the same elements should always be equal. This naturally brings us to the *axiom of extensionality*.

Axiom 1 (Extensionality).
$\forall x \forall y \Big((x = y) \;\Leftrightarrow\; \forall z (z \in x \;\Leftrightarrow\; z \in y) \Big)$.

公理

In our example above, we see that we could now *prove* that $\mathcal{A} = \mathcal{B}$ by first showing $\forall z (z \in \mathcal{A} \;\Leftrightarrow\; z \in \mathcal{B})$ and then invoking Axiom 1. In fact, this is essentially what we've done in the preceding paragraph; because $\mathcal{A}$ and $\mathcal{B}$ are both small, finite sets, by listing all the elements of each set and showing that they're also in the other, we have a proof of $\forall z (z \in \mathcal{A} \;\Leftrightarrow\; z \in \mathcal{B})$. *Extensionality* then lets us conclude that $\mathcal{A} = \mathcal{B}$.

By the same token, if we wanted to show that $\mathcal{A} \neq \mathcal{C}$, we would need to show $\neg \forall z (z \in \mathcal{A} \;\Leftrightarrow\; z \in \mathcal{C})$. We can see that

$$\begin{aligned}
\neg \forall z (z \in \mathcal{A} \;\Leftrightarrow\; z \in \mathcal{C}) &\equiv \exists z \neg (z \in \mathcal{A} \;\Leftrightarrow\; z \in \mathcal{C}) \\
&\equiv \exists z \neg \big((z \in \mathcal{A} \;\Rightarrow\; z \in \mathcal{C}) \wedge (z \in \mathcal{C} \;\Rightarrow\; z \in \mathcal{A}) \big) \\
&\equiv \exists z \big(\neg (z \in \mathcal{A} \;\Rightarrow\; z \in \mathcal{C}) \vee \neg (z \in \mathcal{C} \;\Rightarrow\; z \in \mathcal{A}) \big) \\
&\equiv \exists z \big(\neg (z \notin \mathcal{A} \vee z \in \mathcal{C}) \vee \neg (z \notin \mathcal{C} \vee z \in \mathcal{A}) \big) \\
&\equiv \exists z \big((z \in \mathcal{A} \wedge z \notin \mathcal{C}) \vee (z \in \mathcal{C} \wedge z \notin \mathcal{A}) \big),
\end{aligned}$$

so what we would need to do is *find* an element z that's *in* one of the two sets but *not in* the other. Since we saw that $3 \in \mathcal{C}$ but $3 \notin \mathcal{A}$, that's exactly what it means for $\mathcal{A} \neq \mathcal{C}$ by *extensionality*.

empty

∅

the empty set

What if the set has no elements? We say that a set $\mathcal{X}$ is *empty* by definition if $\forall x (x \notin \mathcal{X})$. Convince yourself first that it would make sense to talk about a set being empty.[1] We will use the symbol $\varnothing$ to refer to *the empty set*, meaning a set for which $\forall x (x \notin \varnothing)$ is satisfied. Clearly, it seems like $\mathcal{D}$ in Figure 3.4 is an example of such a set since it

[1] A good *intuitive* visual analogy might be to think about a set like a box; it should be clear that an empty box is still a box, despite not having anything inside of it.

doesn't contain any elements; is $\mathcal{D}$ equal to any of the other sets in that figure? Taking a look at Axiom 1, we see that 0 is an element of $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$, but $0 \notin \mathcal{D}$, so $\mathcal{D}$ can't be equal to any of those sets. In fact, $\mathcal{D}$ can't be equal to any *non-empty* set because that non-empty set would necessarily contain an element $\mathcal{D}$ doesn't. Are there any other sets that $\mathcal{D}$ might be equal to? In particular, is $\mathcal{D}$ equal to $\varnothing$, or are there multiple *distinct* empty sets? As you might have guessed by looking at the *axiom of extensionality*, the answer is *no!* All empty sets equal each other, so there is *only one* empty set, and we can say $\varnothing$ is *the* empty set.[1]

[1] Neither this analysis nor the following theorem *prove* that $\varnothing$ *exists*, only that any two empty sets must equal each other.

Theorem 3.1 (The Empty Set is Unique).
$\forall x\Big(\forall y\big(y \notin x\big) \;\Rightarrow\; x = \varnothing\Big)$.

定理

Proof. Let x be a set such that $\forall y\big(y \notin x\big)$. We will prove that $x = \varnothing$ by showing they have the same elements and applying Axiom 1.

Let z be a set. We will show $z \in x \;\Leftrightarrow\; z \in \varnothing$ by showing both directions.
If $z \in x$, notice $z \notin x$ follows from $\forall y\big(y \notin x\big)$. Thus, $z \in \varnothing$ by *explosion*.
If $z \in \varnothing$, then $z \neq z$ by definition; but, $z = z$. So, $z \in x$ by *explosion*.
Since $z \in x \;\Leftrightarrow\; z \in \varnothing$, the *axiom of extensionality* grants us $x = \varnothing$.

Q.E.D.

Pairing

set builder

To make our lives easier, let's introduce a bit of *notation.* Given finitely many terms $x_0, x_1, \ldots x_n$, we will denote by $\{x_0, x_1, \ldots x_n\}$ the set[2] whose elements are *exactly* the objects $x_0, x_1, \ldots x_n$. We write out each element of the set explicitly[3] and separate the elements with commas, with the formal understanding that, for any z,

[2] This *does not* assert *existence* of the set.

[3] We can do this because there are only *finitely many* of them, though this might be annoying to do for large finite sets.

$$z \in \{x_0, x_1, \ldots x_n\} \;:\Leftrightarrow\; (z = x_0) \vee (z = x_1) \vee \ldots (z = x_n).$$

This is often called *set builder notation*. From Figure 3.4, we can use this notation to say $\mathcal{A} = \{0, 0, 1, 2\}$ and $\mathcal{B} = \{0, 2, 1\}$, while $\mathcal{C} = \{0, 1, 3, 2\}$. This also gives us a convenient way to denote the empty set as $\varnothing = \{\}$. With this notation, our next axiom is relatively simple.

Axiom 2 (Pairing).
$\forall x \forall y \exists z\Big(z = \{x, y\}\Big)$.

公理

All this says is that given two sets, we can take those sets and *pair* them up inside of a new set containing just those two guys as elements. In other words, this lets us construct *unordered pairs* out of existing sets.

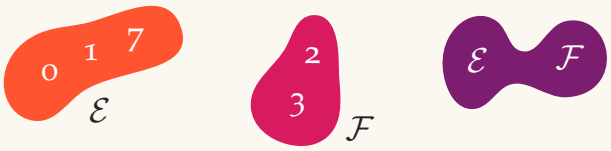

Figure 3.5: Given the sets $\{0,1,7\}$ and $\{2,3\}$ exist, the *pairing axiom* asserts existence of $\{\{0,1,7\},\{2,3\}\}$ containing both sets.

Separation

What if we want to talk about a set with so many elements that it would be cumbersome—or impossible—to write them all down with set builder notation? For instance, how would we write down the set of even natural numbers? If we can identify a *predicate* $\varphi(\cdot)$ that characterizes[1] all of the elements z of this set, then we can refer to the set by writing $\{z \mid \varphi(z)\}$.[2] To represent the set of even natural numbers, we could then simply write $\{n \mid (n \in \mathbb{N}) \wedge (n \text{ is even})\}$ by implicitly defining the predicate $\varphi(x) :=$ "$(x \in \mathbb{N}) \wedge (x \text{ is even})$."[3] Again, we should be clear to heed the warning: just because we have this new notation *does not mean* every time we define a predicate $\psi(t)$ that the string of symbols $\{x \mid \psi(x)\}$ *actually refers to a set that exists*.

unrestricted set comprehension

[1] Recall that *properties* are formally encoded by *predicates* in the first-order logic.

[2] *"The set of all z such that $\varphi(z)$."*

[3] We will learn how to formally express *"x is even"* in the next chapter.

If you think this is a needlessly pedantic obsession, let's see what happens if we drop our guard. Let's define the predicate $\beta(r) :=$ "$r \notin r$." This is a perfectly sensible, innocuous, unassuming predicate. Just as a sanity check, remind yourself about $\mathcal{A}$ from Figure 3.4 and observe that $\mathcal{A} \notin \mathcal{A}$ because $\mathcal{A} \notin \{0,1,2\}$. $\mathcal{A}$ thus satisfies β, meaning $\beta(\mathcal{A})$ is true.

Now, let $\mathfrak{R} := \{x \mid \beta(x)\} = \{x \mid x \notin x\}$, and let's try to see whether $\mathfrak{R}$ makes $\beta(\cdot)$ true or false.[4] If $\beta(\mathfrak{R})$ is the case, then $\mathfrak{R} \notin \mathfrak{R}$ by the definition of β. That means that $\mathfrak{R} \in \{x \mid \beta(x)\}$; but then $\mathfrak{R} \in \mathfrak{R}$. ↯ Well, what happens if $\neg\beta(\mathfrak{R})$ is the case instead? Then, we must have $\neg(\mathfrak{R} \notin \mathfrak{R})$, so that $\mathfrak{R} \in \mathfrak{R}$, meaning $\mathfrak{R} \in \{x \mid \beta(x)\}$ by definition. However, if $\mathfrak{R} \in \{x \mid \beta(x)\}$, then $\mathfrak{R}$ satisfies β, so that $\mathfrak{R} \notin \mathfrak{R}$. ↯

[4] Remember that, since $\beta(\cdot)$ is a *predicate*, substituting its free variable with a term yields a *proposition* equivalent to $\top$ or $\bot$.

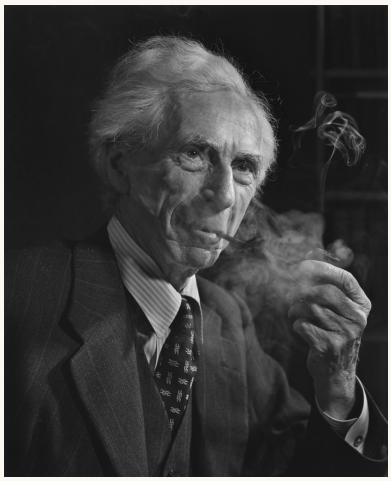

Figure 3.6: Russell's paradox is named after eminent mathematician and philosopher Bertrand Russell. He first mentioned this paradox in a letter to logician and philosopher Gottlob Frege as a critique of his *"Basic Law V,"* which was essentially an *unrestricted* form of comprehension for logical functions.

It seems like no matter what we do, we run into a problem because the *existence* of an object like $\mathfrak{R}$ is *inherently contradictory*. We can not allow things like $\mathfrak{R}$ into our universe of discourse or our logical system will explode. This observation—that the *"set"* of all sets that don't contain themselves doesn't exist—is known as *Russell's paradox*, and it should point out to us that we can not allow *unrestricted* use of set comprehension notation. However, if we *restrict* ourselves to using comprehension only to filter elements from sets that already exist, we can completely avoid the issue of Russell's paradox. By being careful to only use this *restricted* form of *comprehension*, we can enshrine the existence of sets whose elements are filtered—or *separated*—from another existing set with a predicate by introducing our next axiom.

Russell's paradox

Axiom 3 (Schema of Separation).
Given a predicate φ with at most one free variable, we have $\forall x \exists y \Big(y = \{ z \mid z \in x \wedge \varphi(z) \} \Big)$.

公理

Technically, *separation* is called an *axiom schema* because it is actually one axiom for each predicate φ. We can't write this as just one sentence because we can't quantify over predicates; we can only quantify over objects in our universe of discourse—which are sets in this case.

subset
$\subseteq$

The kinds of sets Axiom 3 produces have elements that all belong to another set. When two sets $\mathcal{X}$ and $\mathcal{Y}$ have this relationship, where every element of $\mathcal{X}$ is an element of $\mathcal{Y}$, we say $\mathcal{X}$ is a *subset* of $\mathcal{Y}$. Formally, we define $\mathcal{X} \subseteq \mathcal{Y} \ :\Leftrightarrow \ \forall z (z \in \mathcal{X} \ \Rightarrow \ z \in \mathcal{Y})$. With this new definition,

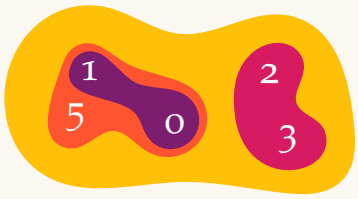

Figure 3.7: The *orange*, *red*, and *purple* sets are all subsets of the *yellow* set. We can see $\textit{purple} \subseteq \textit{orange}$, but $\textit{orange} \not\subseteq \textit{purple}$. Further, $\textit{orange} \not\subseteq \textit{red}$, and $\textit{red} \not\subseteq \textit{orange}$, implying $\textit{purple} \not\subseteq \textit{red}$, and $\textit{red} \not\subseteq \textit{purple}$.

restricted set comprehension

we can see that the point of the *axiom of separation* is the ability to take *arbitrary subsets of existing sets.* Since this notion is so important and will be coming up so often, we will introduce the compact $\{ z \in \mathcal{X} \mid \varphi(z) \}$[1] notation with exactly the same meaning as $\{ z \mid z \in \mathcal{X} \wedge \varphi(z) \}$ given a set $\mathcal{X}$ and a predicate φ. To summarize, for any z we have the following.

[1] *"The set of all z in $\mathcal{X}$ such that $\varphi(z)$."*

$$z \in \{ x \mid \varphi(x) \} \ :\Leftrightarrow \ \varphi(z)$$
$$z \in \{ x \in \mathcal{X} \mid \varphi(x) \} \ :\Leftrightarrow \ z \in \mathcal{X} \wedge \varphi(z)$$

...where $\mathcal{X}$ is a set and φ is a predicate.

We also make sure to note $\{ x \in \mathcal{X} \mid \varphi(x) \} = \{ x \mid x \in \mathcal{X} \wedge \varphi(x) \}$.

With these definitions and axioms, we can now prove a couple of important results. First, as you might have guessed, the concept of subsets is inextricably related to the idea of equality for sets. In fact, if two sets are both subsets of one-another, then they *must* be equal.

Theorem 3.2.
For any sets x and y, we have $(x = y) \ \Leftrightarrow \ \Big((x \subseteq y) \wedge (y \subseteq x) \Big)$.

定理

Proof. Let x and y be sets. Since we are trying to prove an $\Leftrightarrow$ statement, we need to show both the $\Rightarrow$ and $\Leftarrow$ directions.

First, assume $x = y$. By the *axiom of extensionality*, $\forall z \big(z \in x \ \Leftrightarrow \ z \in y \big)$. Let z be a set. If $z \in x$, then $z \in y$ by the above axiom, proving $x \subseteq y$. Similarly, if $z \in y$, then $z \in x$ by that same axiom, proving $y \subseteq x$.

Now, suppose $(x \subseteq y) \wedge (y \subseteq x)$ and let z be a set. If $z \in x$, then $z \in y$ because $x \subseteq y$. Conversely, if $z \in y$, we have $z \in x$ because $y \subseteq x$. Therefore, $z \in x \ \Leftrightarrow \ z \in y$, proving $x = y$ by *extensionality*.

Q.E.D.

An immediate corollary is that every set is a subset of itself.

***Corollary* 3.1.**
For any set x, we have $x \subseteq x$.

推論

Proof. Let x be a set. We will show that $\forall z(z \in x \;\Rightarrow\; z \in x)$. Let z be a set and assume $z \in x$. Then clearly $z \in x$. Thus, $z \in x \;\Rightarrow\; z \in x$. Since z was arbitrary, we conclude $x \subseteq x$ by definition.

Q.E.D.

At some point, our attention will be drawn back to the empty set: since it has no elements, is it a subset of any sets? Well, from the above corollary we know at least that $\varnothing \subseteq \varnothing$. Is $\varnothing$ a subset of $\{0, 1, 2\}$? What about $\mathbb{N}$? In order for $\varnothing$ to be a subset of *any* set, we would need *every* element of $\varnothing$ needs to be present in the other set. How could that be possible if $\varnothing$ has no elements?

***Theorem* 3.3.**
For any set x, we have $\varnothing \subseteq x$.

定理

Proof. Let x be a set. We will show that $\forall z(z \in \varnothing \;\Rightarrow\; z \in x)$. Let z be a set and assume $z \in \varnothing$. By definition, we know $\forall w(w \notin \varnothing)$, so $z \notin \varnothing$. Then, by the *principle of explosion*, we get $z \in x$. Since $z \in \varnothing \;\Rightarrow\; z \in x$ and z was arbitrary, we conclude $\varnothing \subseteq x$.

Q.E.D.

We introduce another convenient notation for sets $\mathcal{X}$ and predicates φ.

$$(\forall x \in \mathcal{X})\big(\varphi(x)\big) \;:\Leftrightarrow\; \forall x\big(x \in \mathcal{X} \;\Rightarrow\; \varphi(x)\big)$$ *"For all x in $\mathcal{X}$: $\varphi(x)$."*

$$(\exists x \in \mathcal{X})\big(\varphi(x)\big) \;:\Leftrightarrow\; \exists x\big(x \in \mathcal{X} \wedge \varphi(x)\big)$$ *"There is some x in $\mathcal{X}$ such that $\varphi(x)$."*

Notice that, when we say $(\forall x \in \mathcal{X})\big(\varphi(x)\big)$, this is *all one statement*. We are *not* saying "$\forall x \in \mathcal{X}$"[1] nor "$\varphi(x)$"[2] nor any combination of those statements by themselves because these independent expressions are not sentences! *They do not mean anything by themselves!*

[1] "$\forall x \in \mathcal{X}$" is nonsense on its own because nothing is actually being said about the x elements of $\mathcal{X}$; there is no *clause.*

[2] "$\varphi(x)$" is nonsense on its own because we don't know who x is; closed sentences can't contain *free variables.*

Union

So far, the only two ways we have of making new sets is by pairing up existing sets using Axiom 2 and by taking subsets using Axiom 3. Intuitively, why shouldn't we be able to take two boxes of things and empty both of their contents into one bigger box? Why shouldn't we be able to *merge* sets together? We definitely would like to!

union
$\cup$

Given two sets $\mathcal{X}$ and $\mathcal{Y}$, we define the *union* of those two sets as $\mathcal{X} \cup \mathcal{Y} \coloneqq \{z \mid (z \in \mathcal{X}) \vee (z \in \mathcal{Y})\}$. This is the set consisting of all of

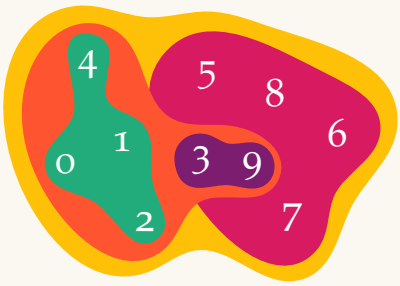

Figure 3.8: In this figure the *orange set* is $\{0,1,2,3,4,9\}$ and the *red set* is $\{3,5,6,7,8,9\}$. The *yellow set* is the *union* of the two sets, consisting of $\{0,1,2,3,4,5,6,7,8,9\}$. The *purple set* is their *intersection*, consisting of $\{3,9\}$. The *green set* consisting of $\{0,1,2,4\}$ is the difference $\{0,1,2,3,4,9\} \setminus \{3,9\}$.

the elements of $\mathcal{X}$ in addition to all of the elements of $\mathcal{Y}$ together. As a way of bolstering your intuition: if the sets we're dealing with are small enough to be *iterated over,*[1] then the union of two sets could be computed with code fragment in Figure 3.9.

[1] We'll expand on this later when we study the *sizes* of sets more formally.

```
def union(xs: set, ys: set) -> set:
    zs = set()
    for x in xs:
        zs.add(x)
    for y in ys:
        zs.add(y)
    return zs
```

Figure 3.9: A simple implementation of the union of two sets in `Python`. We compute `zs` $\coloneqq$ `xs` $\cup$ `ys` by iterating over every element of `xs` and of `ys` and successively adding them to the empty set `set()`. This implementation is obviously cumbersome and inefficient; `Python` actually provides a built-in operator for taking unions, so we could have just written `return xs | ys`.

Now, if we were to stop here and introduce an axiom along the lines of *"the union of two existing sets always exists,"* then we would only ever be able to take the union of *finitely many* sets,[2] but why should we limit ourselves like this? If we have a bunch of sets collected together in a reasonable way, why shouldn't we be allowed to union *all* of them at once? Why not *iterate* the $\cup$ operation *over* all of the sets we want to merge, collecting their elements into one larger set? As it turns out, as long as the sets we want to union are small-enough in number to all fit inside of another set, then there's nothing stopping us from doing this.

[2] Convince yourself of this. How would you take the union of infinitely many sets if you're only allowed pairwise unions?

union over $\cup$

Given a set $\mathcal{X}$, we define the *union over* $\mathcal{X}$, meaning the *iterated* union over the *elements* of $\mathcal{X}$, as $\cup\mathcal{X} \coloneqq \{z \mid (\exists y \in \mathcal{X})(z \in y)\}$. As before, the code in Figure 3.10 provides an example implementation of the idea.

```
def union(xs: set) -> set:
    zs = set()
    for ys in xs:
      for z in ys:
        zs.add(z)
    return zs
```

Figure 3.10: A simple implementation of the union over a set in `Python`. We compute the union over `xs` by iteratively merging the elements of `xs` with the empty set `set()`. A more compact way to write this would have been simply `return {z for z in ys for ys in xs}`.

Since these latter kinds of unions are more general than the former, we will dedicate our next axiom to saying *"unions over existing sets exist."*

Axiom 4 (Union).
$\forall x \exists y (y = \cup x)$.

公理

Notice that the *union axiom* only asserts the existence of unions *over* sets that exist; it does *not* say that the union of *two* existing sets exists. It's up to us now to prove it for ourselves.

Theorem 3.4 (Existence of Unions).
$\forall x \forall y \exists z (z = x \cup y)$.

定理

Proof. Let x and y be sets. By the *pairing axiom*, $A \coloneqq \{x, y\}$ exists. Then, we know that $\cup A$ exists by the *union* axiom, with the recognition that $\cup A = \{b \mid (\exists a \in A)(b \in a)\}$ by definition. Recall that, by definition, $x \cup y = \{w \mid w \in x \vee w \in y\}$. Then, for any z, we have

$$
\begin{aligned}
z \in \cup A &\Leftrightarrow z \in \{b \mid (\exists a \in A)(b \in a)\} && \text{by definition of } \cup A \\
&\Leftrightarrow (\exists a \in A)(z \in a) && \text{by definition of set comprehension} \\
&\Leftrightarrow \exists a (a \in A \wedge z \in a) && \text{by definition of the notation} \\
&\Leftrightarrow \exists a (a \in \{x, y\} \wedge z \in a) && \text{by definition of } A \\
&\Leftrightarrow z \in x \vee z \in y && \text{by definition of set builder notation} \\
&\Leftrightarrow z \in \{w \mid w \in x \vee w \in y\} && \text{by definition of set comprehension} \\
&\Leftrightarrow z \in x \cup y && \text{by definition of } x \cup y.
\end{aligned}
$$

Thus, $\cup A = x \cup y$, so $x \cup y$ exists thanks to the *union axiom*.

Q.E.D.

The *schema of separation* synergizes well with the *union axiom*, allowing us to prove that many useful set-theoretic constructions are possible. Two important ones that we would be remiss to leave out are the *intersection* and the *difference* of two sets. If $\mathcal{X}$ and $\mathcal{Y}$ are sets, then their *intersection* is the set of all elements they *share in common*. This is defined as $\mathcal{X} \cap \mathcal{Y} \coloneqq \{z \mid z \in \mathcal{X} \wedge z \in \mathcal{Y}\}$. Just as with unions, we have an analogous notion of the *intersection over* a set $\mathcal{X}$, which is the intersection operation iterated over all of the elements of $\mathcal{X}$. We define this by $\cap \mathcal{X} \coloneqq \{z \mid (\forall y \in \mathcal{X})(z \in y)\}$. Do not make the mistake of assuming that $\cap \mathcal{X}$ always exists just because $\cup \mathcal{X}$ does! Axiom 4 does not say anything about intersections, so this requires its own analysis. However, the intersection of any two sets *does* exist.

intersection $\cap$

intersection over $\cap$

Theorem 3.5 (Existence of Intersections).
$\forall x \forall y \exists z (z = x \cap y)$.

定理

set minus

The *difference* of $\mathcal{X}$ with $\mathcal{Y}$ refers to the set obtained by *removing* all of

the elements of $\mathcal{Y}$ from $\mathcal{X}$. This is defined using the bizarre notation $\mathcal{X} \setminus \mathcal{Y} \coloneqq \{z \mid z \in \mathcal{X} \wedge z \notin \mathcal{Y}\}$. As with the intersection of two sets, the difference of two arbitrary sets always exists.

\

Theorem* 3.6 *(Existence of Differences).
$\forall x \forall y \exists z (z = x \setminus y)$.

定理

Power

Another seemingly natural operation we would like to perform on sets is to take an existing set and collect *all of its subsets* together into a set. Although it might seem like we already have the power to do that if we flex the *axiom of separation* along with our earlier axioms, it turns out we can't. Although we can construct each *individual* subset of a given set $\mathcal{X}$, there's no way for us to collect *all* of those subsets together in one set.This collection, called the *power set* of $\mathcal{X}$, is defined as $\mathcal{P}(\mathcal{X}) \coloneqq \{x \mid x \subseteq \mathcal{X}\}$. It'll become very important in a few chapters, but we will establish its existence now with the *power axiom*.

power set

$\mathfrak{P}$

Axiom* 5 *(Power).
$\forall x \exists y \big(y = \mathcal{P}(x)\big)$.

公理

Note that $\mathfrak{P}$ is an upper-case letter *"$\mathcal{P}$"*—as in $\mathfrak{power}$—and is often denoted that way when writing by hand and in other resources you might encounter. You may also see the notation $2^{\mathcal{X}}$ to denote the power set since it is an example of an exponential object. This ties in with the fact that a set with n elements will have a power set containing 2^n elements; we will have more to say about this in a later chapter.

Regularity

You may have wondered by this point, either based on the problem sets or out of your own curiosity, whether or not sets can contain themselves as elements. You may even believe that, because of results like Russell's paradox, sets obviously can't contain themselves. While your intuition would be correct, and any physical analogies you might be making to yourself that sets are *"sort of like boxes or containers"* would bolster that intuition, there is actually nothing so far that would prohibit $x \in x$ to be true for some set x. As simple people interested in doing reasonable and computable mathematics, we shouldn't allow sets like $x = \{x\}$ to exist. So, we introduce the *axiom of regularity*.

Axiom* 6 *(Regularity).
$\forall x \big(x \neq \varnothing \;\Rightarrow\; (\exists y \in x)(x \cap y = \varnothing)\big)$.

Figure 3.11: The axiom of regularity was introduced by John von Neumann to facilitate the study of the ordinal numbers. An important philosophical consequence of this axiom is that sets are not allowed to be elements of themselves.

公理

This strangely written axiom has far-reaching consequences, one of which is that *there are no infinitely descending $\in$-chains.* For our purposes, we only need it to establish the fact that *sets do not contain themselves*.

Theorem 3.7 (Well-Foundedness of Elementhood).
$\forall x(x \notin x)$.

定理

Proof. Let x be a set and suppose, towards a contradiction, that $x \in x$. Consider $A \coloneqq \{z \mid z \in x \wedge z = x\}$, which we know exists by the *axiom schema of separation*. Observe that $A = \{x\}$ because $\forall z(z \in A \Leftrightarrow z = x)$. Then, A must be disjoint with one of its elements by the *axiom of regularity*. This implies $A \cap x = \varnothing$. However, since $x \in A$ and $x \in x$, we know $x \in A \cap x$, so that $A \cap x \neq \varnothing$. ↯ Therefore, $x \notin x$.

Q.E.D.

Infinity

Finally, we arrive at what is perhaps the most important axiom of all. The close reader may have noticed by this point that *none* of the previous axioms are *existentially* quantified. The question then becomes: *do any sets actually exist?* Of course, we *need* sets to exist so that we have things to *talk about.* The only way to do this is with an *existential* axiom, and what better set to introduce than the set of natural numbers?

Every single one of them is of the form $\forall x(\dots)$. Even if there are existential quantifications inside of those parentheses, the outer-most quantifier is *universal*.

Axiom 7 (Infinity).
The set of natural numbers $\mathbb{N} \coloneqq \{0, 1, 2, \dots\}$ exists.[1]

公理

[1] For the time being, this axiom is written *informally.* At the end of this chapter, we will reintroduce this axiom *formally.*

Now that we have the existence of $\mathbb{N}$, we can prove the existence of myriad sets. Particularly, we can finally prove that the empty set exists.

Theorem 3.8 (Existence of the Empty Set).
$\exists x(x = \varnothing)$.

定理

Proof. Recall that $\mathbb{N}$ exists by the *axiom of infinity*. Consider the set $\mathcal{E} \coloneqq \{z \in \mathbb{N} \mid z \neq z\}$. We know from *separation* that $\mathcal{E}$ exists, and we will now show $\mathcal{E}$ is empty. Let n be a set and assume, towards a contradiction, that $n \in \mathcal{E}$. Then, we know $(n \in \mathbb{N}) \wedge (n \neq n)$ by definition, so that $n \neq n$ in particular. However, we also know that $n = n$ because equality is reflexive. ↯

This implies $\forall x(x \notin \mathcal{E})$, so $\mathcal{E} = \varnothing$. We conclude $\varnothing$ exists since $\mathcal{E}$ exists.

Q.E.D.

3.3 *Arithmetic*

Now that we have the natural numbers, how do we do *arithmetic?* This should be an almost impulsive desire as soon as we've established the existence of $\mathbb{N}$. How can we approach this topic formally if we don't even know *what* a natural number *is?* Instead of directly answering this question, we will work backwards by first building our intuition of

The first thing to notice is that the natural numbers are structured in a very nice way. They have a determined starting point—the number 0—and they can be listed off iteratively by finding the *"next"* number in the sequence. If this seems obvious, the reader is encouraged to think of an example of a number set that doesn't have this nice property.

We model arithmetic on $\mathbb{N}$ by making the following observations.

1. $0 \in \mathbb{N}$.
2. $(\forall n \in \mathbb{N})\big(\mathcal{S}(n) \neq 0\big)$.
3. $(\forall n \in \mathbb{N})\big(\mathcal{S}(n) \in \mathbb{N}\big)$.
4. $(\forall n \in \mathbb{N})(\forall m \in \mathbb{N})\big(\mathcal{S}(n) = \mathcal{S}(m) \;\Rightarrow\; n = m\big)$.
5. If φ is a predicate with at most one free variable, then we have $\Big(\varphi(0) \wedge (\forall k \in \mathbb{N})\Big(\varphi(k) \;\Rightarrow\; \varphi\big(\mathcal{S}(k)\big)\Big)\Big) \;\Rightarrow\; (\forall n \in \mathbb{N})\big(\varphi(n)\big)$.

This model of arithmetic is referred to as *Peano arithmetic*. We will define the arithmetic operations on natural numbers *recursively*.

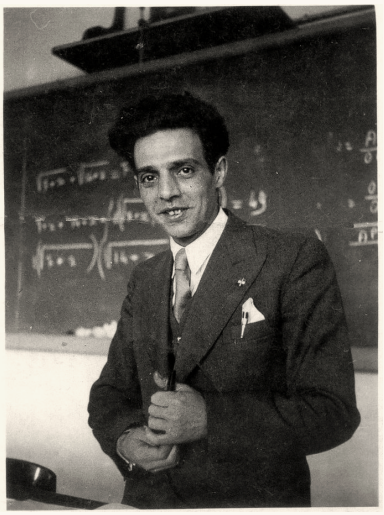

Figure 3.12: Giuseppe Peano was one of the founders of mathematical logic and set theory. As a young man, some of his contributions include the $\cup$ and $\cap$ notation for sets, his eponymous axiomatization of arithmetic, and the first-ever example of a space-filling curve.

Definition 3.2 (Arithemtical Operations).
We define *addition* between natural numbers recursively as follows.

$$\begin{cases} n+0 \coloneqq n \\ n+\mathcal{S}(m) \coloneqq \mathcal{S}(n+m) \end{cases}$$

We define *multiplication* between natural numbers recursively below.

$$\begin{cases} n\cdot 0 \coloneqq 0 \\ n\cdot\mathcal{S}(m) \coloneqq (n\cdot m)+n \end{cases}$$

We define *exponentiation* for natural numbers as follows.

$$\begin{cases} n^0 \coloneqq 1 \\ n^{\mathcal{S}(m)} \coloneqq (n^m)\cdot n \end{cases}$$

If a and b are natural numbers, we say that a is *less than or equal to* b when we can find a natural number $c \in \mathbb{N}$ such that $a + c = b$. Formally, $a \leqslant b \;:\Leftrightarrow\; (\exists c \in \mathbb{N})(a + c = b)$.

***Theorem* 3.9.**
$(\forall n \in \mathbb{N})\big(\mathcal{S}(n) = n + 1\big)$.

定理

Proof. Let $n \in \mathbb{N}$ and observe

$$\begin{aligned} n + 1 &= n + \mathcal{S}(0) && \text{because } 1 \coloneqq \mathcal{S}(0) \\ &= \mathcal{S}(n + 0) && \text{by definition of addition} \\ &= \mathcal{S}(n) && \text{by definition of addition.} \end{aligned}$$

Therefore, $\mathcal{S}(n) = n + 1$.

Q.E.D.

Theorem* 3.10 *(Associativity of Addition).
$(\forall a \in \mathbb{N})(\forall b \in \mathbb{N})(\forall c \in \mathbb{N})\big(a + (b + c) = (a + b) + c\big)$.

定理

Proof. Let $a \in \mathbb{N}$ and $b \in \mathbb{N}$. We will prove this by induction on $c \in \mathbb{N}$.

Basis Step: By definition of addition, $a + (b + 0) = a + b = (a + b) + 0$.

Inductive Step: Let $k \in \mathbb{N}$ and assume $a + (b + k) = (a + b) + k$.[1] We now need to show that $a + \big(b + \mathcal{S}(k)\big) = (a + b) + \mathcal{S}(k)$. Observe

$$\begin{aligned} a + \big(b + \mathcal{S}(k)\big) &= a + \mathcal{S}(b + k) && \text{by definition of addition} \\ &= \mathcal{S}\big(a + (b + k)\big) && \text{by definition of addition} \\ &= \mathcal{S}\big((a + b) + k\big) && \text{by the } \textit{inductive hypothesis} \\ &= (a + b) + \mathcal{S}(k) && \text{by definition of addition,} \end{aligned}$$

so that $a + \big(b + \mathcal{S}(k)\big) = (a + b) + \mathcal{S}(k)$ as desired.

Therefore, $(\forall c \in \mathbb{N})\big(a + (b + c) = (a + b) + c\big)$.

Q.E.D.

[1] This is our *inductive hypothesis*.

Definition* 3.3 *(Iterated Sums & Products).
Let $x_0, x_1, x_2, \ldots$ is a sequence of natural numbers and $m, n \in \mathbb{N}$. We recursively define the *iterated sum* of $x_m, x_{m+1}, \ldots x_n$ as follows.

$$\begin{aligned} \sum_{i=m}^{n} x_i &\coloneqq 0 && \text{if } m > n \\ \sum_{i=m}^{n} x_i &\coloneqq x_m && \text{if } m = n \\ \sum_{i=m}^{n+1} x_i &\coloneqq \left(\sum_{i=m}^{n} x_i\right) + x_{n+1} && \text{if } m < n \end{aligned}$$

```python
def sum(nums: list) -> int:
    if len(nums) == 0:
        return 0
    elif len(nums) == 1:
        return nums[0]
    else:
        return sum(nums[:-1]) + nums[-1]
```

Figure 3.13: A recursive implementation of iterated summation in `Python`.

We similarly define the *iterated product* of $x_m, x_{m+1}, \ldots x_n$ as follows.

$$\prod_{i=m}^{n} x_i := 1 \qquad \text{if } m > n$$
$$\prod_{i=m}^{n} x_i := x_m \qquad \text{if } m = n$$
$$\prod_{i=m}^{n+1} x_i := \left(\prod_{i=m}^{n} x_i\right) \cdot x_{n+1} \qquad \text{if } m < n$$

```python
def prod(nums: list) -> float:
    if len(nums) == 0:
        return 0
    elif len(nums) == 1:
        return nums[0]
    else:
        return prod(nums[:-1]) * nums[-1]
```

Figure 3.14: A recursive implementation of iterated multiplication in `Python`.

3.4 *The Lifting of the Veil*

Definition* 3.4 *(Successor Function).
$S(x) := x \cup \{x\}$

Definition* 3.5 *(Natural Numbers).
We define the natural numbers recursively as follows.

$$0 := \varnothing$$
$$\mathcal{S}(n) := n \cup \{n\}$$

3.5 *Concrete Algebra*

Figure 3.15: Évariste Galois.
[1] in the sense that the `ASCII` letter `x` and the `unicode` letter `x` are not *technically* same, but are the same *in spirit*

Now that we've had a serious encounter with the foundations of mathematics, we will introduce a few important number sets and learn some of their basic algebraic properties. In the interest of time, we won't be *constructing* each of these sets nor will we *prove* each of these properties, but rest assured that there is a formal way to construct each of these sets and prove their properties directly from the axioms.

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

The above chain of inclusions, while not *technically* true in standard set theory, is *true in spirit*.[1] We obtain the different number sets by augmenting the natural numbers with some desirable algebraic properties.

$\mathbb{N}_+$ For convenience, we will define $\mathbb{N}_+ := \mathbb{N} \setminus \{0\}$.

The Natural Semiring

$\mathbb{N}$ The *natural numbers* $\mathbb{N} = \{0, 1, 2, \ldots\}$ are the canonical *ordered semiring*.

***Theorem* 3.11.**
commutative monoid The naturals are a *commutative monoid* under *addition* with *identity* 0.

- $(\forall x \in \mathbb{N})(0 + x = x)$.[2]
- $(\forall x, y, z \in \mathbb{N})(x + (y + z) = (x + y) + z)$.[3]
- $(\forall x, y \in \mathbb{N})(x + y = y + x)$.[4]

[2] *existence of additive identity*
[3] *associativity of addition*
[4] *commutativity of addition*

定理

***Theorem* 3.12.**
They are also a *commutative monoid* under *multiplication* with *identity* 1.

- $(\forall x \in \mathbb{N})(1 \cdot x = x)$.[5]
- $(\forall x, y, z \in \mathbb{N})(x \cdot (y \cdot z) = (x \cdot y) \cdot z)$.[6]
- $(\forall x, y \in \mathbb{N})(x \cdot y = y \cdot x)$.[7]

[5] *existence of multiplicative identity*
[6] *associativity of multiplication*
[7] *commutativity of multiplication*

定理

***Theorem* 3.13.**
commutative semiring *Multiplication* interacts nicely with *addition*.

- $(\forall x, y, z \in \mathbb{N})(x \cdot (y + z) = (x \cdot y) + (x \cdot z))$.[8]
- $(\forall x \in \mathbb{N})(0 \cdot x = 0)$.[9]

[8] *distributivity*
[9] *annihilation*

定理

Theorem 3.14.
Addition and *multiplication* are *monotonic.*

ordered semiring

- $(\forall x, y, z \in \mathbb{N})((x \leqslant y) \Rightarrow (x + z \leqslant y + z))$.[1]
- $(\forall x, y, z \in \mathbb{N})((x \leqslant y \wedge 0 \leqslant z) \Rightarrow (x \cdot z \leqslant y \cdot z))$.[2]

[1] *addition is monotonic*

[2] *multiplication is monotonic*

定理

The Integer Ring

$\mathbb{Z}$

The *integers* $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ extend $\mathbb{N}$ by introducing *additive inverses*[3] for every element and inheriting all of the previous properties. An algebraic structure with all the properties of a monoid, but which also has inverses for every element, is called a *group*.

group

[3] If $\mathfrak{A}$ with operation $\star$ is an algebraic structure with identity element $e_\star$, then we say $b \in \mathfrak{A}$ is an *inverse* for $a \in \mathfrak{A}$ with respect to $\star$ if $a \star b = e_\star$. Depending on the context, we may denote the inverse of a by $-a$ or a^{-1} when it exists.

Theorem 3.15.
The integers form a *(commutative) group* under addition.

- $(\forall z \in \mathbb{Z})(\exists w \in \mathbb{Z})(z + w = 0)$.

定理

An algebraic structure with two operations that is a *commutative group* under one and a *monoid* under the other and where the latter operation distributes over the former is called a *ring*. If the operations are both monotonic, then we call it an *ordered ring*, and the integers $\mathbb{Z}$ are the canonical example of such a structure.

ring
ordered ring

The Rational Field

$\mathbb{Q}$

The set of *rational* numbers $\mathbb{Q} = \left\{ p/q \mid p \in \mathbb{Z} \wedge q \in \mathbb{N}_+ \right\}$ extends $\mathbb{Z}$ by introducing *multiplicative inverses* for every *nonzero* element.

Theorem 3.16.
The nonzero rationals form a *(commutative) group* under multiplication.

- $(\forall q \in \mathbb{Q})(q \neq 0 \Rightarrow (\exists r \in \mathbb{Q})(q \cdot r = 1))$.

定理

Every ring with this additional property is called a *field*. With the inherited properties from the integers, $\mathbb{Q}$ is the canonical *ordered field*.

field
ordered field

The Continuum

The set of real numbers $\mathbb{R}$ augments the set of rationals by including a limit point for every Cauchy-convergent sequence of rational numbers.

All of these number sets happen to be *cancellative* with respect to both of their operations and thus have *no nonzero zero divisors*.

***Theorem* 3.17.**
Let $\mathfrak{A}$ be any of $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ with its standard addition and multiplication operations. Then, we have the following four statements.

- $(\forall x, y, z \in \mathfrak{A})(x = y \;\Rightarrow\; (x + z = y + z \wedge x \cdot z = y \cdot z))$.[1]
- $(\forall x, y, z \in \mathfrak{A})(x + z = y + z \;\Rightarrow\; x = y)$.[2]
- $(\forall x, y, z \in \mathfrak{A})(z \neq 0 \wedge x \cdot z = y \cdot z \;\Rightarrow\; x = y)$.[3]
- $(\forall x, y \in \mathfrak{A})(x \cdot y = 0 \;\Leftrightarrow\; (x = 0 \vee y = 0))$.[4]

[1] *addition and multiplication are functions*

[2] *additive cancellation*

[3] *multiplicative cancellation*

[4] *domain property*

定理

Index