DANIEL GONZALEZ CEDRE

DISCRETE MATHEMATICS

UNIVERSITY OF NOTRE DAME

1st June, 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

Logic

Mathematics

Notation

SYNTAX		SEMANTICS
$\top$	*"True."*	A *true* sentence; a tautology.
$\bot$	*"False."*	A *false* sentence; a contradiction.
$x := y$	*"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 collection containing only a, b, c.
$\{x \mid \varphi(x)\}$	*"the set of all x such that $\varphi(x)$"*	The collection whose elements are 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 collection 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 $f(x) \in \mathcal{B}$.
$\mathfrak{s}(n)$	*"the successor of n"*	The next natural number after n.
$\mathbb{N}$	*"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.
$\mathbb{P}(x)$	*"the power set of x"*	The set of all subsets of x.

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*
🟥	*Definition*
🟧	*Pronunciation*
🟫	*Internal link*
🟩	External link

Table 2: Color legend.

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

Table 3: Notation for organizing topics. These glyphs will be used to demarcate definitions, theorems, lemmas, *etc.*

GLYPH	NAME	IPA
A α	*alpha*	[a]
B β	*beta*	[v]
Γ γ	*gamma*	[ɣ]
Δ δ	*delta*	[ð]
E ε	*epsilon*	[e]
Z ζ	*zeta*	[z]
H η	*eta*	[ɛː]
Θ θ	*theta*	[θ]
I ι	*iota*	[iː]
K κ	*kappa*	[k]
Λ λ	*lambda*	[l]
M μ	*mu*	[m]
N ν	*nu*	[n]
Ξ ξ	*xi*	[ks]
O o	*omicron*	[o]
Π π	*pi*	[p]
P ρ	*rho*	[r]
Σ σ	*sigma*	[s]
T τ	*tau*	[t]
Υ υ	*upsilon*	[yː]
Φ φ	*phi*	[f]
X χ	*chi*	[k^{h}]
Ψ ψ	*psi*	[ps]
Ω ω	*omega*	[ɔː]

Table 4: The Greek alphabet. Each glyph in the alphabet is given first in upper-case and then in lower-case along with its English name and the IPA pronunciation.

GLYPH	NAME	IPA
א	*aleph*	[ø]
ב	*bet*	[v]
ג	*gimel*	[ɣ]
ד	*dalet*	[ð]
ה	*he*	[h]
ו	*waw*	[v]
ז	*zayin*	[z]
ח	*chet*	[χ]
ט	*tet*	[t]
י	*yod*	[j]
ך	*kaf*	[x]
ל	*lamed*	[l]
ם	*mem*	[m]
ן	*nun*	[n]
ס	*samech*	[s]
ע	*ayin*	[ʔ]
ף	*pe*	[f]
ץ	*tsadi*	[ts]
ק	*qof*	[k]
ר	*resh*	[ʁ]
ש	*shin*	[ʃ]
ת	*tav*	[θ]

Table 5: The Hebrew abjad. Only non-final variations of each glyph are shown.

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

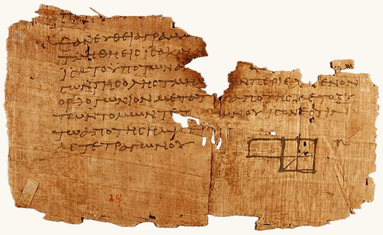


Figure 1: A fragment of book 2 from Euclid's *Elements* taken from the Oxyrhynchus papyri, dated ca. 100 AD.

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.

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.

[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.

[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.

axiom

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 (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 of the interior angles. 公理

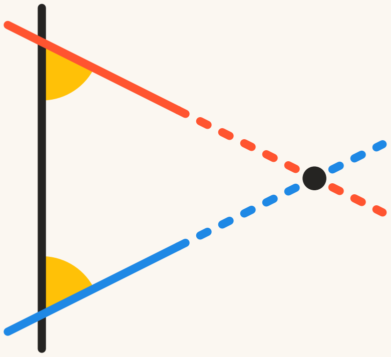


Figure 2: The parallel postulate says that any two lines 🟥 and 🟦 that make acute interior angles ▶ and ▶ with a third line ▬ must intersect at a point ●.

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.

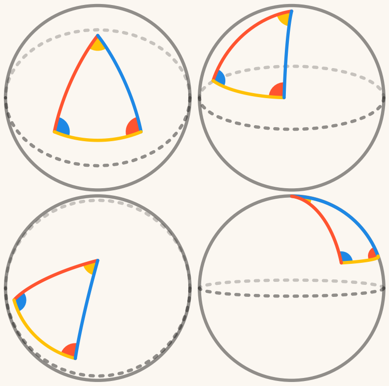


Figure 3: Four views of the same triangle whose angles sum to 270 degrees. Notice how the notions of *straight* and *parallel* differ on the surface of a sphere.

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.*

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 ostracized for decades, causing him to suffer serious depressive crises.

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

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

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

[4] We will study these later.

Once again, mathematicians' *intuitive notions of how infinity should behave* were being contradicted. 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 20^{th} century to *fix* mathematics by establishing it on a firm *logical foundation.*[1]

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*

semantics
syntax
variable
term

Languages encode ideas into sequences of symbols.[2] 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[3] that stands in place for an object that has not been determined yet.[4] We can assign a name to a *particular* object with the := symbol. We call these the *terms* of an expression.

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."

定義

Mathematical practice principally involves *making and justifying observations about mathematical objects.*[5] 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.

[1] This ambitious project would eventually fail with the discovery of Kurt Gödel's infamous *incompleteness theorems.*

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

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

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

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

[5] 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 be described by a *Turing machine*. 直覺

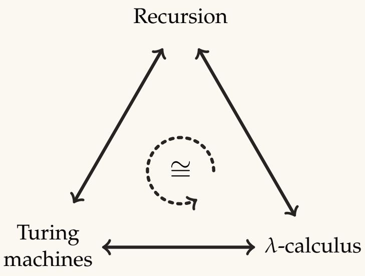


Figure 4: The Church-Turing thesis states that these three concepts—which are all *formally* equivalent—correspond with our *informal* notion of computability. In modern times, many people now take this as a definition for computability.

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 underlying 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 and 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 $17 + 2 = 19$.

$$\begin{align} 3 + 5 + 9 + 2 &= 3 + 5 + 9 + 2 \tag{1}\\ &= 8 + 9 + 2 \tag{2}\\ &= 8 + 9 + 2 \tag{3}\\ &= 17 + 2 \tag{4}\\ &= 17 + 2 \tag{5}\\ &= 19 \tag{6} \end{align}$$

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 $x_0 + x_1 + x_2 + \dots x_{n-2} + x_{n-1}$, we *first* need to compute $x_0 + x_1 + x_2 + \dots x_{n-2}$ and then add that result to x_{n-1}.

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

[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.

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

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 describes the *recurrence.*

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]

This paragraph encounters the *basis.*

recurrence relation

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

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*—*a.k.a. base case*—does exactly this by providing explicit answers to the *smallest* versions of the problem.

recurrence

basis

[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.

1

Zeroth-Order Logic

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

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?*

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

1.1 Truth Values

Let's consider the following declarative sentence.

$$\text{"Ahab is a captain."} \tag{1.1}$$

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
$\top$

$$\text{"Ishmael is a whale."} \tag{1.2}$$

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 $\perp$ for sentences of this kind.

false
$\perp$

The symbols $\top$ and $\perp$ 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] 定義

Axiom (Propositional 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*

This establishes $\equiv$ is an example of an *equivalence relation.* 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 $\sigma_{1.3}$.

$$\text{“Colorless green ideas sleep furiously.”} \tag{1.3}$$

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?

$$\text{“Colorless green ideas \textit{do not} sleep furiously.”} \tag{1.4}$$

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

nonsense

that sentence *has no truth value!* We call expressions like this *nonsensical* because they *carry no semantic meaning.*

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

[2] being (or not) logically equivalent

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

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

$$\text{“This sentence is \textit{false}.”} \tag{1.5}$$

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]

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

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

[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.

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

Table 1.2: Truth table for negations.

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

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

$$\text{“Espresso is not delicious.”} \tag{1.6}$$

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 $\sigma_{1.7}$.

$$\text{“Espresso is delicious.”} \tag{1.7}$$

negation

$\neg$

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 $\sigma_{1.6} \equiv \neg\sigma_{1.7}$.

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]

Conjunctions and Disjunctions

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

$$\text{“Espresso is delicious, and it nourishes the soul.”} \tag{1.8}$$

Table 1.3: Truth table for logical conjunctions and disjunctions.

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

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
$\wedge$

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

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

“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.”

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.

$$\text{“Espresso is delicious, or it nourishes the soul.”} \tag{1.9}$$

We call these connectives *dual* to each other because negating all of the inputs to one of them is equivalent to negating the output of the other.

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 $\neg$ gives the same result as applying $\neg$ after g on *all possible* inputs. 定義

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

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

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.

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 → symbol and defined in *table* 1.5.

implication
→

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

The antecedent and consequent for $\sigma_{1.10}$ are defined above. With these definitions, we can now write $\sigma_{1.10} \equiv p_{1.10} \rightarrow q_{1.10}$ 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 a $\mathcal{B}$ 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]

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

Table 1.5: Truth table for conditionals.

p	q	$p \rightarrow q$	$p \leftrightarrow q$
$\top$	$\top$	$\top$	$\top$
$\top$	$\bot$	$\bot$	$\bot$
$\bot$	$\top$	$\top$	$\bot$
$\bot$	$\bot$	$\top$	$\top$

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

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

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

[3] $\top \rightarrow \top \equiv \top$

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

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

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

"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

$\leftrightarrow$

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.

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. $\lambda = (\varphi) \rightarrow (\psi)$ where φ and ψ are propositions.
6. $\lambda = (\varphi) \leftrightarrow (\psi)$, where φ and ψ are propositions.

定義

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 lets us verify statements like $((\neg\top) \wedge (\bot \wedge \top)) \rightarrow \top$ are indeed propositions by recursively decomposing it until we reach the bases.

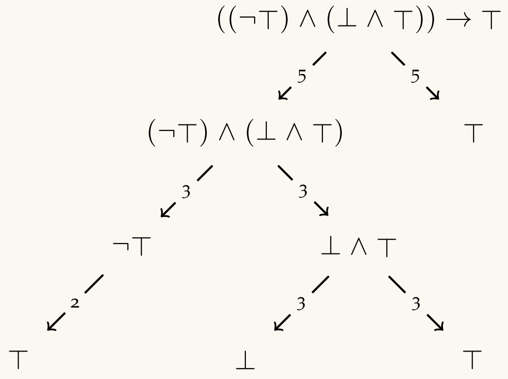


Figure 1.2: In this example, we have dropped some unambiguous parentheses for clarity. Notice, however, that some parentheses *cannot* be dropped: for example, those around the premise of the $\rightarrow$ conditional, and those separating the arguments of the two $\wedge$ conjunctions. If those parentheses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

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

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

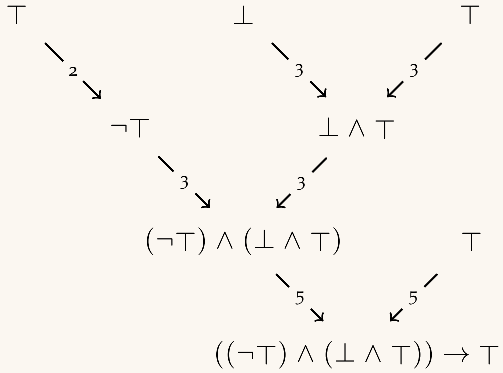

$\top$
$\bot$
$\top$
2
3
3
$\neg\top$
$\bot \wedge \top$
3
3
$(\neg\top) \wedge (\bot \wedge \top)$
$\top$
5
5
$((\neg\top) \wedge (\bot \wedge \top)) \to \top$

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. 定義

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.

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

Equivalent propositions are essentially the same when we view them through the lens of truth values.[1]

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 $\varphi(p_1, p_2, \ldots p_n) \overset{?}{\equiv} \psi(p_1, p_2, \ldots p_n)$ 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*.[2]

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

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*

[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.

[2] 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.

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).

logical equivalence

$\equiv$

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 non equivalence

$\not\equiv$

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 $\varphi \not\equiv \psi$. 定義

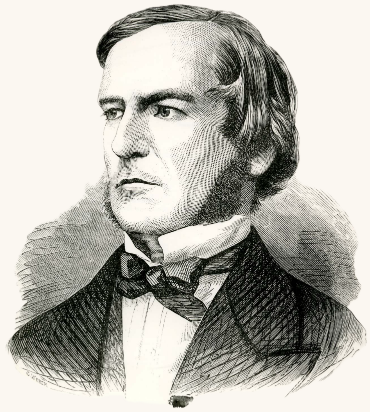


Figure 1.4: George Boole, a largely self-taught mathematician, logician, and philosopher, first described the eponymous *Boolean algebra* in his 1854 monograph *The Laws of Thought*.

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

Theorem* 1.1 *(Uniqueness of Complements).
For any 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.

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

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 $q \equiv \neg p \wedge q$. Thus, 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.

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

[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.

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 then 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.

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

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

[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 ...

meant to correspond to those truth values. We can now prove this as a *corollary*—a simple consequence—of *theorem* 1.1.

***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 $\top \vee \bot \equiv \top$ by the *identity* axiom. Thus, $\bot \equiv \neg\top$ by *theorem* 1.1. Q.E.D.

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

[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, $p := \bot$ and $q := \top$). That means, having satisfied the premises, we get to assert the conclusion, justified by that theorem.

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.

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 p acts like the negation of $\neg p$. Observe $\neg p \wedge p \equiv p \wedge \neg p \equiv \bot$ by *commutativity* and the *complement* axiom. Similarly, $\neg p \vee p \equiv p \vee \neg p \equiv \top$ by *commutativity* and *complement*. Therefore, $p \equiv \neg(\neg p)$ by *theorem* 1.1. Q.E.D.

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]

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

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

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. We first prove the conjunctive fragment.

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

[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.

$$\begin{aligned}
&\equiv p \lor \neg p && \text{by } \textit{idempotence}\\
&\equiv \top && \text{by } \textit{complement}
\end{aligned}$$

The disjunctive fragment works out similarly.

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

We therefore conclude $p \lor \top \equiv \top$ and $p \land \bot \equiv \bot$. Q.E.D.

Theorem* 1.5 *(De Morgan's Laws).
$\neg(p \land q) \equiv \neg p \lor \neg q$ and $\neg(p \lor q) \equiv \neg p \land \neg q$ for any p and q. 定理

Proof. Let p and q be propositions. We will leave the proof of $\neg(p \lor q) \equiv \neg p \land \neg q$ as an exercise to the reader.

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

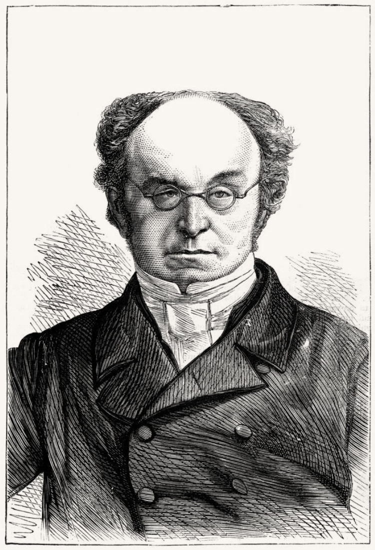


Figure 1.6: Augustus De Morgan, after whom these laws are named, is also notable for his work on logical quantification and mathematical induction.

In the conjunctive branch above, we derived $(p \land q) \land (\neg p \lor \neg q) \equiv \bot$. We show $(p \land q) \lor (\neg p \lor \neg q) \equiv \top$ in the disjunctive branch below.

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

Therefore, by *theorem* 1.1, we conclude $\neg(p \land q) \equiv \neg p \lor \neg q$ 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.

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 permit *one-way*, *inferential* arguments. 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

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

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

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

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.[1]

The next rule, named *reductio ad absurdum*,[2] 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.[3]

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 $\neg q, (p \rightarrow q) \vdash \neg p$ for any propositions p and q. 定理

Proof. Let p and q be arbitrary propositions, and suppose $\neg q$ and also $p \rightarrow q$. We know that $p \rightarrow q \equiv \neg q \rightarrow \neg p$,[4] so we have $\neg q \rightarrow \neg p$. Then, by *modus ponens,* we can conclude $\neg p$. Q.E.D.

The interested reader might be excited to learn that *all* of propositional logic can be encoded using *just two connectives* ($\neg$ and $\rightarrow$) and *just three*

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

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

[3] 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.

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

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.

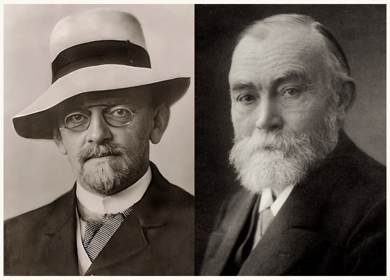


Figure 1.7: David Hilbert and Gottlob Frege were two of the most influential figures in the *logicist program* that was attempting to reduce mathematics to pure logic. Outside of logic, Hilbert was an extremely accomplished algebraist (maybe you've heard of Hilbert spaces in the context of linear algebra). 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.

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, which we now prove as theorems 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, 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.* Since we derived ξ from φ, we can assert $\varphi \vdash \xi$.

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, 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 (Implication 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 the following chain of equivalences.

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

[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."*

So, we have $p \to \neg q$, from which we can derive $\neg q$ by *modus ponens.* However, since already we had q, we now have a contradiction. ↯ [1]

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

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	$(p \to q), (q \to r) \vdash p \to r$	
IMPLICATION 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.

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

2

First-Order Logic

> *"I am in a charming state of confusion."*
>
> – Ada Lovelace

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

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.

$$\begin{aligned} s &:= \text{“We eat \textit{shepherd's pie}.”} \\ p &:= \text{“We eat \textit{paella}.”} \\ n &:= \text{“We do not eat \textit{anything}.”} \end{aligned}$$

The humble *paella*, national dish of Spain.

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

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

Tostada & café, a classic Cuban breakfast.

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.

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

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.

$$\begin{array}{rl} & \text{Every man is mortal.} \\ & \text{Socrates is a man.} \\ \hline \therefore & \text{Socrates is mortal.} \end{array}$$

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!* 定義

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.* 定義

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

"For all x, $\varphi(x_1, \ldots x, \ldots x_n)$."

```
def forall(universe, predicate):
    for x in universe:
        if not predicate(x):
            return False
    return True
```

Figure 2.1: A hypothetical implementation of $\forall x(\varphi(x))$. If it returns `False`, then there is at least one `x` in `universe` such that `predicate(x) == False`, which is equivalent to $\forall x(\varphi(x)) \equiv \bot$. Otherwise, every `x` satisfies `predicate(x) == True`, meaning $\forall x(\varphi(x)) \equiv \top$.

existential

$\exists$

free variable

The *existential quantification* of x_i is denoted $\exists x\big(\varphi(x_1, \ldots x, \ldots x_n)\big)$ 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 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*. Because this will be useful in the future, 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 $\exists! x\big(\varphi(x_1, \ldots x, \ldots x_n)\big)$ to denote this, and read this in English as *"there exists a unique x such that $\varphi(x)$."*

"There exists x such that $\varphi(x_1, \ldots x, \ldots x_n)$."

```
def exists(universe, predicate):
    for x in universe:
        if predicate(x):
            return True
    return False
```

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

unique existential

$\exists!$

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

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 (Formulæ).

atomic formula

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

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

well-formed formula

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

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. $\lambda = \forall x\big(\varphi\big)$, where φ is a *wff*.
8. $\lambda = \exists x\big(\varphi\big)$, 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. 定義

2.2 *Rules of Inference*

UNIVERSAL INTRODUCTION	$\varphi(t)$ for an *arbitrary* $t \vdash \forall x\big(\varphi(x)\big)$	If we know $\varphi(t)$ and t is *arbitrary*, then we can say $\forall x\big(\varphi(x)\big)$.
UNIVERSAL ELIMINATION	$\forall x\big(\varphi(x)\big) \vdash \varphi(t)$ for *any term* t	If we have $\forall x\big(\varphi(x)\big)$, then we can pick *any* t and say $\varphi(t)$.
EXISTENTIAL INTRODUCTION	$\varphi(t)$ for a *particular* $t \vdash \exists x\big(\varphi(x)\big)$	If we know $\varphi(t)$ for a *specific* term t, then we can say $\exists x\big(\varphi(x)\big)$.
EXISTENTIAL ELIMINATION	$\exists x\big(\varphi(x)\big) \vdash \varphi(t)$ for a *new term* t	If we have $\exists x\big(\varphi(x)\big)$, 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.

$$\begin{array}{ll}
\forall x\big(\varphi(x)\big) \land p \equiv \forall x\big(\varphi(x) \land p\big) & \exists x\big(\varphi(x)\big) \land p \equiv \exists x\big(\varphi(x) \land p\big) \\
\forall x\big(\varphi(x)\big) \lor p \equiv \forall x\big(\varphi(x) \lor p\big) & \exists x\big(\varphi(x)\big) \lor p \equiv \exists x\big(\varphi(x) \lor p\big)
\end{array}$$

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.

$$\begin{array}{ll}
\forall x\big(\varphi(x) \land \psi(x)\big) \vdash \forall x\big(\varphi(x)\big) \land \psi(t) & \exists x\big(\varphi(x)\big) \land \psi(t) \vdash \exists x\big(\varphi(x) \land \psi(x)\big) \\
\forall x\big(\varphi(x) \lor \psi(x)\big) \vdash \forall x\big(\varphi(x)\big) \lor \psi(t) & \exists x\big(\varphi(x)\big) \lor \psi(t) \vdash \exists x\big(\varphi(x) \lor \psi(x)\big)
\end{array}$$

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

$$\begin{array}{ll}
\forall x\big(\varphi(x)\big) \land \psi(t) \nvdash \forall x\big(\varphi(x) \land \psi(x)\big) & \exists x\big(\varphi(x) \land \psi(x)\big) \nvdash \exists x\big(\varphi(x)\big) \land \psi(t) \\
\forall x\big(\varphi(x)\big) \lor \psi(t) \nvdash \forall x\big(\varphi(x) \lor \psi(x)\big) & \exists x\big(\varphi(x) \lor \psi(x)\big) \nvdash \exists x\big(\varphi(x)\big) \lor \psi(t)
\end{array}$$

Finally, the following four equivalences hold for conditional statements.

$$\begin{array}{ll}
\forall x\big(\varphi(x) \to p\big) \equiv \exists x\big(\varphi(x)\big) \to p & \forall x\big(p \to \varphi(x)\big) \equiv p \to \forall x\big(\varphi(x)\big) \\
\exists x\big(\varphi(x) \to p\big) \equiv \forall x\big(\varphi(x)\big) \to p & \exists x\big(p \to \varphi(x)\big) \equiv p \to \exists x\big(\varphi(x)\big)
\end{array}$$

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.

$$\begin{array}{ll}
\forall x\forall y\big(\varphi(x,y)\big) \equiv \forall y\forall x\big(\varphi(x,y)\big) & \exists x\exists y\big(\varphi(x,y)\big) \equiv \exists y\exists x\big(\varphi(x,y)\big) \\
\forall x\exists y\big(\varphi(x,y)\big) \nvdash \exists y\forall x\big(\varphi(x,y)\big) & \exists x\forall y\big(\varphi(x,y)\big) \vdash \forall y\exists x\big(\varphi(x,y)\big)
\end{array}$$

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.*

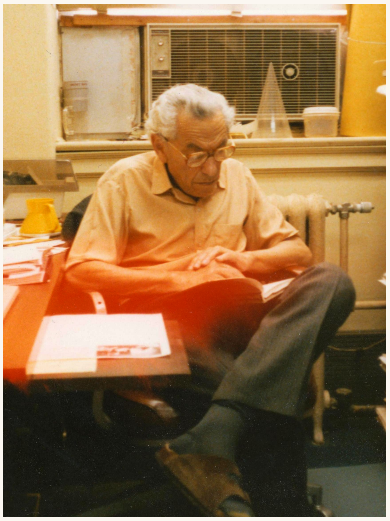


Figure 2.3: *"The purpose of life is to prove and to conjecture."* – Paul Erdős

Quantified Formulæ

If we are trying to prove a statement like $\forall x\big(\varphi(x)\big)$, 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 $\exists x\big(\varphi(x)\big)$, 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 $p \rightarrow q$. 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 $p \rightarrow q$ directly, we can always think to prove $\neg q \rightarrow \neg p$ 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 feeling like a proposition p is *obviously true*, but its proof feels insurmountable, 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 $p \equiv \bot \to q$ 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?

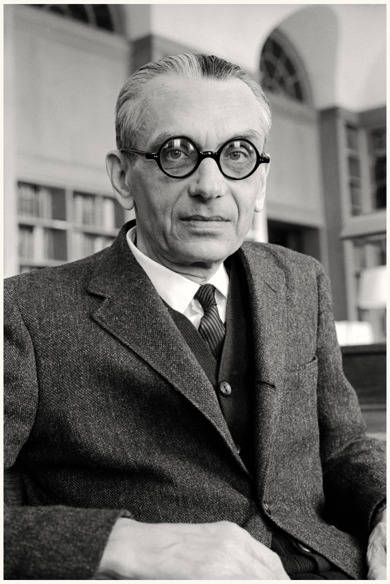


Figure 3.1: Kurt Gödel was an absolutely monumental figure in mathematical logic. He famously showed all universal truths in the first-order logic are provable (a property known as *completeness*). Despite this, he then infamously demonstrated there are *mathematical* truths that *cannot* be proven (the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

3.1 Informal Notions

Thanks to insights made throughout the 20th and 21st 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 could 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. Zero is a natural number.
2. If n is a natural number, then $\mathfrak{s}(n)$ is also a natural number.

$\mathfrak{s}(n)$

In the above recurrence, the notation $\mathfrak{s}(n)$—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).

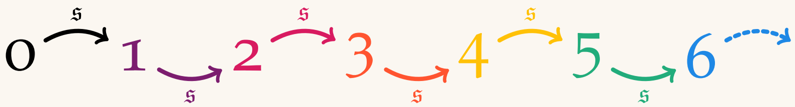


Figure 3.2: An initial segment of the natural number line, which begins at zero.

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

co/domain

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 the moment, we will say a *function* is an object that *maps inputs from a domain* to *outputs in a codomain* in a *deterministic 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]

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

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?"* All roads eventually lead to the idea of *a collection of things.* Functions map *collections of inputs to outputs.* Polygons are *collection of points.* Numbers measure the sizes of *collection of things.* In fact, any form of speech will find it hard to avoid invoking the concept of a *collection of things* eventually.

A notion of such *fundamental* importance to mathematics should therefore have a central place in our universe of discourse. In the same way binary numbers form a foundation for the files in your computer, we will be building our mathematical universe using *collections* as our fundamental unit of reference. We will call these collections *sets*, and refer to the objects they contain as their *elements*. For example, we might say that the number 0 is an element of the set of all natural numbers.

set

element

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.

As the most fundamental and basic object in our universe, we will study these first and *encode* their behavior in the form of *axioms*. Each axiom will incorporate some *intuitive property* that we would expect to be *true* about sets based on their inspiration as *"abstract collections of things."* This system of axioms—which we will study in the next section—is called *Zermelo-Fraenkel set theory*.

A Note on Notation

	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.

$\Rightarrow$

$\Leftrightarrow$

3.2 Set Theory

A *set* is an abstraction of the idea of a *collection of objects.* This idea, carried forward, naturally implies the need to communicate two kinds of relationships between objects: *equality* and *elementhood.* These will be the two basic predicate symbols of our *theory of sets.*

$=$

In order to identify objects that are the same, we introduce the binary *equality* predicate: given two objects x and y, we say $x = y$ precisely when x is *identical* to y. If you've seen the $=$ symbol before in your life, this is exactly the same symbol you're used to, and it has the natural properties you would expect of a predicate called *"equality."*

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

You'll notice that these are precisely the same three properties that *logical equivalence* had; these are both examples of equivalence relations. We will assume these three statements about equality axiomatically.

$\in$

The second, and more interesting, predicate relates sets to the elements they contain. We call this predicate *elementhood* and denote it with the $\in$ symbol. These two predicates are enough to express anything we could possibly want about sets. As an example, suppose that $\mathcal{A}$ is a set. By saying $(0 \in A) \wedge (1 \in A)$, we are saying that $\mathcal{A}$ contains both 0 and 1 as elements, and by saying $2 \notin \mathcal{A}$ we claim that 2 is *not* an element of $\mathcal{A}$. However, saying $(0 \in \mathcal{A}) \wedge (1 \in \mathcal{A})$ doesn't prevent $\mathcal{A}$ from possibly containing *more* elements. If we wanted to say that $\mathcal{A}$ contains *only* the elements 0 and 1, we would have to assert that $0 \in \mathcal{B}$ and that $1 \in \mathcal{B}$, but we would also need to say $\forall x(x \in \mathcal{B} \implies (x = 0 \vee x = 1))$. This asserts that not only are 0 and 1 among the elements of $\mathcal{A}$, but that any element of $\mathcal{A}$ *must* be one of those two. Now, notice that we can rewrite $0 \in \mathcal{A} \wedge 1 \in \mathcal{A}$ as $\forall x((x = 0 \vee x = 1) \implies x \in \mathcal{A})$. So, saying that $\mathcal{A}$ contains *exactly* the elements 0 and 1 tells us that being 0 or being 1 is an *equivalent condition* for being an element of $\mathcal{A}$. We can write this as $\forall x(x \in \mathcal{A} \iff (x = 0 \vee x = 1))$. This would be a lot to write every time, so let's introduce some *notation.*

Definition* 3.1 *(Set Notation).

$\{x_0, \ldots x_{n-1}\}$

Given finitely many terms $x_0, x_1, \ldots x_{n-1}$, we denote by $\{x_0, x_1, \ldots x_{n-1}\}$ the set whose elements are *exactly* the objects $x_0, x_1, \ldots x_{n-1}$. We write out each element of the set explicitly, separating the elements with commas, with the understanding that the following is *true* for any z.

"The set containing $x_0, x_1, \ldots x_{n-1}$."

$$z \in \big\{x_0, x_1, \ldots x_{n-1}\big\} \;:\Leftrightarrow\; (z = x_0) \vee (z = x_1) \vee \ldots (z = x_{n-1})$$

This is often called *set builder notation*. From *figure* 3.6, we can use this notation to say $\mathcal{A} = \{0,0,1,2\}$ and $\mathcal{B} = \{0,2,1\}$ whereas $\mathcal{C} = \{0,1,3,2\}$. Notice that set builder notation is extremely restrictive; it only lets us describe sets with *finitely many elements*, and it forces us to *write them all out*. What if we want to talk about a set with so many elements that it would be annoying—or impossible—to write them all down? How would we write down the set of *even* natural numbers, or the set of *prime* numbers, or even the set of natural numbers *itself*? To solve this problem, we introduce *set comprehension notation*.

$$z \in \{x \mid \varphi(x)\} \;:\Leftrightarrow\; \varphi(z)$$

$\{x \mid \varphi(x)\}$

“The set of all x such that $\varphi(x)$.”

With this notation, we can pick a predicate φ and refer to the collection of all those things that satisfy that predicate by writing $\{x \mid \varphi(x)\}$. In this way, we can refer to the set of even natural numbers by writing $\{x \mid x \in \mathbb{N} \land \text{“}x\textit{ is even}\text{”}\}$. We don't yet have a formal way of expressing *“x is even;”* once we do, $x \in \mathbb{N} \land$ *“x is even”* will be a predicate.

定義

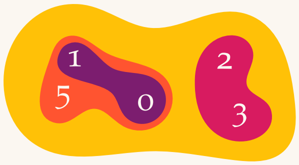


Figure 3.4: The *orange*, *red*, and *purple* sets are all subsets of the *yellow* set. We can see *purple* $\subseteq$ *orange*, but *orange* $\nsubseteq$ *purple*. Further, *orange* $\nsubseteq$ *red*, and *red* $\nsubseteq$ *orange*, implying *purple* $\nsubseteq$ *red*, and *red* $\nsubseteq$ *purple*.

The elementhood predicate is our fundamental relational symbol (apart from equality) between sets, but this predicate naturally implies another interesting relationship that two sets can share. For example, the blue set in *figure* 3.5 represents the set of all odd natural numbers, which we just learned can be written as $\{x \mid x \in \mathbb{N} \land \text{“}x\textit{ is odd}\text{”}\}$ using set comprehension notation. It should be pretty clear that every element of this set is a natural number. The same is true about $\{0,1,2\}$ and $\{0,1,2,3\}$. Every element of each one of these sets is *also* an element of $\mathbb{N}$. Taking this further, the elements of $\{0,1,2\}$ are each $\{0,1,2,3\}$. This emergent relationship is captured by the definition below.

Definition* 3.2 *(Subset).
Given two sets x and y, we say that *x is a subset of y*, denoted with the notation $x \subseteq y$, when every element of x is also an element of y.

$x \subseteq y$

$$x \subseteq y \;:\Leftrightarrow\; \forall z\big(z \in x \;\Rightarrow\; z \in y\big)$$

We can now see $\{x \mid x \in \mathbb{N} \land \text{“}x\textit{ is odd}\text{”}\} \subseteq \mathbb{N}$ and $\{0,1,2\} \subseteq \{0,1,2,3\}$. However, $\{0,1,2,3\} \nsubseteq \{0,1,2\}$ because $3 \in \{0,1,2,3\}$ but $3 \notin \{0,1,2\}$.

定義

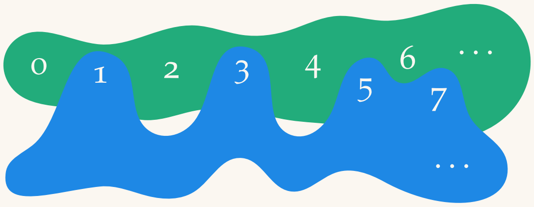


Figure 3.5: The set of *all natural numbers*, the smallest set $\mathbb{N}$ for which $0 \in \mathbb{N}$ and $\forall x(x \in \mathbb{N} \Rightarrow \mathfrak{s}(x) \in \mathbb{N})$, shown with the subset of *odd natural numbers*.

Infinity

We should keep one thing clear: these *definitions do not assert anything!* Just because we now have the ability to write something down with this new notation *doesn't* mean the notation *refers* to an existing object. To *formally* have sets to talk about, we need to introduce them with either an *axiom* or a *proof.* There is, of course, a set that has been looming over us this whole time—the set of *natural numbers*—that we certainly want to exist. Towards that goal, we introduce one more definition.

Definition 3.3 (Inductive Set).

inductive We say a set $\mathcal{I}$ is *inductive* if $0 \in \mathcal{I}$ and $\forall x\big(x \in \mathcal{I} \Rightarrow \mathfrak{s}(x) \in \mathcal{I}\big)$. 定義

Axiom 0 (Infinity).

$\exists x\Big(x \textit{ is inductive} \land \forall y\big(y \textit{ is inductive} \Rightarrow x \subseteq y\big)\Big)$. 公理

The set described by *axiom* 0 is—in a sense—the *"smallest" inductive set,* which is precisely the set of natural numbers.[1] Therefore, *axiom* 0 establishes the *existence of the set of natural numbers.* Once this understanding is clear, it is common to make the following recursive declaration.

$$\mathbb{N} := \left\{ x \;\middle|\; x = 0 \lor \exists y\big(y \in \mathbb{N} \land x = \mathfrak{s}(y)\big) \right\}$$

The rest of this chapter introduces *six more axioms* for set theory, each encoding a particular piece of *intuition* about *how sets should behave.*

Extensionality

Sets are entirely determined by their elements. Because sets abstract the idea of *a collection of objects*, everything we need to know about a set should determined by the elements it contains. We should expect that *looking inside* the and *comparing the elements* of two sets to answer the question *"are these two sets equal?"*

In *figure* 3.6, we have the sets $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, and $\mathcal{D}$. 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

[1] The fact that the smallest inductive set is actually the set of natural numbers is a *theorem,* but we will not take the time nor effort to prove it here.

$3 \notin \mathcal{A}$, 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.

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

This relationship between $=$ and $\in$ is exactly what the *axiom of extensionality* encodes. In our example above, we can now use this axiom to *prove* that $\mathcal{A} = \mathcal{B}$ by showing that $\forall z(z \in \mathcal{A} \Leftrightarrow z \in \mathcal{B})$. 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 all the same, we have a proof of $\forall z(z \in \mathcal{A} \Leftrightarrow z \in \mathcal{B})$. *Extensionality* tells us this means $\mathcal{A} = \mathcal{B}$.

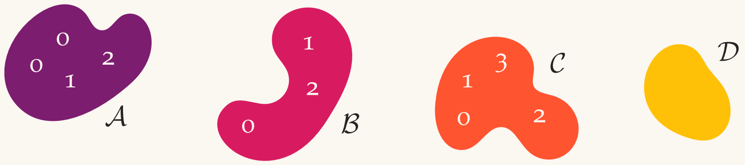


Figure 3.6: A visual representation of two sets. The *purple* set has the same elements as the *red* set, the figures refer to the same set, letting us infer $\mathcal{A} = \mathcal{B}$. The *orange* set contains an element not present in the other two sets, so $\mathcal{C} \neq \mathcal{A}$ and $\mathcal{C} \neq \mathcal{B}$. The *yellow* set has no elements, so it is empty.

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 decompose this statement below.

$$\begin{aligned}
\neg\forall z(z \in \mathcal{A} \Leftrightarrow z \in \mathcal{C}) &\equiv \exists z \neg(z \in \mathcal{A} \Leftrightarrow z \in \mathcal{C}) \\
&\equiv \exists z \neg\big((z \in \mathcal{A} \Rightarrow z \in \mathcal{C}) \land (z \in \mathcal{C} \Rightarrow z \in \mathcal{A})\big) \\
&\equiv \exists z \big(\neg(z \in \mathcal{A} \Rightarrow z \in \mathcal{C}) \lor \neg(z \in \mathcal{C} \Rightarrow z \in \mathcal{A})\big) \\
&\equiv \exists z \big(\neg(z \notin \mathcal{A} \lor z \in \mathcal{C}) \lor \neg(z \notin \mathcal{C} \lor z \in \mathcal{A})\big) \\
&\equiv \exists z \big((z \in \mathcal{A} \land z \notin \mathcal{C}) \lor (z \in \mathcal{C} \land z \notin \mathcal{A})\big)
\end{aligned}$$

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 $\mathcal{A} \neq \mathcal{C}$ according to the *axiom of extensionality*.

Lemma 3.1.
$\forall x \forall y \big(x = y \Leftrightarrow (x \subseteq y) \land (y \subseteq x) \big).$ 引理

Proof. Let x and y be sets. Observe the following chain of equivalences.

$$\begin{aligned}
x = y &\Leftrightarrow \forall z \big(z \in x \Leftrightarrow z \in y \big) && \text{by } \textit{extensionality} \\
&\Leftrightarrow \forall z \Big(\big(z \in x \Rightarrow z \in y \big) \land \big(z \in y \Rightarrow z \in x \big) \Big) \\
&\Leftrightarrow \forall z \big(z \in x \Rightarrow z \in y \big) \land \forall z \big(z \in y \Rightarrow z \in x \big) \\
&\Leftrightarrow \big(x \subseteq y \big) \land \big(y \subseteq x \big) && \text{by definition}
\end{aligned}$$

Therefore, $x = y \Leftrightarrow (x \subseteq y) \land (y \subseteq x)$. Q.E.D.

What about the set $\mathcal{D}$? In the figure, it would seem like $\mathcal{D}$ has no elements at all. *Extensionality* reveals to us that this means $\mathcal{D}$ cannot equal any of $\mathcal{A}$, $\mathcal{B}$, nor $\mathcal{C}$. In fact, $\mathcal{D}$ can't be equal to *any* set containing *any* elements because that set would contain something $\mathcal{D}$ doesn't.

Definition* 3.4 *(Empty Set).

empty

We say that a set x is *empty iff* $\forall y(y \notin x)$. We also define the following.

$$\varnothing := \{z \mid z \neq z\}$$

$\varnothing$

The referent of the $\varnothing$ symbol above is called *the empty set*. 定義

If we think of sets as *abstract containers,* it should be easy to conceptualize an empty container, which is exactly what $\varnothing$ would correspond to. With such a suggestive name, we should be able to say that $\varnothing$ is empty, right? Let's prove this as our first real theorem of set theory.

Theorem* 3.1 *(The Empty Set is Empty).
$\forall x(x \notin \varnothing)$. 定理

Proof. Let x be a set. Suppose, towards a contradiction, that $x \in \varnothing$. Then, we know $x \in \{z \mid z \neq z\}$ by definition of the empty set. This further tells us, by the definition of set comprehension notation, that $x \neq x$. However, we know $x = x$. $\lightning$ Therefore, $x \notin \varnothing$. Q.E.D.

Based on how $\mathcal{D}$ is drawn in *figure* 3.6, $\mathcal{D}$ empty since $\forall x(x \notin \mathcal{D})$. Does that mean that $\mathcal{D} = \varnothing$, or is it possible to have multiple distinct empty sets? As you might have guessed by what the *axiom of extensionality* says, *there is only one empty set* because all empty sets are equal to each other, justifying the name *the empty set* for $\varnothing$.

Theorem* 3.2 *(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 show x has all the same elements as $\varnothing$. Let z be a set. We will show $z \in x \Leftrightarrow z \in \varnothing$.

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*.

Recall *ex falso quodlibet;* anything follows from a contradiction.

Thus, $\forall z(z \in x \Leftrightarrow z \in \varnothing)$. So, $x = \varnothing$ by the *axiom of extensionality*. Q.E.D.

It's important to note that none of the prior analyses nor theorems *prove* that $\varnothing$ exists, only that there can be at most one empty set. We will need to wait until the *axiom of separation* to discuss this.

As you may have guessed, the empty set is the *smallest* set in a precise sense. Given any two sets $\mathcal{X}$ and $\mathcal{Y}$, we can define an *ordering* by saying that $\mathcal{X}$ is *"less than"* $\mathcal{Y}$ in when $\mathcal{X} \subseteq \mathcal{Y}$. With this notion of ordering induced by the $\subseteq$ relation, we can see that the $\varnothing$ is *ordered below* every other set, making it *minimal* in the $\subseteq$ ordering among all sets. Since there is only one empty set, $\varnothing$ is the *minimum* of this ordering.

***Theorem* 3.3.**
$\forall x(\varnothing \subseteq x)$. 定理

Proof. Let x be a set. Towards a contradiction, suppose $\varnothing \nsubseteq x$. Then, there exists some z such that $z \in \varnothing \wedge z \notin x$ by definition. This implies $z \in \varnothing$; however, we know $\forall w(w \notin \varnothing)$. ↯ Therefore, $\varnothing \subseteq x$. Q.E.D.

We might be lead to ask: is there a *maximum* set with respect to this $\subseteq$ ordering? We will answer this question in a short while. In the meantime, this is not the only nice property of the *set inclusion* ordering induced by the $\subseteq$ relation. In fact, this relation has all the defining properties of a *partial order*: *reflexivity*, *antisymmetry*, and *transitivity.*

Theorem* 3.4 *(Set Inclusion is a Partial Order).
The following three statements hold about the $\subseteq$ relation.

1. $\forall x(x \subseteq x)$ *reflexivity*
2. $\forall x \forall y\big(((x \subseteq y) \wedge (y \subseteq x)) \;\Rightarrow\; x = y\big)$. *antisymmetry*
3. $\forall x \forall y \forall z\big(((x \subseteq y) \wedge (y \subseteq z)) \;\Rightarrow\; x \subseteq z\big)$. *transitivity*

This makes $\subseteq$ an example of a *partial order* on the class of sets. We prove the *reflexive* property below, leaving the rest as exercises. 定理

Proof. Let x be a set. Let z be a set and recall that $(z \in x) \Rightarrow (z \in x)$. Therefore, since z was arbitrary, we have $x \subseteq x$ by definition. Q.E.D.

Pairing

If you remember from our earlier discussion of set notation, we have a way of expressing *"the set containing a, b, and c"* by writing down $\{a, b, c\}$. However, just having the ability to *say* something doesn't make what we're saying *meaningful.* If we want to be sure that $\{a, b, c\}$ actually refers to an object that *exists,* then we will either need *proof* that it exists, or we'll need to rely on an *axiom* to grant us its existence. This next axiom partially addresses the problem with our set notation by guaranteeing that *set builder notation* always refers to an existing set so long as all of its elements also exist.

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

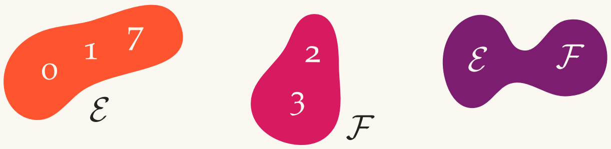


Figure 3.7: Given the sets $\{0, 1, 7\}$ and $\{2, 3\}$ exist, the *pairing axiom* asserts the existence of $\{\{0, 1, 7\}, \{2, 3\}\}$.

By definition, we call a set a *singleton* if it contains exactly *one* element and a *doubleton* if it contains exactly *two* elements. The *pairing axiom* makes the straight-forward assertion that $\{x, y\}$ exists so long as x and y also exist—this set $\{x, y\}$ may be a *singleton* if $x = y$ or a *doubleton* if $x \neq y$. In other words, this axiom lets us construct *unordered pairs.*

Separation

We can similarly express *"the set of all things that make $\varphi(\cdot)$ true"* for any predicate φ by writing $\{x \mid \varphi(x)\}$, but again we have the same problem regarding the existence of the referent. If you think this obsession might be needlessly neurotic, let's take a moment to see what happens if we pretend that $\{x \mid \varphi(x)\}$ exists for any predicate we feel like; after all, it should be natural to say that *"the set of all x with some property"* exists if a set is simply an abstract collection of objects.

Define the predicate $\rho(s) :=$ "$s \notin s$." Just as a sanity check, remind yourself about $\mathcal{A}$ from *figure* 3.6 and notice that $\mathcal{A} \notin \mathcal{A}$ because $\mathcal{A}$ is not 0, 1, nor 2. This means $\mathcal{A}$ satisfies ρ, making $\rho(\mathcal{A})$ is *true*—the point here being that ρ is sometimes *true* for some sets. Let's consider $\mathfrak{R} := \{x \mid (x)\} = \{x \mid x \notin x\}$ and analyse the truth value of $\rho(\mathfrak{R})$.

If $\rho(\mathfrak{R})$ is the case, then $\mathfrak{R} \notin \mathfrak{R}$ by the definition of ρ. That means that $\mathfrak{R} \in \{x \mid \rho(x)\}$, implying $\mathfrak{R} \in \mathfrak{R}$. ↯ What happens if $\neg\rho(\mathfrak{R})$ instead? Then, $\neg(\mathfrak{R} \notin \mathfrak{R})$, which simply says $\mathfrak{R} \in \mathfrak{R}$, implying $\mathfrak{R} \in \{x \mid \rho(x)\}$ by definition. However, this would mean $\rho(\mathfrak{R})$, so that $\mathfrak{R} \notin \mathfrak{R}$. ↯

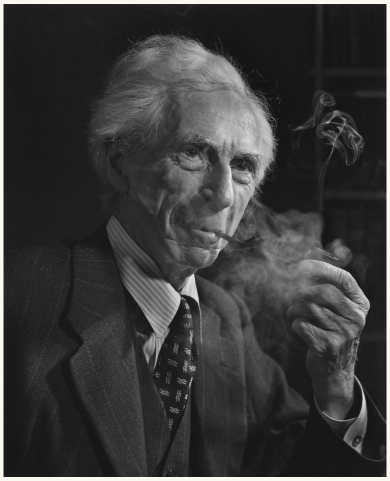


Figure 3.8: Russell's paradox is named after eminent mathematician and philosopher Bertrand Russell. He first mentioned this paradox in a letter to logician and philosopher Gottlob Frege as a critique of his *"Basic Law V,"* which was essentially an *unrestricted* form of comprehension for logical functions.

It seems like no matter what we do, we run into a problem. The mere *existence* of something like $\mathfrak{R}$ is *inherently contradictory*. We cannot allow things like $\mathfrak{R}$ to exist or they would introduce a contradiction into our system. This observation—that the *"set"* of all sets that don't contain themselves doesn't exist—is known as *Russell's paradox.*

Russell's paradox

This paradox stemmed from our reckless use of *unrestricted comprehension*. If we *restrict* comprehension only to *existing* sets, we avoid this issue. Instead of demanding $\{x \mid \varphi(x)\}$ always exists, we should *separate* off those elements satisfying φ from an *already existing set.*

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 only quantify over *objects*, not *predicates.*

Axiom 3 (Schema of Separation).
For any predicate φ with at most one free variable, the following is *true*.
$\forall x \exists y \big(y = \{z \mid z \in x \wedge \varphi(z)\}\big)$. 公理

Power

Since the *axiom of separation* gives us the ability to take arbitrary subsets of existing sets, you would hope to be able to talk about the collection of *all* those subsets as its own set.

Definition* 3.5 *(Power Set).

power set
$\mathbb{P}(x)$

Given a set x, we define the *power set of x* to be the set of *all possible subsets* of x. We denote this by writing $\mathbb{P}(x) := \{z \mid z \subseteq x\}$. 定義

Remarkably, despite the litany of axioms we have so far, we don't actually have any *guarantee* that the power set of an arbitrary set exists! We need to introduce a whole new axiom to assert this fact.

Axiom* 4 *(Power).
$\forall x \exists y (y = \{z \mid z \subseteq x\})$. 公理

As a small example, consider the sets $\mathcal{G} := \{0, 1\}$ and $\mathcal{H} := \{2, 3, 5\}$. Their respective power sets are given below.

$$\begin{aligned} \mathbb{P}(\mathcal{G}) &= \{\{\}, \{0\}, \{1\}, \{0, 1\}\} \\ &= \{\varnothing, \{0\}, \{1\}, \mathcal{G}\} \\ \mathbb{P}(\mathcal{H}) &= \{\{\}, \{2\}, \{3\}, \{5\}, \{2, 3\}, \{3, 5\}, \{2, 5\}, \{2, 3, 5\}\} \\ &= \{\varnothing, \{2\}, \{3\}, \{5\}, \{2, 3\}, \{3, 5\}, \{2, 5\}, \mathcal{H}\} \end{aligned}$$

You'll notice that $\mathbb{P}(\mathcal{G})$ has 4 elements while $\mathcal{G}$ has 2, and $\mathbb{P}(\mathcal{H})$ has 8 elements while $\mathcal{H}$ has 3; this is no coincidence: power sets grow *exponentially* in the size of their input—hence the name *power* set.[1] You might also notice that $\varnothing$ and the set itself are each elements of the power sets in our example above; this generalizes to *all* sets.

***Lemma* 3.2.**
$\forall x (\varnothing \in \mathbb{P}(x) \land x \in \mathbb{P}(x))$. 引理

Union

So far, the we can only make new sets by pairing up existing sets using *axiom* 2, by taking subsets using *axiom* 3, and collecting all those subsets together using *axiom* 4. We would also like to *merge* two sets together, combining all of their elements all in one set.

Definition* 3.6 *(Union of Two Sets).

union
$x \cup y$

Given two sets x and y, we define the *union* of those two sets as $x \cup y := \{z \mid z \in x \lor z \in y\}$. This is the set consisting of all of the elements of x in addition to all of the elements of y together. 定義

[1] We will prove this interesting fact later.

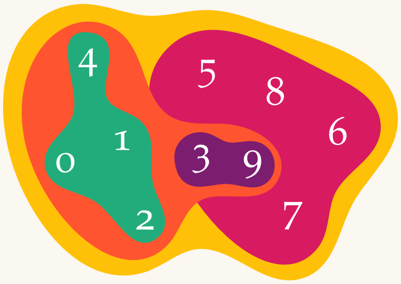


Figure 3.9: In this figure, the *orange set* is $\{0,1,2,3,4,9\}$ and the *red set* is $\{3,5,6,7,8,9\}$. The *yellow set* is the *union* of the two sets, consisting of $\{0,1,2,3,4,5,6,7,8,9\}$. The *purple set* is their *intersection*, consisting of $\{3,9\}$. The *green set* consisting of $\{0,1,2,4\}$ is the difference $\{0,1,2,3,4,9\} \setminus \{3,9\}$.

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.[1] Why should we limit ourselves like this? If we've reasonably gathered some amount of sets together, why shouldn't we be allowed to take the union of *all* of them together? Along the same lines, why not give ourselves the freedom to *iterate* the *"union operation"* over the elements of an arbitrary set?

Definition 3.7 (Union Over a Set).

union over
$\cup x$

Given a set x, we define the *union over x*, meaning the *iterated union* over the elements of x, as $\cup x := \{z \mid \exists y (y \in x \land z \in y)\}$. 定義

You'll notice that the definition above takes a set and gathers the *elements of all of its elements* into a set by themselves. As an example, consider the set $\mathcal{J} := \{\{0,1,2\},\{3,\{5,7\}\},\{\{8\},9\}\}$. The union over $\mathcal{J}$ is then given by $\cup\mathcal{J} = \{0,1,2,3,\{5,7\},\{8\},9\}$. We will dedicate our next axiom to these kinds of iterated unions, asserting that *"the iterated union over the elements of an existing set exists."*

Axiom 5 (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 3.5 (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*, $\tau := \{x,y\}$ exists. Then, we know that $\cup\tau$ exists by the union axiom, with the recognition that $\cup\tau = \{b \mid \exists a (a \in \tau \land b \in a)\}$ by definition. Recall that, by definition, $x \cup y = \{w \mid w \in x \lor w \in y\}$. We now witness the following for any z.

$$\begin{aligned} z \in \cup\tau &\Leftrightarrow z \in \big\{b \,\big|\, \exists a (a \in \tau \land b \in a)\big\} && \text{by definition of } \cup\tau \\ &\Leftrightarrow \exists a (a \in \tau \land z \in a) && \text{by definition} \\ &\Leftrightarrow \exists a (a \in \{x,y\} \land z \in a) && \text{by definition of } \tau \end{aligned}$$

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

$$\begin{aligned}
&\Leftrightarrow \exists a((a = x \vee a = y) \wedge z \in a) && \text{because } \tau = \{x, y\}\\
&\Leftrightarrow z \in x \vee z \in y && \text{by } \textit{extensionality}\\
&\Leftrightarrow z \in \{w \mid w \in x \vee w \in y\} && \text{by set comprehension notation}\\
&\Leftrightarrow z \in x \cup y && \text{by definition of } x \cup y
\end{aligned}$$

Thus, $\cup\tau = x \cup y$, so $x \cup y$ exists. 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 x and y are sets, then their *intersection* is the set of all elements they *share in common.* This is defined as $x \cap y := \{z \mid z \in x \wedge z \in y\}$. The *axiom of separation* easily guarantees us that $x \cap y$ always exists.

intersection

$x \cap y$

Theorem 3.6 (Existence of Intersections).
$\forall x \forall y \exists z(z = x \cap y)$. 定理

intersection over

$\cap x$

As with $\cup x$, we define what it means to iterate the *intersection over x*, collecting those things that are shared in common by *all* elements of x. We define this by $\cap x := \{z \mid \forall y(y \in x \Rightarrow z \in y)\}$. Although we *axiom 5* tells us that iterated unions always exist, do not mistakenly presuppose that $\cap x$ should behave the same way! As an exercise, think about $\cap\varnothing$.

set minus

$x \setminus y$

The *difference* of x and y is the set obtained by *removing* every element of y from x. This is bizarrely denoted $x \setminus y := \{z \mid z \in x \wedge z \notin y\}$, notation which we are not responsible for. As with unions and intersections of two sets, the difference of two arbitrary sets always exists.

Theorem 3.7 (Existence of Differences).
$\forall x \forall y \exists z(z = x \setminus y)$. 定理

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 inline with mainstream mathematics and all of the physical intuition surrounding sets, there is actually nothing so far that would *formally* prohibit $x \in x$ to be *true* about some set x. As simple people—interested in doing *reasonable* and *mostly computable* mathematics—we should adopt the mainstream view that sets like $x = \{x\}$ and $\{x, y\} = \{\{y\}, \{x\}\}$ shouldn't exist.

Figure 3.10: The axiom of regularity was introduced by John von Neumann to facilitate the study of the ordinal numbers. An important practical consequence of this axiom is that sets are not allowed to be elements of themselves.

Axiom* 6 *(Regularity).
$\forall x\big(x \neq \varnothing \;\Rightarrow\; \exists y(y \in x \wedge x \cap y = \varnothing)\big).$ 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* 3.8 *(Well-Foundedness of Elementhood).
$\forall x(x \notin x).$ 定理

Proof. Let x be a set and suppose that $x \in x$ towards a contradiction. Consider $y := \{z \mid z \in x \wedge z = x\}$, which the *axiom of separation* assures us exists. Note $y = \{x\}$ by *extensionality* since $\forall z(z \in y \Leftrightarrow z = x)$. Then, $y \neq \varnothing$, so the *axiom of regularity* says $\exists z(z \in y \wedge y \cap z = \varnothing)$.

$$\begin{aligned} \exists z\big(z \in y \wedge y \cap z = \varnothing\big) &\Leftrightarrow \exists z\big(z \in \{x\} \wedge \{x\} \cap z = \varnothing\big) \\ &\Leftrightarrow \{x\} \cap x = \varnothing \end{aligned}$$

This implies $y \cap x = \varnothing$. However, since $x \in y$ and $x \in x$, we know $x \in y \cap x$, so that $y \cap x \neq \varnothing$. ↯ Therefore, $x \notin x$. Q.E.D.

The *axiom of regularity* also prohibits the existence of *"universal sets,"* objects U with the property $\forall x(x \in U)$. For instance, *"the set of all sets,"* sometimes called *"the universe,"* is typically denoted by $\mathfrak{U} := \{z \mid z = z\}$. This *"set"* is not really a set according to our rules because, if it were, then we would immediately know $\mathfrak{U} \in \mathfrak{U}$ because $\mathfrak{U} = \mathfrak{U}$, contradicting the fact that the $\in$ predicate is well-founded that we just proved.

Theorem* 3.9 *(The Universe Does Not Exist).
$\neg\exists x \forall y(y \in x).$ 定理

Proof. Towards a contradiction, suppose there exists a universal set x characterized by $\forall y(y \in x)$. We then obtain $x \in x$, contradicting the fact that $\forall z(z \notin z)$. ↯ Therefore, there is no x such that $\forall y(y \in x)$. Q.E.D.

Another Note on Notation

We will introduce one last bit of incredibly convenient notation here. Given any set $\mathcal{X}$ and predicate φ, we have a more compact way of expressing "*$\varphi(x)$ for all x in $\mathcal{X}$*" and "*there exists x in $\mathcal{X}$ such that $\varphi(x)$.*"

$$\begin{aligned} (\forall x \in \mathcal{X})\big(\varphi(x)\big) &:\Leftrightarrow \forall x\big(x \in \mathcal{X} \;\Rightarrow\; \varphi(x)\big) \\ (\exists x \in \mathcal{X})\big(\varphi(x)\big) &:\Leftrightarrow \exists x\big(x \in \mathcal{X} \wedge \varphi(x)\big) \end{aligned}$$

"For all x in $\mathcal{X}$, $\varphi(x)$."

"There is some x in $\mathcal{X}$ such that $\varphi(x)$."

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

A statement like "$(\forall x \in \mathcal{X})$" is nonsense on its own because nothing is actually being said about the x elements of $\mathcal{X}$; there is no *clause* in this expression, so it's not a sentence. Similarly, "$(\varphi(x))$" would be nonsense *unless we know who x is;* sentences can't contain *free variables.*

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

We finish by introducing, above, a compact analogue of the *restricted* set comprehension notation that *axiom* 5 facilitates. This new notation $\{x \in \mathcal{X} \mid \varphi(x)\}$ is read as follows: *"the set of all x in $\mathcal{X}$ such that $\varphi(x)$."*

3.3 *Functions*

Central to the history, tradition, and practice of mathematics is the concept of a *function*—is a special kind of *relation* between two sets in which *every* element of the first set *has* a *unique* corresponding element in the second set. We spoke about these intuitively in section 3.1, but it has come time to think about how to define these within set theory.

Suppose we have two sets $\mathcal{A}$ and $\mathcal{B}$. A function from $\mathcal{A}$ to $\mathcal{B}$ establishes an associating between the elements $a \in \mathcal{A}$ and the elements $b \in \mathcal{B}$ in a way that corresponds intuitively with our notions of *input* and *output* respectively. If we wanted to pair up these inputs with their corresponding outputs, we might first think to construct the unordered pair $\{a, b\}$; however, it should be clear that is fails to represent which element of $\{a, b\}$ was the *input* and which one was the *output*, since $\{a, b\}$ and $\{b, a\}$ are indistinguishable in set theory. We need a way of establishing sets in which the *order* of the elements also matters.

To distinguish them from unordered pairs, we will denote an *ordered pair* using $(\cdot, \cdot)$ parentheses instead of $\{\cdot, \cdot\}$ brackets. Two ordered pairs (x_1, y_1) and (x_2, y_2) should be equal *iff* all of their *corresponding coordinates* are equal in all the same positions.

$$(x_1, y_1) = (x_2, y_2) \quad \Leftrightarrow \quad (x_1 = x_2 \wedge y_1 = y_2)$$

This is the *characterization* of ordered pairs; any definition or implementation using sets that we come up with *must* enforce this relationship, or it wouldn't really capture what we *mean* by *"ordered pair."* The following definition given by Kazimierz Kuratowski accomplishes precisely this.

Definition* 3.8 *(Ordered Pair).
ordered pair (x, y)
Given sets x and y, we define the *ordered pair* whose first coordinate is x and second coordinate is y as $(x, y) := \{\{x\}, \{x, y\}\}$. 定義

***Lemma* 3.3.**
$\forall a \forall b \forall x \forall y \Big(((a, b) = (x, y)) \;\Leftrightarrow\; (a = x \wedge b = y) \Big).$ 引理

This gives us a way of associating the elements of two sets by constructing sets of ordered pairs whose coordinates are elements of each respective set. Thus, a *relation* between $\mathcal{A}$ and $\mathcal{B}$ is nothing more than a particular set of ordered pairs (a, b) where $a \in \mathcal{A}$ and $b \in \mathcal{B}$. More precisely, we say $\mathcal{R}$ is a *relation between $\mathcal{A}$ and $\mathcal{B}$* when $\mathcal{R} \subseteq \{(a, b) \mid a \in \mathcal{A} \wedge b \in \mathcal{B}\}$ for any two sets $\mathcal{A}$ and $\mathcal{B}$. The *largest* relation between two sets is the set of *all* such possible ordered pairs. This important construction—named in honor of René Descartes—is defined below with its own dedicated notation.

relation

Definition 3.9 (Cartesian Product).
The *Cartesian product* of two sets x and y is the set of *all possible ordered pairs between them.* Formally, $x \times y := \{(a, b) \mid a \in x \wedge b \in y\}$. 定義

set product

$x \times y$

Importantly, the Cartesian product of any two sets always exists. This conveniently means that whenever we are interested in relating the elements of two sets—or of constructing a function between two sets—we won't have to worry about existence questions thanks to the *axiom of separation* because it will simply be a subset of the Cartesian product.

Theorem 3.10 (Existence of Cartesian Products).
$\forall x \forall y \exists z (z = x \times y)$. 定理

A function, as we previously motivated, is a special kind of relation: one in which *every element of the domain* has a *unique image in the codomain*. This means that a function f from $\mathcal{A}$ to $\mathcal{B}$ should, first and foremost, be a *relation* $f \subseteq \mathcal{A} \times \mathcal{B}$. Then, we should impose the special condition on the ordered pairs $(a, b) \in f$ that, *for every $a \in \mathcal{A}$*, there always *exists exactly one $b \in \mathcal{B}$* such that a is paired up with b in f.

Definition 3.10 (Function).
Given sets $\mathcal{X}$ and $\mathcal{Y}$, we introduce the notation $f : \mathcal{X} \to \mathcal{Y}$ to indicate that *f is a function from $\mathcal{X}$ to $\mathcal{Y}$*. We define what this means below.

$f : \mathcal{X} \to \mathcal{Y}$

$$f \subseteq \mathcal{X} \times \mathcal{Y} \quad \wedge \quad (\forall x \in \mathcal{X})(\exists! y \in \mathcal{Y})\Big((x, y) \in f\Big)$$

The sets $\mathcal{X}$ and $\mathcal{Y}$ are called the *domain* and *codomain* of f respectively. When we know that f is a function, we can replace the ordered pair notation above with the traditional *functional* notation below.

$f(x) = y$

$$f(x) = y \;:\Leftrightarrow\; (x, y) \in f$$

This convenient notation lets us rewrite the right-hand side of our definition as $(\forall x \in \mathcal{X})(\exists! y \in \mathcal{Y})(f(x) = y)$. 定義

3.4 *Lifting the Veil*

Equipped with the axioms of set theory, we are now ready to discover *who* the natural numbers *really are* with, of course, a recursive definition.

$$\begin{aligned} 0 &:= \varnothing \\ \mathfrak{s}(n) &:= n \cup \{n\} \end{aligned}$$

We begin by establishing that *the first natural number* is *the empty set*. We then obtain the *successors* of zero by iteratively *adding one new element* to the previous natural number. If we apply this definition, we can compute that the natural number 1 is actually the set containing 0.

Figure 3.11: The natural 0 as a set.

$$1 := \mathfrak{s}(0) = 0 \cup \{0\} = \varnothing \cup \{\varnothing\} = \{\varnothing\} = \{0\}$$

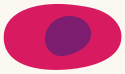


Figure 3.12: The natural 1 as a set.

A similar computation reveals that 2 is the set containing both 0 and 1.

$$2 := \mathfrak{s}(1) = 1 \cup \{1\} = \{\varnothing\} \cup \{\{\varnothing\}\} = \{\varnothing, \{\varnothing\}\} = \{0, 1\}$$

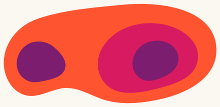


Figure 3.13: The natural 2 as a set.

If we continue this process, you'll start to notice a pattern emerging.

$$\begin{aligned} 0 &= \varnothing && = \{\} \\ 1 &= \{\varnothing\} && = \{0\} \\ 2 &= \{\varnothing, \{\varnothing\}\} && = \{0, 1\} \\ 3 &= \big\{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\big\} && = \{0, 1, 2\} \\ 4 &= \Big\{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}, \big\{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\big\}\Big\} && = \{0, 1, 2, 3\} \\ &\vdots && \vdots \end{aligned}$$

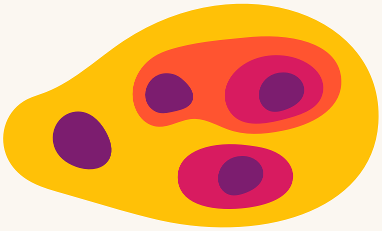


Figure 3.14: The natural 3 as a set.

This characterization results from $0 = \varnothing$ and the following theorems.

Theorem 3.11 (Successor Function has no Fixed Points).
$\forall x \big(x \neq x \cup \{x\}\big)$. 定理

Theorem 3.12 (Every Natural Number is Transitive).
$(\forall x \in \mathbb{N})(\forall y \in x)(\forall z \in y)(z \in x)$. 定理

These two facts show us *every natural number is the set of all the natural numbers that came before it*. This lets us define $(m < n) \; :\Leftrightarrow \; (m \in n)$ for any natural numbers $m, n \in \mathbb{N}$,[1] inspiring the following notation.[2]

$m < n$

$$[\![n]\!] := \{x \in \mathbb{N} \mid x \in n\} = \{x \in \mathbb{N} \mid x < n\}$$

We can clearly see that $n = [\![n]\!]$ for any $n \in \mathbb{N}$. While this might seem like useless notation at first, it will be useful in the future when we need to make a natural number *as a set* and *as a number*. It should be less confusing if we use notation like $m + n$ when treating them like numbers and $[\![m]\!] \cup [\![n]\!]$ when treating them like sets.

[1] We say $m \leqslant n$ if $(m < n) \vee (m = n)$.

[2] Note that this notational definition *only applies to natural numbers.*

4

Arithmetic

> *"Don't for heaven's sake, be afraid of talking nonsense! But you must pay attention to your nonsense."*
>
> – Ludwig Wittgenstein

4.1 *The Categorical Structure of Arithmetic*

Now that we know *who* the natural numbers are, we'd like to be able to *use* them for something, so we need to understand their basic structure and behavior. First, let's remind ourselves of an obvious fact.

$$0 \in \mathbb{N}.$$

Secondly, the successor of any natural number is also a natural number.

$$(\forall n \in \mathbb{N})(\mathfrak{s}(n) \in \mathbb{N}).$$

However, zero being the *first* natural number means *it has no predecessors.*

$$(\forall n \in \mathbb{N})(0 \neq \mathfrak{s}(n)).$$

Further, numbers are *equal* precisely when they have *the same successor.*

$$(\forall n, m \in \mathbb{N})\Big((\mathfrak{s}(n) = \mathfrak{s}(m)) \;\Rightarrow\; (n = m)\Big).$$

Finally, and most importantly, *every natural number can eventually be reached by starting at zero and iteratively finding successors.* This gives us a remarkably powerful way to prove statements about the naturals.

As a note: it is not difficult to show that the reverse direction of this statement is also *true*, but it is much less interesting than the forward direction given here.

$$\Big(\varphi(0) \wedge (\forall k \in \mathbb{N})\Big(\varphi(k) \;\Rightarrow\; \varphi\big(\mathfrak{s}(k)\big)\Big)\Big) \;\Rightarrow\; (\forall n \in \mathbb{N})(\varphi(n))$$

Given a predicate φ, the above statement proclaims that $\varphi(x)$ is *true* about every natural number x if we first know $\varphi(0)$ is *true* and then, whenever $\varphi(k)$ is *true* for an arbitrary $k \in \mathbb{N}$, the statement $\varphi(\mathfrak{s}(k))$ about the next natural number is *induced* into being *true* as well. This is known as *mathematical induction*, a concept spiritually dual to *recursion.*

induction

Each of the aforementioned statements about $\mathbb{N}$ is a theorem of set theory, and we have taken great care in setting up our axioms and definitions so that this would be the case. Although some parts of this journey may have felt delicate, arbitrary, or contrived, the remarkable fact of the matter is that these five properties *canonically* represent the *essence* of the natural numbers. Any structure that also satisfies these five properties will *encodes* within it a copy of the natural numbers. *Any structure arranged like the natural numbers behaves like the natural numbers.*

At the end of the day, the specific choices we made to *implement* the natural numbers set-theoretically were fundamentally unimportant. What matters is that we *have* a representation of $\mathbb{N}$ so that we can reason about them formally. The following section will define many of the operations on $\mathbb{N}$ you may be familiar with, but you should keep in mind that any definitions we make—any theorems we prove—about $\mathbb{N}$ will also be true about *anything that looks like* $\mathbb{N}$.

Definition 4.1 (Addition & Multiplication).
The two basic algebraic operations on $\mathbb{N}$ are *addition* and *multiplication*.

$$\begin{aligned} n + 0 &:= n & \qquad n \cdot 0 &:= 0 \\ n + \mathfrak{s}(m) &:= \mathfrak{s}(n+m) & \qquad n \cdot \mathfrak{s}(m) &:= (n \cdot m) + n \end{aligned}$$

We define these binary operations above through recursion on the *second argument* while keeping the *first argument* fixed. 定義

Definition 4.2 (Exponentiation & Tetration).
We also define how to *exponentiate* and *tetrate* natural numbers below.

$$\begin{aligned} n^0 &:= 1 & \qquad n \uparrow\uparrow 0 &:= 1 \\ n^{\mathfrak{s}(m)} &:= n \cdot n^m & \qquad n \uparrow\uparrow \mathfrak{s}(m) &:= n^{n \uparrow\uparrow m} \end{aligned}$$

Again, these are recursive definitions in the *second argument* that take an arbitrary natural number as their *first argument*. 定義

Definition 4.3 (Sums & Products).
Given a function $f : \mathbb{N} \to \mathbb{N}$, we define the *sum* and *product* of the first n values of this function recursively below.

$$\begin{aligned} \sum_{i=0}^{0} f(i) &:= f(0) & \qquad \prod_{i=0}^{0} f(i) &:= f(0) \\ \sum_{i=0}^{\mathfrak{s}(n)} f(i) &:= \left(\sum_{i=0}^{n} f(i) \right) + f(\mathfrak{s}(n)) & \qquad \prod_{i=0}^{\mathfrak{s}(n)} f(i) &:= \left(\prod_{i=0}^{n} f(i) \right) \cdot f(\mathfrak{s}(n)) \end{aligned}$$

We can generalize these definitions to cases where the lower index is nonzero as long as the upper index dominates the lower index. 定義

***Theorem* 4.1.**
$(\forall n \in \mathbb{N})(\mathfrak{s}(n) = n + 1)$. 定理

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

$$\begin{aligned} n + 1 &= n + \mathfrak{s}(0) && \text{since } 1 := \mathfrak{s}(0) \\ &= \mathfrak{s}(n + 0) && \text{by definition of addition} \\ &= \mathfrak{s}(n) && \text{by definition of addition} \end{aligned}$$

Therefore, we have $\mathfrak{s}(n) = n + 1$. Q.E.D.

***Theorem* 4.2.**
$(\forall n \in \mathbb{N})(n + 0 = n)$. 定理

Proof. Let $n \in \mathbb{N}$ and notice that $n + 0 = n$ by the definition of addition. Q.E.D.

***Theorem* 4.3.**
$(\forall n \in \mathbb{N})(0 + n = n)$. 定理

Proof. We will prove this by induction.

Basis Step:
Observe that $0 + 0 = 0$ by the definition of addition.

Inductive Step:
Let $k \in \mathbb{N}$ and assume $0 + k = k$. We will now show that $0 + \mathfrak{s}(k) = \mathfrak{s}(k)$. Bear witness to the following deduction.

$$\begin{aligned} 0 + \mathfrak{s}(k) &= \mathfrak{s}(0 + k) && \text{by definition of addition} \\ &= \mathfrak{s}(k) && \text{by the \textit{inductive hypothesis}} \end{aligned}$$

Therefore, we conclude $(\forall n \in \mathbb{N})(0 + n = n)$. Q.E.D.

Theorem* 4.4 *(Associativity of Addition).
$(\forall x, y, z \in \mathbb{N})(x + (y + z) = (x + y) + z)$. 定理

Proof. Let $x, y \in \mathbb{N}$. We will prove this by induction.

Basis Step:
Notice $x + (y + 0) = x + y = (x + y) + 0$ by definition of addition.

Inductive Step:
Let $k \in \mathbb{N}$ and assume $x + (y + k) = (x + y) + k$. Observe.

$$\begin{aligned} x + (y + \mathfrak{s}(k)) &= x + \mathfrak{s}(y + k) && \text{by definition of addition} \\ &= \mathfrak{s}(x + (y + k)) && \text{by definition of addition} \\ &= \mathfrak{s}((x + y) + k) && \text{by the \textit{inductive hypothesis}} \\ &= (x + y) + \mathfrak{s}(k) && \text{by definition of addition} \end{aligned}$$

Thus, $x + (y + \mathfrak{s}(k)) = (x + y) + \mathfrak{s}(k)$ as desired.

Therefore, we conclude $(\forall x, y, z \in \mathbb{N})(x + (y + z) = (x + y) + z)$. Q.E.D.

4.2 Abstraction and Extension

$x \leqslant y$

$x < y$

Given $n, m \in \mathbb{N}$, we say $n \leqslant m \iff (\exists x \in \mathbb{N})(n + x = m)$, meaning n is *less than or equal to* m. We also define a *strict* version of this order by saying $n < m \iff (n \leqslant m) \wedge (n \neq m)$. Knowing this, we realize the natural numbers have all the defining properties of an *ordered semiring*.

Theorem 4.5 (The Naturals are an Ordered Semiring).
$\mathbb{N}$ is a *commutative monoid* under *addition* with *identity element 0*.

1. $(\exists e \in \mathbb{N})(\forall x \in \mathbb{N})(e + x = x + e = x)$. *existence of additive identity*
2. $(\forall x, y, z \in \mathbb{N})(x + (y + z) = (x + y) + z)$. *associativity of addition*
3. $(\forall x, y \in \mathbb{N})(x + y = y + x)$. *commutativity of addition*

$\mathbb{N}$ is a *commutative monoid* under *multiplication* with *identity element 1*.

4. $(\exists e \in \mathbb{N})(\forall x \in \mathbb{N})(e \cdot x = x \cdot e = x)$. *existence of multiplicative identity*
5. $(\forall x, y, z \in \mathbb{N})(x \cdot (y \cdot z) = (x \cdot y) \cdot z)$. *associativity of multiplication*
6. $(\forall x, y \in \mathbb{N})(x \cdot y = y \cdot x)$. *commutativity of multiplication*

Multiplication *distributes* over addition, and the additive identity is also the *multiplicative annihilator*. This makes $\mathbb{N}$ a *commutative semiring*.

7. $(\forall x, y, z \in \mathbb{N})(x \cdot (y + z) = (x \cdot y) + (x \cdot z))$. *distributivity*
8. $(\forall x \in \mathbb{N})(0 \cdot x = 0)$. *annihilation*

Addition and multiplication are *monotonic*, making $\mathbb{N}$ an *ordered semiring*.

9. $(\forall x, y, z \in \mathbb{N})((x \leqslant y) \Rightarrow (x + z \leqslant y + z))$. *addition is monotonic*
10. $(\forall x, y, z \in \mathbb{N})((x \leqslant y \wedge 0 \leqslant z) \Rightarrow (x \cdot z \leqslant y \cdot z))$. *multiplication is monotonic*

We usually say that $\mathbb{N}$ is the *canonical* ordered semiring because any other algebraic structure that has all of these same properties *must contain a copy of $\mathbb{N}$ within it as a substructure.* 定理

The Integer Ring

$\mathbb{Z}$

group

The *integers* $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ extend $\mathbb{N}$ by introducing *additive inverses*[1] 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*. Since addition is also *commutative* on $\mathbb{Z}$, also say $\mathbb{Z}$ is a *commutative group*.

Theorem 4.6 (The Integers are a Group).
$(\forall z \in \mathbb{Z})(\exists w \in \mathbb{Z})(z + w = 0)$. 定理

[1] 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.

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 with respect to a linear order $\leqslant$, then we call it an *ordered ring*. The integers $\mathbb{Z}$ with standard $+$ and $\cdot$ operations, ordered by $\leqslant$ as usual, are the *canonical* example of an ordered ring. There is an intimate relationship between $\mathbb{N}$ and $\mathbb{Z}$ that is revealed by the *absolute value function*, denoted $|\cdot| : \mathbb{Z} \to \mathbb{N}$ and defined below.

$$|z| := \begin{cases} z & \textit{if} \quad z \geqslant 0 \\ -z & \textit{if} \quad z < 0 \end{cases}$$

$|z|$ The *absolute value* of an integer $z \in \mathbb{Z}$ is then denoted $|z|$.

The Rational Field

$\mathbb{Q}$ The set of *rational* numbers $\mathbb{Q} = \{ {}^{p}/_{q} \mid p \in \mathbb{Z} \wedge q \in \mathbb{N}_+ \}$ extends $\mathbb{Z}$ by introducing *multiplicative inverses* for every *nonzero* element. Every ring with this additional property is called a *field*. With the inherited properties from the integers, $\mathbb{Q}$ is the canonical *ordered field*.

Figure 4.1: Augustin-Louis Cauchy

Theorem* 4.7 *(The Rationals are a Field).
$(\forall q \in \mathbb{Q})\big(q \neq 0 \Rightarrow (\exists r \in \mathbb{Q})(q \cdot r = 1)\big)$. 定理

The Continuum

$\mathbb{R}$ The set of *real* numbers $\mathbb{R}$ *completes* $\mathbb{Q}$ by ensuring that every Cauchy sequence of rational numbers has a limit that it converges to.

Zero-Product Property

All of these algebraic structures happen to be *cancellative* with respect to both of their operations. This implies there are *no nonzero zero divisors*.

***Theorem* 4.8.**
Let $\mathfrak{A}$ be any of $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ with its standard addition and multiplication operations. Then, the following three statements are *true*.

1. $(\forall x, y, z \in \mathfrak{A})\Big((x + z = y + z) \Rightarrow (x = y)\Big)$. *additive cancellation*
2. $(\forall x, y, z \in \mathfrak{A})\Big((x \cdot z = y \cdot z \;\wedge\; z \neq 0) \Rightarrow (x = y)\Big)$. *multiplicative cancellation*
3. $(\forall x, y \in \mathfrak{A})\Big((x \cdot y = 0) \Leftrightarrow (x = 0 \vee y = 0)\Big)$. *domain property*

定理

5

Ancient Number Theory

“Αὐτός μέν Πῡθᾰγόρας, ἐν τῷ ἱέρῳ λογῳ διαρρήδην μορφών καί ἰδέων κράντορα τόν ἀριθμόν ἐλεγεν ἐιναι, καί θέων καί δαιμόνων αἶτιον· καί τῷ πρέσβυτατῳ καί κρατιστεύοντι τέχνιτῃ θέῳ κανονα, καί λογον τεχνικόν, νουν τε καί σταθμάν ἀκλῐνέσταταν τόν ἀριθμόν ὑπεικε συστάσιος καί γενέσεως τῶν πάντων.”

– Ἰάμβλιχος

“Number is the ruler of forms and ideas and the cause of Gods and dæmons.”

– Pythagoras

Figure 5.1: Pythagoras (Πυθαγόρης).

5.1 *The Greeks*

Definition 5.1 (Divisibility).

divides

For any $a, b \in \mathbb{Z}$, we say that *a divides b* when b is a multiple of a.

$a \mid b$

$$a \mid b \;:\Leftrightarrow\; (\exists k \in \mathbb{Z})(a \cdot k = b)$$

Note that this is a *sentence* establishing a relation on $\mathbb{Z}$. 定義

Theorem 5.1 (Absolute Monotonicity of Divisibility).

Let $a, b \in \mathbb{Z}$ such that $b \neq 0$. Then, $a \mid b$ implies $|a| \leqslant |b|$. 定理

Lemma 5.1.

Let $z \in \mathbb{Z}$. Then, $1 \mid z$ and $z \mid 0$. Further, we have $(0 \mid z) \Leftrightarrow (z = 0)$. Finally, $(z \mid 1) \Leftrightarrow (z \in \{-1, 1\})$. 引理

Definition 5.2 (Parity).

even

odd

Let $z \in \mathbb{Z}$. We say that z is *even* by definition if $2 \mid z$. Analogously, we z is *odd* if $2 \mid z - 1$. This characteristic of z is called its *parity*. 定義

Theorem 5.2 (Even-Odd Dichotomy).

For every $z \in \mathbb{Z}$, we know z is either even or odd but not both. 定理

***Theorem* 5.3.**
Let $n, a, b, x, y \in \mathbb{Z}$ such that $n \mid x$ and $n \mid y$. Then, $n \mid ax + by$. 定理

Theorem* 5.4 *(Divisibility is a Partial Order).
The divisibility relation on $\mathbb{N}$ has the three following properties.

1. $(\forall a \in \mathbb{N})(a \mid a)$. *reflexivity*
2. $(\forall a, b \in \mathbb{N})((a \mid b \wedge b \mid a) \Rightarrow a = b)$. *antisymmetry*
3. $(\forall a, b, c \in \mathbb{N})((a \mid b \wedge b \mid c) \Rightarrow a \mid c)$. *transitivity*

This makes divisibility on $\mathbb{N}$ an example of a *partial order.* 定理

Definition* 5.3 *(Primality).
prime We say that a natural number $p \in \mathbb{N}$ is *prime* when $p > 1$ and p is *minimally divisible*, meaning $(\forall n \in \mathbb{N})(n \mid p \Rightarrow n \in \{1, p\})$. Any *composite* natural number that is *not prime* is called *composite* by definition. 定義

Lemma* 5.2 *(Fundamental Lemma of Arithmetic).
Let $n \in \mathbb{N}$ such that $n \geqslant 2$. Then, $(\exists p \in \mathbb{N})(p \text{ is prime} \wedge p \mid n)$. 引理

Theorem* 5.5 *(Fundamental Theorem of Arithmetic).
Let $n \in \mathbb{N} \setminus 2$. Then, $\exists! k \in \mathbb{N}$ and $\exists!(p_0, \alpha_0), \ldots (p_k, \alpha_k) \in \mathbb{N} \times \mathbb{N}$ such that $p_0, \ldots p_k$ are *distinct prime numbers* and the following holds.

$$n = \prod_{i=0}^{k} p_i^{\alpha_i} = p_0^{\alpha_0} p_1^{\alpha_1} \ldots p_k^{\alpha_k}$$

定理

Theorem* 5.6 *(Euclid's Theorem).
There are infinitely many prime numbers. 定理

Proof. We know there is at least one prime number since 2 is prime. Towards a contradiction, suppose $p_0, \ldots p_k \in \mathbb{N}$ is a complete list of *all* the prime numbers, where $k \in \mathbb{N}$. Consider the product $\mathcal{P} := \prod_{i=0}^{k} p_i$ of all of these prime numbers. Since $p_i \geqslant 2$ for each $i \in k + 1$, we know $\mathcal{P} \geqslant 2$, meaning $\mathcal{P}$ has a prime divisor by *lemma* 5.2. Let p_j be that prime divisor, so that $p_j \mid \mathcal{P} + 1$, and observe the following.

$$p_j \left(\prod_{i=0, i \neq j}^{k} p_i \right) = \prod_{i=0}^{k} p_i = \mathcal{P}$$

This observation implies $p_j \mid \mathcal{P}$. Since p_j divides both $\mathcal{P}$ and $\mathcal{P} + 1$, *theorem* 5.3 leads us to the following astonishing revelation.

$$p_j \mid (\mathcal{P} + 1) - \mathcal{P}$$

This implies $p_j \mid 1$, so $p_j \leqslant 1$. However, $p_j > 1$ since p_j is prime. ↯

Therefore, $p_0, \ldots p_k$ must *not* have been a complete list of the primes. Applying this argument to any *finite* set of primes leads us to our conclusion: *there are not finitely many prime numbers.* Q.E.D.

Definition* 5.4 *(Greatest Divisors and Least Multiples).

$\gcd(a, b)$ The *greatest common divisor* of two integers $a, b \in \mathbb{Z}$—denoted $\gcd(a, b)$—is a natural number $d \in \mathbb{N}$ that lives up to its name: d is a *common divisor* of a and b, and d is *greatest* among all possible common divisors.

1. $\gcd(a, b) \mid a$
2. $\gcd(a, b) \mid b$
3. $(\forall z \in \mathbb{Z})\Big(\big(z \mid a \wedge z \mid b\big) \Rightarrow z \mid \gcd(a, b)\Big)$

Note that we define the *greatness* of $\gcd(a, b)$ with respect to *divisibility* as opposed to the traditional $\leqslant$ linear ordering. This allows us to observe $\gcd(0, 0) = 0$ where it would otherwise not be well-defined.

$\operatorname{lcm}(a, b)$ We define the *least common multiple* of $a, b \in \mathbb{Z}$ *dually* as the common multiple that is *least* among all possible common multiples.

1. $a \mid \operatorname{lcm}(a, b)$
2. $b \mid \operatorname{lcm}(a, b)$
3. $(\forall z \in \mathbb{Z})\Big(\big(a \mid z \wedge b \mid z\big) \Rightarrow \operatorname{lcm}(a, b) \mid z\Big)$

These definitions can naturally be extended to finite sets of more than two integers at a time. 定義

Definition* 5.5 *(Coprimality).

coprime We say $x, y \in \mathbb{Z}$ are *coprime* when $\gcd(x, y) = 1$. Given $\mathcal{Z} \subseteq \mathbb{Z}$ and $k \in \mathbb{N} \setminus 2$, we say the numbers in $\mathcal{Z}$ are *k-wise relatively prime* when $\gcd(z_0, z_1, \ldots z_{k-1}) = 1$ for each choice of distinct $z_0, z_1, \ldots z_{k-1} \in \mathcal{Z}$. 定義

***Lemma* 5.3.**

For any $a, b \in \mathbb{Z}$, the following two statements are *true.*

1. $\gcd(a, b) = 0 \Leftrightarrow (a = 0 \wedge b = 0)$
2. $\gcd(a, b) \geqslant 1 \Leftrightarrow (a \neq 0 \vee b \neq 0)$

Further, $\gcd(x, x) = \gcd(x, 0) = x$ and $\gcd(x, 1) = 1$ for all $x \in \mathbb{Z}$. 引理

***Theorem* 5.7.**

Given arbitrary integers $a, b \in \mathbb{Z}$, the following statement is *true.*

$$\gcd(a, b) = 1 \Leftrightarrow (\forall p \in \mathbb{N})\Big(p \textit{ is prime} \Rightarrow \big(p \nmid a \vee p \nmid b\big)\Big)$$

This means precisely that *coprime numbers share no prime factors*. 定理

Lemma* 5.4 *(Euclid's Division Lemma).
If $a, b \in \mathbb{Z}$ and $b \neq 0$, there exist *unique* $q, r \in \mathbb{Z}$ satisfying the following.

$$a = q \cdot b + r \qquad \text{and} \qquad 0 \leqslant r < |b|$$

We call q and r above the *quotient* and *remainder* respectively. 引理

Algorithm* 5.1 *(Euclidean Division).
Given $a, b \in \mathbb{Z}$, we compute their greatest common divisor as follows.

$$\texttt{gcd}(a,b) := \begin{cases} a & \textit{if } b = 0 \\ \texttt{gcd}(b,r) & \textit{if } b \neq 0, \textit{ where } r \in \mathbb{Z} \textit{ is the integer satisfying} \\ & \qquad\qquad (\exists q \in \mathbb{Z})(a = qb + r) \wedge 0 \leqslant r < |b| \end{cases}$$

演算法

```
def gcd(a, b):
  return a if b == 0 else gcd(b, a % b)
```

Figure 5.2: A recursive `Python` implementation of the *Euclidean division algorithm* in $\mathcal{O}(\log(\min(a,b)))$ time and $\mathcal{O}(1)$ space.

Theorem* 5.8 *(Bézout's Identity).
$(\forall a, b \in \mathbb{Z})(\exists x, y \in \mathbb{Z})\big(ax + by = \gcd(a,b)\big)$. 定理

Theorem* 5.9 *(Euclid's Lemma).
For any $a, b \in \mathbb{Z}$ and any prime $p \in \mathbb{N}$, if $p \mid ab$, then $p \mid a$ or $p \mid b$. 定理

Proof. Let $a, b \in \mathbb{Z}$ and let $p \in \mathbb{N}$ be prime such that $p \mid ab$. If $p \mid a$, then we are done; on the contrary, suppose $p \nmid a$. Since p is prime, we can derive $q \nmid p \vee q \nmid a$ for any arbitrary prime $q \in \mathbb{N}$ as follows.

$$q \mid p \quad \Rightarrow \quad q \in \{1, p\} \quad \Rightarrow \quad q = p \quad \Rightarrow \quad q \nmid a$$

This tells us p and a *share no prime factors*, so $\gcd(p,a) = 1$. Applying *Bézout's identity*, there exist $x, y \in \mathbb{Z}$ making the following equality hold.

$$1 = px + ay$$

Since $p \mid ab$, we know $pk = ab$ for some $k \in \mathbb{Z}$. Now, we can sit back.

$$\begin{aligned} 1 = xp + ya &\Rightarrow 1b = (px + ay)b \\ &\Rightarrow b = (px)b + (ay)b \\ &\Rightarrow b = p(xb) + (ab)y \\ &\Rightarrow b = p(xb) + (pk)y \\ &\Rightarrow b = p(xb) + p(ky) \\ &\Rightarrow b = p(xb + ky) \end{aligned}$$

This demonstrates $p \mid b$ because $xb + ky \in \mathbb{Z}$. Q.E.D.

***Corollary* 5.1.**
For any $a, b, c \in \mathbb{Z}$, if $a \mid bc$ and $\gcd(a,b) = 1$, then $a \mid c$. 推論

6

Combinatorics

> *"What we can't say we can't say, and we can't whistle it either."*
>
> – Frank P. Ramsey

The study of counting.

6.1 *Judging the Size of a Set*

function

Recall that a *function* $f : X \to Y$ from a *domain* X to a *codomain* Y establishes a *relation* that associates *every* element $x \in X$ of the domain with *exactly one* element $f(x) \in Y$ of the codomain.

$$(\forall x \in X)(\exists! y \in Y)\big(f(x) = y\big)$$

The phrase $f : X \to Y$ can be read either as the *noun* *"f from X to Y"* or as the *full sentence* *"f is a function from X to Y"* depending on context.

image

preimage

Commonly, *the output* $f(x) \in Y$ of a given input $x \in X$ is called the *image of x under f*. Analogously, *the input* $x \in X$ that generates a given output $y := f(x) \in Y$ is referred to as the *preimage of y under f*.

When $f(x) = y$, we refer to x as the *preimage* of y, and we call y the *image* of x.

***Definition* 6.1.**

injection

Let X and Y be sets and consider a function $f : X \to Y$. We say that f is *injective* if f always maps *distinct inputs* to distinct outputs.[2] Formally, this means f satisfies the following statement.

$$(\forall a, b \in X)\big(f(a) = f(b) \;\Rightarrow\; a = b\big)$$

An equivalent, but often more useful, way to express this is given below.

$$(\forall a, b \in X)\big(a \neq b \;\Rightarrow\; f(a) \neq f(b)\big)$$

Once we know that f is an injection, we can denote this characteristic of f by writing $f : X \hookrightarrow Y$, reading this as *"f is an injection from X to Y"* or *"f injects X into Y"* to taste. Notice the use of the word *"into."*

surjection

We say that f is *surjective* when *every codomain element has a preimage*.[3] This means that f *"covers"* its entire codomain—that the range of f is identical to its codomain. Formally, we say this as follows.

$$(\forall y \in Y)(\exists x \in X)(f(x) = y)$$

[2] *Injections* are also known as *"one-to-one."*

[3] *Surjections* are sometimes called *"onto."*

Knowing that f is surjective grants access to the convenient denotational syntax $f : X \twoheadrightarrow Y$, which can be read as *"f is a surjection from X to Y"* or *"f surjects X onto Y."* Notice the use of the word *"onto."*

bijection

When f is both injective and surjective at the same time, we say that the function is *bijective* and use the combined $f : X \hookrightarrow\!\!\!\!\rightarrow Y$ syntax.[1] 定義

It's often a good idea to have a visual in mind to ground your intuition. In the same way that we can think of *functions* as *"curves that pass the vertical line test,"* we can think of *injective functions* as *"curves that pass the horizontal line test."*

We judge the relative sizes of sets by the kinds of functions that exist between them, and use the notions of injectivity and surjectivity to give formal meaning to *"the size of a set."*

Definition* 6.2 *(Equinumerosity).
We define A to be *no smaller than* B when A can be *injected* into B.

$|A| \leqslant |B|$

$$|A| \leqslant |B| \;:\Leftrightarrow\; \exists f(f : A \hookrightarrow B)$$

We define A to be *no larger than* B when A can be *surjected* onto B.

$|A| \geqslant |B|$

$$|A| \geqslant |B| \;:\Leftrightarrow\; \exists g(g : A \twoheadrightarrow B)$$

We say that two sets A and B have the *same cardinality*—meaning *same size* or *same number of elements*—there is a *bijection* between A and B.

$|A| = |B|$

$$|A| = |B| \;:\Leftrightarrow\; \exists h(h : A \hookrightarrow\!\!\!\!\rightarrow B)$$

Definitions for $|A| < |B|$ and $|A| > |B|$ spring naturally from these. 定義

Lemma* 6.1 *(Reflexivity of Cardinality).
$\forall A(|A| = |A|)$. 引理

Proof. Let A be a set and consider the function $f : A \to A$ given by $f(a) := a$ for every $a \in A$. We will show f is a bijection.

To show f is injective, suppose $a_1, a_2 \in A$ and assume $f(a_1) = f(a_2)$. Then, since $f(a_1) = a_1$ and $f(a_2) = a_2$, we know $a_1 = a_2$ by definition. This proves $(\forall x, y \in A)(f(x) = f(y) \Rightarrow x = y)$, meaning f is injective.

To show that f is surjective, let $a \in A$ and observe $f(a) = a$. This proves $(\forall y \in A)(\exists x \in A)(f(x) = y)$, meaning f is surjective.

Therefore, since f is both injective and surjective, we know that f is a bijection from A to A, and thus $|A| = |A|$ by definition. Q.E.D.

[1] There are *"people"* who refer to *bijections* as *"one-to-one correspondences."* They have been abandoned by God and will never feel the warm light of heaven.

$\mathtt{id}_X$

The above lemma involves an important construction that shows up frequently in many contexts.[1] The *identity function on a set X* is the function $\mathtt{id}_X : X \to X$ that maps every element of X back to itself; formally, $\mathtt{id}_X(x) := x$ for every $x \in X$. This function *always* exists for any X, and this function is *always* a bijection on X. This is actually a special case of $X \subseteq Y$, in which case we can make a very similar construction known as the *canonical embedding of X in Y*, which is the unique injection that identifies in Y those elements that are also in the subset X. Every injection $X \hookrightarrow Y$ between any two arbitrary sets is a *"structure-preserving map,"* also known as an *embedding*, that identifies *a substructure of Y that "looks like X."* When $X \subseteq Y$, the *canonical* embedding picks out an identical copy of X within Y.

***Lemma* 6.2.**
$\forall A \forall B(A \subseteq B \Rightarrow |A| \leqslant |B|)$. 引理

Proof. Consider sets A and B such that $A \subseteq B$, and let $f : A \to B$ be the function given by $f(a) := a$ for $a \in A$.[2] We will show f is injective. Let $a_1, a_2 \in A$ such that $f(a_1) = f(a_2)$. We then have $a_1 = a_2$ by definition of f. Therefore, f is injective, so $|A| \leqslant |B|$ by definition. Q.E.D.

These definitions expose to us a formal way of *counting* the elements of a set. Suppose we have a set $\mathcal{A} := \{a, b, c, d\}$. To count the elements of $\mathcal{A}$, we might point at a first, then b second, then c third, and finally d. This implicitly defines the function $f : \{0, 1, 2, 3\} \to \{a, b, c, d\}$ below.

$$\begin{tikzcd}
0 \arrow[r, mapsto, "f"] & a \\
1 \arrow[r, mapsto, "f"] & b \\
2 \arrow[r, mapsto, "f"] & c \\
3 \arrow[r, mapsto, "f"] & d
\end{tikzcd}$$

We can interpret this mapping as saying that the element a that f assigns as the output of 0 is the *first* element of $\mathcal{A}$, with the element b being the *second* because it is the output of 1 under f, and so on. If this *"counting function"* f is a bijection, then what we've done is establish a perfect association between $\mathcal{A}$ and *the natural number* $4 = \{0, 1, 2, 3\}$.[3] Any other set in bijection with $\mathcal{A}$ will also be in bijection with 4, so we can think of 4 as the *canonical representative* of *"sets with 4 elements."*

cardinal

$|X|$

We refer to these canonical representatives as *cardinal numbers*, and we use the notation $|X|$ to refer to *the cardinality of X*—the cardinal number that represents the *"size of X."*

If a set is what we call *"finite,"* then we should be able to count its elements using a natural number $n = \{0, 1, \ldots, n-1\}$, and in that case the *natural* choice of cardinal for X is simply $|X| = n$.

[1] We will soon see this is an echo of a recurring pattern we already encountered.

[2] The fact that $A \subseteq B$ guarantees that $\{f(a) \mid a \in A\} \subseteq B$, ensuring existence of the output of f for every input. Uniqueness of these outputs is given by the *axiom of extensionality.*

[3] Recall $n := \{0, 1, \ldots, n-1\}$ for $n \in \mathbb{N}$.

Definition* 6.3 *(Finite).
We say a set F is *finite* if there exists $n \in \mathbb{N}$ such that $|F| = |n|$. In this situation, the natural number n is *unique*, so we define $|F| := n$. 定義

***Lemma* 6.3.**
For any $n \in \mathbb{N}$, we have $|\{1, 2, \dots n\}| = n$. 引理

Proof. Let $n \in \mathbb{N}$. We will show $|\{1, 2, \dots n\}| = |\{0, 1, \dots n-1\}|$. Consider the function $f : \{1, 2, \dots n\} \to \{0, 1, \dots n-1\}$ given by $f(x) := x - 1$ for each $x \in \{1, 2, \dots n\}$.

To see that f is an injection, consider $a, b \in \{1, 2, \dots n\}$ and suppose $f(a) = f(b)$. We then know $a - 1 = b - 1$ by the definition of f. Cancelling on both sides then yields $a = b$ as desired.

To see that f is surjective, let $y \in \{0, 1, \dots n-1\}$. Notice $0 \leqslant y \leqslant n-1$, so that $1 \leqslant y + 1 \leqslant n$, implying $y + 1 \in \{1, 2, \dots n\}$.[1] We can now simply observe that $f(y+1) = (y+1) - 1 = y$. Q.E.D.

It should hopefully be intuitively straightforward to say that *"every set has a size,"* and that therefore the cardinalities of sets are always comparable: for any two sets A and B, we should know that either $|A| \leqslant |B|$ or that $|B| \leqslant |A|$. As it turns out, *this is not a theorem* that we can prove using the massive mathematical system we've established. If we want to know this fact, we need one final axiom.[2]

Axiom* 7 *(Equivalent to the Axiom of Choice).
Every set has a unique cardinality. 公理

Theorem* 6.1 *(Dichotomy of Cardinality).
For any sets A and B, either $|A| \leqslant |B|$ or $|B| \leqslant |A|$. 定理

6.2 *Compositionality and Invertibility*

Definition* 6.4 *(Composition).
Let X, Y, and Z be sets. Given *compatible* functions $f : X \to Y$ and $g : Y \to Z$, the *composition of g with f* is a function $g \circ f : X \to Z$ defined by $(g \circ f)(x) := g\big(f(x)\big)$ for all $x \in X$. We read the name of this function as *"g composed with f"* or *"g after f."* 定義

$g \circ f$

Theorem* 6.2 *((·)-jections are (·)-morphisms).
Let X and Y be sets and consider a function $f : X \to Y$. If we know f is an injection, then f must have a *surjective left inverse* and vice versa.

$|X| \leqslant |Y| \Leftrightarrow |Y| \geqslant |X|$

$$f \text{ is injective} \Leftrightarrow (\exists g : Y \twoheadrightarrow X)(g \circ f = \mathtt{id}_X)$$

Conversely, f is a surjection exactly when f has an *injective right inverse.*

$|X| \geqslant |Y| \Leftrightarrow |Y| \leqslant |X|$

[1] This verifies $y + 1$ is in the domain of f.

[2] While this is the final axiom we will be introducing for our purposes, there *is* actually one more axiom in standard ZFC: *the axiom schema of replacement*, which tersely says *"the image of a set under a definable class function is a set"* We won't be using this axiom for anything, so it won't be mentioned or discussed in the text.

$$f \textit{ is surjective } \Leftrightarrow (\exists g : Y \hookrightarrow X)(f \circ g = \texttt{id}_Y)$$

When f is a bijection, there is a *unique*, *bijective*, *two-sided inverse* for f.

$|X| = |Y| \Leftrightarrow |Y| = |X|$

$$f \textit{ is bijective } \Leftrightarrow (\exists! g : Y \hookrightarrow\!\!\!\!\rightarrow X)(g \circ f = \texttt{id}_X \wedge f \circ g = \texttt{id}_Y)$$

f^{-1} In this last case, when f is bijective, we refer to the unique two-sided inverse of f as *the inverse of f* and use f^{-1} to denote this function. 定理

Theorem* 6.3 *(Cantor-Schröder-Bernstein).
Suppose X and Y are sets. If there exist injections $f : X \hookrightarrow Y$ and $g : Y \hookrightarrow X$ in opposite directions between the two sets, then a bijection $h : X \hookrightarrow\!\!\!\!\rightarrow Y$ exists from one set to the other. We restate this as follows.

$$\forall A \forall B \Big((|A| \leqslant |B| \wedge |B| \leqslant |A|) \Rightarrow |A| = |B| \Big)$$

Notice that this establishes the *antisymmetry of cardinality.* 定理

6.3 *Counting with Our Fingers*

***Theorem* 6.4.**
If A and B are finite sets, then $|A \times B| = |A| \cdot |B|$. 定理

This is one of the reasons why $A \times B$ is called the Cartesian *product* of A with B.

Theorem* 6.5 *(Inclusion/Exclusion Principle).
If A and B are finite, then $|A \cup B| = |A| + |B| - |A \cap B|$. In general, given n finite sets $A_1, A_2, \ldots A_n$ with $n \in \mathbb{N}_+$, the following is *true.*

$$\left| \bigcup_{i=1}^{n} A_i \right| = \sum_{k=1}^{n} (-1)^{k+1} \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}| \leqslant \sum_{i=1}^{n} |A_i|$$

As a consequence, the union of finitely many finite sets is finite. 定理

***Corollary* 6.1.**
If A and B are finite and $B \subseteq A$, then $|A \setminus B| = |A| - |B|$. 推論

***Definition* 6.5.**
The *floor function* is the map $\lfloor \cdot \rfloor : \mathbb{R} \to \mathbb{Z}$ given below for any $x \in \mathbb{R}$.

$$\lfloor x \rfloor := \max\{z \in \mathbb{Z} \mid z \leqslant x\}$$

$\lfloor x \rfloor$ This defines $\lfloor x \rfloor$ to be the *greatest integer less than or equal to x.*[1] In other words, $\lfloor x \rfloor$ is the result of *rounding x down* to the nearest integer. The *ceiling function* $\lceil \cdot \rceil : \mathbb{R} \to \mathbb{Z}$, given below, is dual to the floor function.

$$\lceil x \rceil := \min\{z \in \mathbb{Z} \mid z \geqslant x\}$$

$\lceil x \rceil$ This defines $\lceil x \rceil$ as the *least integer greater than or equal to x,* which corresponds analogously to *rounding x up* to the nearest integer. 定義

[1] As with any definition we make, but especially with definitions such as these where we define an *object* based on a *property we want it to have,* we should always ask the question: does such an object *actually exist?* As with the $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$ for $a, b \in \mathbb{Z}$, the answer here is that *yes,* $\lfloor x \rfloor$ always exists for any $x \in \mathbb{R}$.

Theorem* 6.6 *(Pigeonhole Principle).
Consider any two sets A and B. The following two statements are *true.*

$$|A| > |B| \Rightarrow (\forall f : A \to B)(f \text{ is not injective})$$
$$|A| < |B| \Rightarrow (\forall f : A \to B)(f \text{ is not surjective})$$

Further, if there exist $n, k \in \mathbb{N}_+$ such that $|A| = n$ and $|B| = k$, then for any $f : A \to B$ there exists $b \in B$ for which the inequality below holds.

$$\Big|\{a \in A \mid f(a) = b\}\Big| \geqslant \left\lfloor \frac{n-1}{k} \right\rfloor + 1 = \left\lceil \frac{n}{k} \right\rceil$$

定理

6.4 *Structure and Substructure*

Definition* 6.6 *(Combination).
Given a finite set A of cardinality $n := |A|$, we know that the set of *all possible* subsets of A is given by $\mathbb{P}(A) = \{z \mid z \subseteq A\}$. We now know that each of those subsets $B \subseteq A$ must have cardinality $B \in \{0, \ldots n\}$. Letting $k := |B|$, we say that B in this case is a *k-combination of A*.

k-combination

For any natural numbers $n, k \in \mathbb{N}$, we define the combinatorial number *n choose k* to be the number of cardinality k subsets of n as below.

n choose k

$$\binom{n}{k} := \Big|\{z \mid z \subseteq \{0, 1, \ldots, n-1\} \wedge |z| = k\}\Big|$$

$\binom{n}{k}$

We denote *n choose k* with the notation $\binom{n}{k}$. Since the *identities* of the elements of a set don't influence its *size,* it should be clear to see that *$\binom{n}{k}$ measures the number of k-combinations of any set of cardinality n*.

$$\forall X (\forall n, k \in \mathbb{N}) \left(|X| = n \Rightarrow \Big|\{z \mid z \subseteq X \wedge |z| = k\}\Big| = \binom{n}{k} \right)$$

定義

1

1 1

1 2 1

1 3 3 1

1 4 6 4 1

1 5 10 10 5 1

1 6 15 20 15 6 1

1 7 21 35 35 21 7 1

1 8 28 56 70 56 28 8 1

1 9 36 84 126 126 84 36 9 1

Figure 6.1: Ten rows of Pascal's triangle.

***Theorem* 6.7.**
Let $n, k \in \mathbb{N}$. The numbers $\binom{n}{k}$ satisfy the following recurrence relation.

$$\binom{n}{0} = \binom{n}{n} = 1 \qquad \binom{n+1}{k+1} = \binom{n}{k+1} + \binom{n}{k}$$

In the edge cases, we know $k > n \Leftrightarrow \binom{n}{k} = 0$. 定理

***Theorem* 6.8.**
Let $n, k \in \mathbb{N}$ such that $k \leqslant n$. Then, $\binom{n}{k} = \binom{n}{n-k}$. 定理

Theorem* 6.9 *(Binomial Theorem).
Let $x, y \in \mathbb{R}$ and $n \in \mathbb{N}$. The following equality then holds.

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

定理

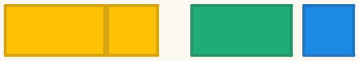


Figure 6.2: The binomial line $(x+y)^1$ can be written $1x + 1y$.

To understand this intuitively, consider expanding the product below.

$$(x+y)^2 = x^2 + xy + yx + y^2$$

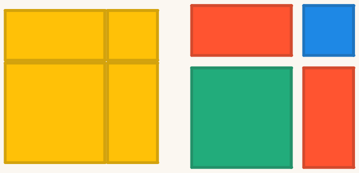
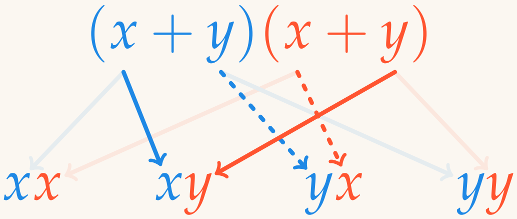


Figure 6.3: The binomial square $(x+y)^2$ can be written $1x^2 + 2xy + 1y^2$.

When we fully distribute $(x+y)^2 = (x+y)(x+y)$, each term in the resulting sum will have exactly two factors[1] because each copy of $(x+y)$ contributes either an x or a y to that term. We obtain the $xx = x^2$ in the final sum when both $(x+y)$ factors contribute one x to the term. Since there is only one way to select an x from each factor, there is only one copy of x^2 in the final result. Analogous reasoning applies to y^2. The xy term in the sum is produced by taking an x from the first $(x+y)$ and a y from the second; however, because multiplication is commutative, this is equal to the yx term we would get from taking a y from the first $(x+y)$ and an x from the second. Notice, in this scenario, that we are selecting a *total* of one x and one y from among all the $(x+y)$, and that there are *two* ways to make such a selection, resulting in a $2xy$ term in the final sum. We can generalize this argument as follows.



$$(x+y)^n = x^n + x^{n-1}y + x^{n-2}yx + \cdots + yxy^{n-2} + xy^{n-1} + y^n$$

When distributing the n copies of $(x+y)$ above, each term in the resulting sum will have k copies of x and $n-k$ copies of y, with each value of $k \in \{0, \ldots, n\}$ accounting for one of these terms.[2] When we pick k of the $(x+y)$ to select an x from, we are immediately determining that the remaining $n-k$ must be copies of y. Every time that we do this, we are selecting k of the $(x+y)$ to contribute their x, and this collection of k-many $(x+y)$ taken out of the total n-many $(x+y)$ corresponds precisely *(bijectively!)* to a k-combination taken from a size n set. This should make it clear then that the number of copies of $x^k y^{n-k}$ in the final result—after commuting—will be exactly $\binom{n}{k}$. Summing over the range of values for k yields the result $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$.

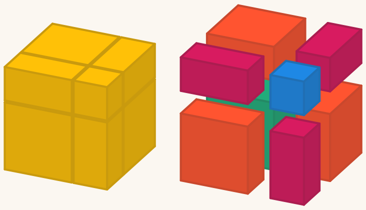


Figure 6.4: The binomial cube $(x+y)^3$ can be written $1x^3 + 3x^2y + 3xy^2 + 1y^3$.

[1] This can easily be proven by induction.

[2] Remember that each term of the resulting sum must have a total of n factors.

***Corollary* 6.2.**
If X is a finite set, then $|\mathbb{P}(X)| = 2^{|X|}$. 推論

6.5 *Arrangement and Derangement*

Definition* 6.7 *(String).
Given a natural number $n \in \mathbb{N}$ and a set $\mathcal{A}$, a *finite string* over $\mathcal{A}$ is simply a function $f : n \to \mathcal{A}$. The *length* of the string f is given by $|f| = |n| = n$.[1] We refer to $f(i)$ as the *i^{th} character* of the string, and we thus sometimes call $\mathcal{A}$ an *alphabet* appropriately. If $k \in n$ and $\ell \leqslant n$, then we call the function $f[k : k+\ell] : \ell \to \mathcal{A}$ that maps $f[k : k+\ell](x) := f(x-k)$ for each $x \in N$ a *substring* of f of length ℓ.[2] We will adopt the convention $f[:\ell] := f[0:\ell]$ and $f[k:] := f[k:n]$.

$f[k : k+\ell]$

The *concatenation* of two finite strings $f : k_1 \to \mathcal{A}$ and $g : k_2 \to \mathcal{B}$ is another string, denoted $f \mathbin{+\!\!+} g : (k_1 + k_2) \to \mathcal{A} \cup \mathcal{B}$ and defined below.

$f \mathbin{+\!\!+} g$

$$(f \mathbin{+\!\!+} g)(x) := \begin{cases} f(x) & \text{if } 0 \leqslant x < k_1 \\ g(x-k_1) & \text{if } k_1 \leqslant x < k_1 + k_2 \end{cases}$$

定義

When f is a finite string of length n, we will sometimes take the convenience of notating the string by writing "$f(0)f(1)\dots f(n-1)$". For example, let $s : 12 \to \{\mathtt{d},\mathtt{e},\mathtt{h},\mathtt{l},\mathtt{o},\mathtt{r},\mathtt{w},\mathtt{!},\text{␣}\}$ be the following string.

$$\begin{array}{lcl} 0 \longmapsto \mathtt{h} & \quad & 6 \longmapsto \mathtt{w} \\ 1 \longmapsto \mathtt{e} & & 7 \longmapsto \mathtt{o} \\ 2 \longmapsto \mathtt{l} & & 8 \longmapsto \mathtt{r} \\ 3 \longmapsto \mathtt{l} & & 9 \longmapsto \mathtt{l} \\ 4 \longmapsto \mathtt{o} & & 10 \longmapsto \mathtt{d} \\ 5 \longmapsto \text{␣} & & 11 \longmapsto \mathtt{!} \end{array}$$

By writing $s =$ "hello␣world!", we say that $|s| = 12$ and that the first character of s is $s(0) = \mathtt{h}$, the second character is $s(1) = \mathtt{e}$, and so on. By writing $s[6:11]$, we refer to the substring "world" of length $|\text{"world"}| = 5$. The concatenation $s[:5] \mathbin{+\!\!+} s[5:6] \mathbin{+\!\!+} s[6:11] \mathbin{+\!\!+} s[11:]$ is then "hello" ⧺ "␣" ⧺ "world" ⧺ "!" and is another way to rewrite s.

***Theorem* 6.10.**
Given two finite sets X and Y, there exist $|Y|^{|X|}$ distinct *functions* from X to Y. Formally, $\big|\{f \mid f : X \to Y\}\big| = |Y|^{|X|}$ for any finite X and Y. As a consequence, we know that there are n^k distinct *strings* of length $k \in \mathbb{N}$ over any finite alphabet A of cardinality $n \in \mathbb{N}$. Formally stated, $\big|\{\text{"}\mathtt{a}_0\mathtt{a}_1\dots\mathtt{a}_{k-1}\text{"} \mid (\forall i \in k)(\mathtt{a}_i \in A)\}\big| = n^k$ when $|A| = n \in \mathbb{N}$. 定理

Inspired by this theorem, some authors write the set $\{f \mid f : A \to B\}$ as B^A, so $|B^A| = |B|^{|A|}$. Accordingly, the set of functions from A to B is sometimes called an *exponential object in the category of sets.*

[1] Remember that a function is formally just a set of ordered pairs, so the string $f : 3 \to \{\mathtt{a},\mathtt{b},\mathtt{c}\}$ given by $f =$ "bac" is actually the set $f = \{(0,\mathtt{b}),(1,\mathtt{a}),(2,\mathtt{c})\}$. In fact, whenever $\varphi : X \to Y$ is a function, we know $|\varphi| = |X|$.

[2] The notation $f[k : k+\ell]$ is often called *slice indexing* when applied to lists or arrays in a programming language. In that context, the substring $f[k : k+\ell]$ would be called a *slice* of f starting from index k and ending at index $k+\ell-1$.

Definition* 6.8 *(Factorial).
The *factorial* $(\,\cdot\,)! : \mathbb{N} \to \mathbb{N}$ is the recursively defined function below.

$$\begin{aligned} 0! &:= 1 \\ (n+1)! &:= (n+1) \cdot n! \end{aligned}$$

$n!$

When $n > 0$, we can write $n! = \left(\prod_{i=1}^{n} i\right) = n \cdot (n-1) \cdots 3 \cdot 2 \cdot 1.$ 定義

***Theorem* 6.11.**
There exist $|Y|!/(|Y|-|X|)!$ distinct *injective functions* between any two finite sets X and Y that satisfy $|X| \leqslant |Y|$.[1] We write this formally below.

$$\left|\left\{f \mid f : X \hookrightarrow Y\right\}\right| = \begin{cases} \frac{|Y|!}{(|Y|-|X|)!} & \textit{if} \quad |X| \leqslant |Y| \in \mathbb{N} \\ 0 & \textit{otherwise} \end{cases}$$

As a consequence, if A is a finite alphabet of cardinality $n \in \mathbb{N}$ and $k \leqslant n$, then there are $n!/(n-k)!$ *strings* of length k over A whose *characters are all distinct*. This is written formally below assuming $k \leqslant n = |A|$.

$$\left|\left\{\texttt{"a}_{\texttt{0}}\texttt{a}_{\texttt{1}}\texttt{...a}_{\texttt{k-1}}\texttt{"} \;\middle|\; (\forall i,j \in k)\left(\texttt{a}_{\texttt{i}} \in A \wedge \left(i \neq j \Leftrightarrow \texttt{a}_{\texttt{i}} \neq \texttt{a}_{\texttt{j}}\right)\right)\right\}\right| = \frac{n!}{(n-k)!}$$

定理

***Theorem* 6.12.**
Let X and Y be finite sets and $k_1, k_2 \in \mathbb{N}$ and suppose we have two sets of strings $F_X \subseteq \{f \mid f : k_1 \to X\}$ and $G_Y \subseteq \{g \mid g : k_2 \to Y\}$ of lengths k_1 and k_2 over X and Y respectively. Then, the following equality holds.

$$\left|\left\{f \mathbin{+\!\!+} g \;\middle|\; (f \in F_X) \wedge (g \in G_Y)\right\}\right| = |F_X| \cdot |G_Y|$$

定理

Definition* 6.9 *(Permutation).

permutation

Given a set X, we call a bijection $f : X \lhook\joinrel\twoheadrightarrow X$ a *permutation on X*. 定義

***Theorem* 6.13.**
Given a finite set X, there are $|X|!$ distinct *permutations* on X. Consequently, if $|X| = n \in \mathbb{N}$, then there are $n!$ *strings* of length n over X where *all the characters are distinct*. 定理

6.6 *Equivalence and Partitioning*

Given a nonempty set $X \neq \varnothing$, a partition is a way of splitting up X into a collection of non-empty subsets such that every element of X appears in *exactly one* of those subsets. Formally, for any $P \subseteq \mathbb{P}(X)$, we say P is a *partition of X* if P satisfies each of the following three criteria.

partition

[1] In the case that $X \subseteq Y$, we let $k := |X|$ and refer to any injection $f : X \hookrightarrow Y$ as a *k-permutation of Y*.

1. $(\forall A \in P)(A \neq \varnothing)$.
2. $(\forall A, B \in P)(A \neq B \Rightarrow A \cap B = \varnothing)$.
3. $\cup P = X$.

Partitions of sets have several nice combinatorial properties. For instance, whenever we have a partition P of a finite set X, we know that $\sum_{p \in P} |p| = |X|$. This follows from the *inclusion/exclusion theorem* using the facts that $\cup P = X$ and that the sets in that union are all pairwise disjoint from each other (so the higher-order terms will be zero).

Every partition on a set defines a different notion of *equivalence* for the elements of that set. To see what we mean by this, we introduce a new definition. A relation $R \subseteq X \times X$ on a set X is called an *equivalence relation* if R is *reflexive*, *symmetric*, *and* *transitive*. These three qualities are defined formally below.

1. $(\forall a \in X)\big((x, x) \in R\big)$. *reflexivity*
2. $(\forall a, b \in X)\big((a, b) \in R \Rightarrow (b, a) \in R\big)$. *symmetry*
3. $(\forall a, b, c \in X)\big(((a, b) \in R \land (b, c) \in R) \Rightarrow (a, c) \in R\big)$. *transitivity*

$[a]_R$

X/R

Given an element $a \in X$, the *equivalence class of a* under the equivalence relation R is given by $[a]_R := \{b \in X \mid (a, b) \in R\}$, which is the set of all elements $b \in X$ that a is *equivalent to according to R*. As it turns out, the set of all equivalence classes according to R *is a partition on X*. We denote this set of all equivalence classes by $X/R := \{[x]_R \mid x \in X\}$.[1]

***Lemma* 6.4.**
If R is an equivalence relation on X, then X/R is a partition on X. 引理

Proof. Let X be a set and let R be an equivalence relation on X. We will show that $X/R = \{[x]_R \mid x \in X\}$ is a partition on X.

> First, take an arbitrary equivalence class $[x]_R \in X/R$, where $x \in X$. We know $(x, x) \in R$ since R is reflexive, so $x \in [x]_R$. This shows $[x]_R \neq \varnothing$.
>
> Next, consider $[x]_R, [y]_R \in X/R$ with $x, y \in X$ and assume $[x]_R \neq [y]_R$. Towards a contradiction, assume $[x]_R \cap [y]_R \neq \varnothing$. Then, there exists i such that $i \in [x]_R$ and $i \in [y]_R$. Let $z \in X$ and observe the following.
>
> $$\begin{aligned} z \in [x]_R &\Leftrightarrow (x, z) \in R && \text{by definition} \\ &\Leftrightarrow (z, x) \in R && \text{by } \textit{symmetry} \text{ of } R \\ &\Leftrightarrow (z, x) \in R \land (x, i) \in R && \text{because } i \in [x]_R \\ &\Leftrightarrow (z, i) \in R && \text{by } \textit{transitivity} \text{ of } R \\ &\Leftrightarrow (z, i) \land (i, y) \in R && \text{because } i \in [y]_R \\ &\Leftrightarrow (z, y) \in R && \text{by } \textit{transitivity} \text{ of } R \\ &\Leftrightarrow z \in [y]_R && \text{by definition} \end{aligned}$$
>
> Then, $[x]_R = [y]_R$ by the *axiom of extensionality*. ↯ Thus, $[x]_R \cap [y]_R = \varnothing$.

[1] This is typically read *"X mod R."*

Finally, let $x \in X$. We know $(x,x) \in R$ because R is *reflexive*, so $x \in [x]_R$. Since $[x]_R \in X/R$, we have that $x \in \cup(X/R)$. This shows $X \subseteq \cup(X/R)$. Conversely, let $y \in \cup(X/R)$. Then, $y \in [z]_R$ for some $z \in X$, which means $(y,z) \in R$. Since $R \subseteq X \times X$, we then know $y \in X$. Therefore, $\cup(X/R) = X$ by the *axiom of extensionality*.

These three observations let us conclude that X/R partitions X. Q.E.D.

***Lemma* 6.5.**
If P partitions X, then $P = X/R$ for some equivalence relation R. 引理

Proof. Let X be a set and suppose P is a partition on X. Consider the relation $R := \{(a,b) \in X \times X \mid (\exists Z \in P)(a \in Z \wedge b \in Z)\}$. First, we will show that R is an equivalence relation on X.

Reflexivity:
Let $x \in X$. Since $\cup P = X$, we know there exists $Z \in P$ such that $x \in Z$, implying $x \in Z \wedge x \in Z$, so $(x,x) \in R$ by the definition of R.

Symmetry:
Let $x, y \in X$ and assume $(x,y) \in R$. Then, $x \in Z \wedge y \in Z$ for some $Z \in P$. This implies $y \in Z \wedge x \in Z$, so $(y,x) \in R$ by definition.

Transitivity:
Let $x,y,z \in X$ and assume $(x,y) \in R$ and $(y,z) \in R$. Then, by the definition of R, there exist $A, B \in P$ such that $x \in A \wedge y \in A$ and $y \in B \wedge z \in B$. Since $y \in A$ and $y \in B$, we then know $y \in A \cap B$, so $A \cap B \neq \varnothing$. Therefore, $A = B$.[1] As a result, $z \in A$, letting us arrive at $x \in A \wedge z \in A$, from which we conclude $(x,z) \in R$.

Now that we know R is an equivalence relation on X, we will show that $X/R = P$. Let $A \in X/R$ and recall that $A = [x]_R$ for some $x \in X$. Since $\cup P = X$, we know there is some $Z \in P$ such that $x \in Z$.

$$\forall y(y \in Z \Leftrightarrow (x,y) \in R \Leftrightarrow y \in A)$$

Therefore, $A \in P$ because $A = Z$. This shows $X/R \subseteq P$. Conversely, let $B \in P$. $B \neq \varnothing$ because P is a partition, so there exists some $a \in B$.

$$\forall b(b \in B \Leftrightarrow (a,b) \in R \Leftrightarrow b \in [a]_R)$$

Hence, $B \in X/R$ because $B = [a]_R$; so, $P \subseteq X/R$. Thus, $P = X/R$. Q.E.D.

***Theorem* 6.14.**
For any natural numbers $n, k \in \mathbb{N}$ with $k \leqslant n$, the following are equal.

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

定理

[1] $A \cap B \neq \varnothing \Rightarrow A = B$ is the *contrapositive* of $A \neq B \Rightarrow A \cap B = \varnothing$.

6.7 Simple Graphs

V_G E_G

Graphs abstract and generalize the idea of a *relation on a set*. A *graph* G is determined by a set of *vertices* V_G that are connected together by a set of *edges* E_G in some arrangement.[1] A graph is called *simple* when *every edge is a 2-combination of nodes*, meaning that the edges are *undirected* and must connect *two distinct* vertices.[2] Formally, $\mathsf{E}_G \subseteq \{e \subseteq \mathsf{V}_V \mid |e| = 2\}$. We say a graph is *finite* when V_G and E_G are both finite.

$\mathsf{N}_G(v)$ $\mathsf{I}_G(v)$

Given a vertex $v \in \mathsf{V}_G$, we define the *neighborhood* of v in G to be the set of all vertices that connect to v through an edge in the graph and denote this by $\mathsf{N}_G(v) := \{u \in \mathsf{V}_G \mid \{u, v\} \in \mathsf{E}_G\}$. We also define the set of *incident edges* on v as the set of all edges that v participates in. Formally, $\mathsf{I}_G(v) := \{e \in \mathsf{E}_G \mid v \in e\}$. For simple graphs, $|\mathsf{N}_G(v)| = |\mathsf{I}_G(v)|$.[3]

Every *finite* graph G comes equipped with a function $\mathtt{deg}_G(v) : \mathsf{V}_G \to \mathbb{N}$ that assigns a *degree* to each node, given by $\mathtt{deg}_G(v) := |\mathsf{I}_G(v)|$.

***Lemma* 6.6.**
If G is a finite graph, then $0 \leqslant \mathtt{deg}(v) < |V(G)|$ for every $v \in V(G)$. 引理

Lemma* 6.7 *(Handshake Lemma).
Suppose G is a (finite, simple) graph on $n \geqslant 2$ nodes. Then, G contains two distinct vertices v and w such that $\mathtt{deg}(v) = \mathtt{deg}(w)$. 引理

[1] Vertices are also commonly called *nodes*.

[2] No multiedges nor self-loops.

[3] This can be proven by noticing that each neighbor of v is connected to v by *exactly one* edge, and each edge incident on v connects v to *exactly one* of its neighbors. One then simply constructs this bijection.

7

Asymptotic Analysis

Definition* 7.1 *(Landau Notation).
Given two arbitrary functions $f : \mathbb{N} \to \mathbb{R}$ and $g : \mathbb{N} \to \mathbb{R}$, we declare that *$f$ is asymptotically dominated by g* if the following sentence is *true*.

$$(\exists n \in \mathbb{N})(\exists k \in \mathbb{N})(\forall x \in \mathbb{N})\Big(n \leqslant x \;\Rightarrow\; \big|f(x)\big| \leqslant k\big|g(x)\big|\Big)$$

$\mathcal{O}(f)$

The *set of all functions that g asymptotically dominates* is denoted by $\mathcal{O}(g) := \{h : \mathbb{N} \to \mathbb{R} \mid (\exists n, k \in \mathbb{N})(\forall x \in \mathbb{N})(n \leqslant x \Rightarrow |h(x)| \leqslant k|g(x)|)\}$. With these definitions, we write $f \in \mathcal{O}(g)$—said *“f is big-oh of g”* out loud—to mean that *f grows no faster than g in the size of the input*. 定義

8

Infinity

"No one shall expel us from the paradise Cantor has created."

– David Hilbert

Figure 8.1: Georg F. L. P. Cantor

8.1 Silence

***Theorem* 8.1.**
$|\mathbb{N}| = |\mathbb{N}_+|$. 定理

Proof. Consider the function $f : \mathbb{N} \to \mathbb{N}_+$ given by $f(n) := n + 1$ for each $n \in \mathbb{N}$. We will now show that f is a bijection.

Injectivity:
Let $n, m \in \mathbb{N}$ and assume $f(n) = f(m)$. Then, $n + 1 = m + 1$, so $n = m$.

Surjectivity:
Let $y \in \mathbb{N}_+$ and notice that $y \neq 0$. By definition, we then know $y = \mathfrak{s}(x)$ for some $x \in \mathbb{N}$. We can then observe $f(x) = x + 1 = \mathfrak{s}(x) = y$.

Therefore, since f is a bijection, we can conclude $|\mathbb{N}| = |\mathbb{N}_+|$. Q.E.D.

***Theorem* 8.2.**
$|\mathbb{N}| = \left|\left\{n \in \mathbb{N} \;\middle|\; (2 \mid n)\right\}\right|$. 定理

Proof. For convenience, define $\mathbb{N}_e := \left\{n \in \mathbb{N} \;\middle|\; (2 \mid n)\right\}$ and consider the function $f : \mathbb{N} \to \mathbb{N}_e$ given by $f(n) = 2n$ for each $n \in \mathbb{N}$. We will now show that f is both injective and surjective.

Injectivity:
For any $n, m \in \mathbb{N}$, $\big(f(n) = f(m)\big) \Rightarrow (2n = 2m) \Rightarrow (n = m)$ since $2 \neq 0$.

Surjectivity:
Let $y \in \mathbb{N}_e$, so that $2 \mid y$. Then, we know there exists $k \in \mathbb{Z}$ such that $2k = y$. We know $k \geqslant 0$ because, if $k < 0$, then $2k < 0$, implying $y < 0$ and contradicting the fact that $y \geqslant 0$. Thus $k \in \mathbb{N}$ and we have $f(k) = 2k = y$.

Therefore, since f is a bijection, we can conclude $|\mathbb{N}| = |\mathbb{N}_e|$. Q.E.D.

***Theorem* 8.3.**
$|\mathbb{N}| = |\mathbb{Z}|$. 定理

Proof. Consider the function $f : \mathbb{N} \to \mathbb{Z}$ given by $f(n) := n$ for each $n \in \mathbb{N}$. To see that f is injective, take arbitrary $a, b \in \mathbb{N}$ and observe that $f(a) = f(b) \Rightarrow a = b$ because $f(a) = a$ and $f(b) = b$ by definition.

Consider the function $g : \mathbb{Z} \to \mathbb{N}$ given, for each $z \in \mathbb{Z}$, by the following.

$$g(z) := \begin{cases} 2z & \text{if } z \geqslant 0 \\ 2|z| - 1 & \text{if } z < 0 \end{cases}$$

In order to show that g is injective, let $x, y \in \mathbb{Z}$ and assume $g(x) = g(y)$. We now have two cases.

Case 1:
Suppose $g(x)$ is even. Then $g(y)$ is also even because $g(x) = g(y)$. Towards a contradiction, assume $x < 0$; this would imply $g(x) = 2|x| - 1$, telling us that $g(x)$ is odd. ↯ Therefore, $x \geqslant 0$; by the same reasoning, $y \geqslant 0$. This yields $g(x) = 2x = 2y = g(y)$, implying $x = y$ because $2 \neq 0$.

Case 2:
Suppose $g(x)$ is odd.[1] Again, we see $g(y)$ is odd because $g(x) = g(y)$. Towards a contradiction, assume $x \geqslant 0$; this implies $g(x) = 2x$, showing us that $g(x)$ is even. ↯ Therefore, as before, we obtain $x < 0$; the same reasoning leads us to realize $y < 0$. So, $g(x) = 2|x| - 1 = 2|y| - 1 = g(y)$.

$$\big(2|x| - 1 = 2|y| - 1\big) \Leftrightarrow \big(2|x| = 2|y|\big) \Leftrightarrow \big(|x| = |y|\big)$$

Now, $|x| = -x$ and $|y| = -y$ because $x < 0$ and $y < 0$, so we have $-x = -y$. We can now simply conclude $x = y$.

We now have two injections $f : \mathbb{N} \hookrightarrow \mathbb{Z}$ and $g : \mathbb{Z} \hookrightarrow \mathbb{N}$. By the grace of the *Cantor-Schröder-Bernstein theorem*, we are gifted the existence of a bijection $h : \mathbb{N} \hookrightarrow\!\!\!\!\!\rightarrow \mathbb{Z}$, letting us conclude $|\mathbb{N}| = |\mathbb{Z}|$. Q.E.D.

***Theorem* 8.4.**
$|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$. 定理

Proof. Consider the function $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ given by $f(n) := (n, n)$ for each $n \in \mathbb{N}$. Let $x, y \in \mathbb{N}$ and observe the following chain of reasoning.

$$\big(f(x) = f(y)\big) \Rightarrow \big((x, x) = (y, y)\big) \Rightarrow (x = y \wedge x = y) \Rightarrow (x = y)$$

This shows us that f is an injection by definition.

Now, consider the function $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ given by $g((n, m)) := 2^n 3^m$. In order to show that g is injective, take $(a, b), (x, y) \in \mathbb{N} \times \mathbb{N}$ such that $g((a, b)) = g((x, y))$ and assume $(a, b) \neq (x, y)$ towards a contradiction.

Case 1:
Suppose $a \neq x$. *Without loss of generality*,[2] let $a < x$. This implies $x - a > 0$, so that $x - a - 1 \geqslant 0$. We know $2^a 3^b = 2^x 3^y$, so $3^b = 2^{x-a} 3^y$, so that $3^b = 2(2^{x-a-1} 3^y)$. This means $2 \mid 3^b$ because $2^{x-a-1} 3^y \in \mathbb{Z}$. ↯

[1] Recall that even and odd are mutually exclusive and exhaustive over $\mathbb{Z}$.

[2] Because $a \neq x$ and $a, x \in \mathbb{N}$, we know that either $a < x$ or $a > x$. Technically, we *do* need to prove that a contradiction occurs in *both* cases; however, the proof we would write in the case that $a > x$ would be *identical* to the proof we written here for $a < x$ if we simply swapped the names of a and x. This fact—that a *relabelling of the names of some variables and identities of some constants is enough to turn one proof into the other*—means that we can save time and space by proving *just one* of these statements *without losing generality* in the strength of our argument. In these instances—when there is *symmetry* in our proofs that can be exploited—we now have the and experience to invoke the incantation *"without loss of generality"* to declare our intentions. Be sure to wield this spell with *great fear and trepidation.*

Case 2:
A contradiction follows *mutatis mutandis*.[1] ↯ Details are left to the reader.

Because we encountered contradictions in each case, we can therefore conclude that $(a, b) = (x, y)$, showing that g is injective. Since we have injections $f : \mathbb{N} \hookrightarrow \mathbb{N} \times \mathbb{N}$ and $g : \mathbb{N} \times \mathbb{N} \hookrightarrow \mathbb{N}$, we bask in the warm light of the *Cantor-Schröder-Bernstein theorem* and enjoy the existence of a bijection $h : \mathbb{N} \lhook\joinrel\twoheadrightarrow \mathbb{N} \times \mathbb{N}$. Therefore, $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$. Q.E.D.

***Corollary* 8.1.**
$|\mathbb{N}| = |\mathbb{Q}|$. 推論

8.2 *The Sound of Seven Trumpets*

The Bottomless Abyss

Definition* 8.1 *(Countable).

countable

We call X *countable* if $|X| \leqslant |\mathbb{N}|$, meaning *$X$ can be injected into $\mathbb{N}$*. 定義

***Lemma* 8.1.**
Every subset of $\mathbb{N}$ is countable. 引理

Definition* 8.2 *(Infinite).

infinite

Let X be a set and recall that we define X to be *finite* precisely when $(\exists n \in \mathbb{N})(|X| = n)$, which is to say that *$X$ can be put in bijection with the natural number $\{0, 1, \ldots n-1\}$*. We will say that X is *infinite* precisely when *no finite set can be bijected with X*, meaning $(\forall n \in \mathbb{N})(|X| \neq n)$. When a set is both *countable* and *infinite*, we call it *countably infinite*. 定義

Theorem* 8.5 *(Infinite Means Dedekind Infinite).
$\forall \mathcal{X}(\mathcal{X}$ is infinite $\Leftrightarrow (\exists \mathcal{Y} \subseteq \mathcal{X})(\mathcal{Y} \neq \mathcal{X} \wedge |\mathcal{Y}| = |\mathcal{X}|))$. 定理

***Theorem* 8.6.**
$\mathbb{N}$ is infinite. 定理

Proof. Suppose, towards a contradiction, that $\mathbb{N}$ is finite. This means $|\mathbb{N}| = |n|$ for some $n \in \mathbb{N}$, so we have a bijection $f : n \lhook\joinrel\twoheadrightarrow \mathbb{N}$. Define $S := \sum_{i=0}^{n-1} f(i)$ and observe the following inequalities hold for all $k \in n$.

$$f(k) \leqslant f(k) + \sum_{\substack{i \in n \\ i \neq k}} f(i) = \sum_{i=0}^{n-1} f(i) = S < S + 1$$

Because $(\forall i \in n)(f(i) \in \mathbb{N})$, we know that $S + 1 \in \mathbb{N}$, which implies $f(k) = S + 1$ for some $k \in n$ by the fact that f is surjective. However, $S + 1 = f(k) < S + 1$ by the above analysis. ↯ Thus, $\mathbb{N}$ is infinite. Q.E.D.

[1] *Mutatis mutandis* is another incantation that, when used with *flawless judgement and shrewd discernment*, can save the seasoned mathemagician massive amounts of time. It means *“with those things changed that should be changed,”* or *“once what must be modified has been modified.”*

Definition* 8.3 *(Infinite String).

infinite string

Given a set A, an *infinite string* over A is a function $f : \mathbb{N} \to A$. 定義

Theorem* 8.7 *(The Set of Natural Numbers is the Smallest Infinite Set).
If $\mathcal{A}$ is an infinite set, then $|\mathbb{N}| \leqslant |\mathcal{A}|$. 定理

Proof. Let $\mathcal{A}$ be an infinite set. We clearly have $\mathcal{A} \neq \varnothing$ because $|\mathcal{A}| \neq 0$, so there exists some $a_0 \in \mathcal{A}$. We will now *recursively* define an injective string $f_n : (n+1) \to \mathcal{A}$ of length $n+1$ for each $n \in \mathbb{N}$ below.

Base Case:
We let $f_0 : 1 \to \mathcal{A}$ be the string $f_0 :=$ "a_0" as the basis for recursion.

Recursive Case:
Let $k \in \mathbb{N}$ and suppose we have already defined $f_k =$ "$a_0 \dots a_k$". Note that $\{a_0, \dots, a_k\} \subseteq \mathcal{A}$ and that $\mathcal{A} \setminus \{a_0, \dots, a_k\} \neq \varnothing$ because otherwise $|\mathcal{A}| \leqslant |\{a_0, \dots, a_k\}| \leqslant k+1$, contradicting the fact that $\mathcal{A}$ is infinite. Therefore, there must be some $a_{k+1} \in \mathcal{A}$ such that $a_{k+1} \notin \{a_0, \dots, a_k\}$. We now define $f_{k+1} : (k+2) \to \mathcal{A}$ to be the string $f_{k+1} := f_k \mathbin{+\!\!\!+}$ "a_{k+1}".

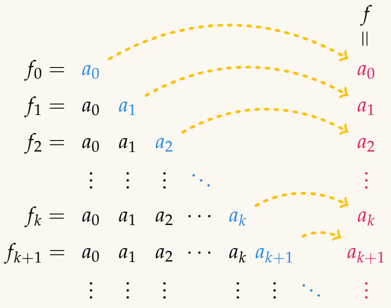

f
$\|$
$f_0 =$ a_0
$f_1 =$ a_0 a_1
$f_2 =$ a_0 a_1 a_2
$\vdots$ $\vdots$ $\vdots$ $\ddots$
$f_k =$ a_0 a_1 a_2 $\cdots$ a_k
$f_{k+1} =$ a_0 a_1 a_2 $\cdots$ a_k a_{k+1}
$\vdots$ $\vdots$ $\vdots$ $\vdots$ $\vdots$ $\ddots$
a_0
a_1
a_2
$\vdots$
a_k
a_{k+1}
$\vdots$

Figure 8.2: A visualization of the infinite sequence $\langle f_n \rangle$ and the infinite string f.

With this infinite sequence of strings in hand, we now define $f : \mathbb{N} \to \mathcal{A}$ by $f(n) := f_n(n)$ for each $n \in \mathbb{N}$. This is the infinite string whose n^{th} character is the last character of f_n. Let's show that f is injective.

Let $i, j \in \mathbb{N}$ and suppose $f(i) = f(j)$. This means $f_i(i) = a_i = a_j = f_j(j)$ by definition. Towards a contradiction, assume $i \neq j$ and without loss of generality let $i < j$. Notice then that $a_i \in \{a_0, \dots, a_{j-1}\}$, which means $a_j \in \{a_0, \dots, a_{j-1}\}$. However, we picked $a_j \in \mathcal{A}$ such that $a_j \notin \{a_0, \dots, a_{j-1}\}$ in the recursive case of our definition. ↯ Thus, $i = j$.

Therefore, since $f : \mathbb{N} \hookrightarrow \mathcal{A}$, we have $|\mathbb{N}| \leqslant |\mathcal{A}|$. Q.E.D.

Theorem* 8.8 *(Countable Unions of Countable Sets are Countable).
Consider a countable collection of countable sets $\mathcal{A} := \{A_i \mid i \in \mathbb{N}\}$, so $|\mathcal{A}| \leqslant |\mathbb{N}|$ and $(\forall i \in \mathbb{N})(|A_i| \leqslant |\mathbb{N}|)$. The union over $\mathcal{A}$ is countable.

$$\left| \bigcup_{i=0}^{\infty} A_i \right| = |\cup \mathcal{A}| \leqslant |\mathbb{N}|$$

定理

***Corollary* 8.2.**
If A is a finite set, then $\left| \left\{ f \mid (\exists k \in \mathbb{N})(f : k \to A) \right\} \right| = |\mathbb{N}|$. 推論

***Lemma* 8.2.**
If X is infinite and Y is a set where $|Y| < |X|$, then $|X \setminus Y| = |X|$. 引理

Scarlet Smoke

Definition* 8.4 *(Cardinal Numbers).

cardinal

The *cardinal numbers* are the *canonical representatives* for the different *"sizes"* sets can have (*cf.*, section 6.1). The *finite cardinals*—which represent the cardinalities of finite sets—are the *natural numbers*.[1] To represent the cardinalities of *infinite sets,* we introduce *infinite cardinals* called *aleph numbers*.[2] The first infinite cardinal $\aleph_0$ represents *countable infinity*, corresponding to the cardinality of the *smallest* infinite set $\aleph_0 = |\mathbb{N}|$. Inspired by our use of $\{0, 1, \ldots, n-1\}$—the set of the first n natural numbers—to represent the finite cardinality n, we define $\aleph_0 := \mathbb{N}$ and use *the set of all natural numbers* to denote the first infinite cardinality.

$\aleph_0$

定義

Definition* 8.5 *(Cardinal Arithmetic).

Let X and Y be sets with cardinalities $\kappa := |X|$ and $\mu := |Y|$ respectively. We *add* by taking the cardinality of the disjoint union of X with Y.

$$\kappa + \mu := \Big|\big(X \times \{0\}\big) \cup \big(Y \times \{1\}\big)\Big|$$

We *multiply* by taking the cardinality of the Cartesian product $X \times Y$.

$$\kappa \cdot \mu := |X \times Y|$$

We *exponentiate* by counting the functions mapping exponent to base.

$$\kappa^\mu := \Big|\{f \mid f : Y \to X\}\Big|$$

As it turns out, addition and multiplication are both associative and commutative, and multiplication distributes over addition. We also have the expected identities 0 and 1 for addition and multiplication respectively. With the order $\kappa \leqslant \mu \;:\Leftrightarrow\; \exists f (f : X \hookrightarrow Y)$ given to us by the *axiom of choice*, these form an ordered commutative monoid. 定義

***Lemma* 8.3.**

Given sets X and Y, if $\aleph_0 \leqslant |X|$ and $|Y| \leqslant |X|$, then $|X \cup Y| = |X|$.

引理

***Lemma* 8.4.**

Given sets X and Y, if $\aleph_0 \leqslant |X|$ and $|Y| \leqslant |X|$, then $|X \times Y| = |X|$.

引理

***Lemma* 8.5.**

If $\aleph_0 \leqslant |X|$ and $2 \leqslant |Y| \leqslant |X|$, then the following are equal.

$$\Big|\{f \mid f : X \to Y\}\Big| = \Big|\{f \mid f : X \to \{0,1\}\}\Big| = |\mathbb{P}(X)|$$

引理

[1] For example, $\big|\{\varnothing, \{\pi, 2/7\}, \mathbb{Z}\}\big| = 3$ because we can biject that set with $\{0, 1, 2\}$.

[2] The *aleph numbers* are denoted using the first letter of the Hebrew abjad ℵ, which is said *"aleph"* in English. The cardinal $\aleph_0$ is usually pronounced *"aleph naught"* or *"aleph null"* or even *"aleph sub zero."*

8.3 Apocalypse

Theorem* 8.9 *(Cantor's Diagonal Argument).
$\aleph_0 < \left|\{f \mid f : \mathbb{N} \to \{0,1\}\}\right|$. 定理

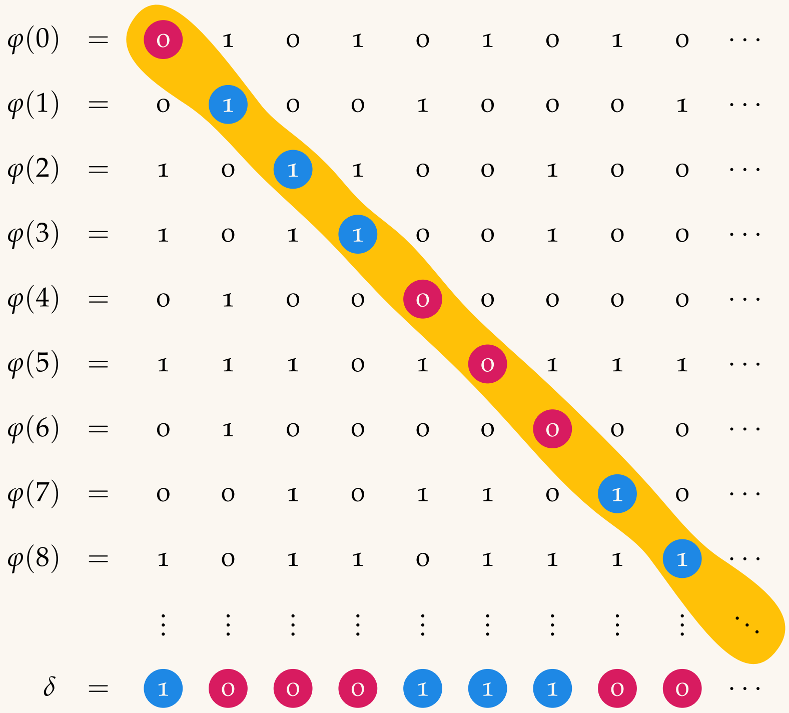
Proof. Let $\mathcal{B} := \{f \mid f : \mathbb{N} \to \{0,1\}\}$. Towards a contradiction, assume that $\aleph_0 \geqslant |\mathcal{B}|$, so that there exists a surjection $\varphi : \mathbb{N} \twoheadrightarrow \mathcal{B}$. Consider the string $\delta : \mathbb{N} \to \{0,1\}$ whose n^{th} digit is given below for each $n \in \mathbb{N}$.

$$\delta(n) := \begin{cases} 0 & \text{if } \varphi(n)(n) = 1 \\ 1 & \text{if } \varphi(n)(n) = 0 \end{cases}$$

Notice that $\delta \in \mathcal{B}$. Since φ is a surjection, we then know $\varphi(k) = \delta$ for some $k \in \mathbb{N}$. This implies $(\forall i \in n)(\varphi(k)(i) = \delta(i))$.[1] However, observe.

$$\begin{aligned} \delta(k) = 0 \;\Leftrightarrow\; \varphi(k)(k) = 1 \;\Leftrightarrow\; \varphi(k)(k) \neq 0 \\ \delta(k) = 1 \;\Leftrightarrow\; \varphi(k)(k) = 0 \;\Leftrightarrow\; \varphi(k)(k) \neq 1 \end{aligned}$$

This shows $(\exists i \in n)(\varphi(k)(i) \neq \delta(i))$. ϟ Therefore, $\aleph_0 < |\mathcal{B}|$. Q.E.D.



$$\begin{array}{rcccccccccccc}
\varphi(0) & = & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & \cdots \\
\varphi(1) & = & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & \cdots \\
\varphi(2) & = & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & \cdots \\
\varphi(3) & = & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & \cdots \\
\varphi(4) & = & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots \\
\varphi(5) & = & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & \cdots \\
\varphi(6) & = & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots \\
\varphi(7) & = & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & \cdots \\
\varphi(8) & = & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & \cdots \\
 & & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \\
\delta & = & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & \cdots
\end{array}$$

Figure 8.3: An example $\varphi : \mathbb{N} \to \mathcal{B}$ of a function mapping each natural number to an infinite-length binary string. The n^{th} string $\varphi(n)$ is visualized as the n^{th} row of an infinite matrix. The string δ shown below the matrix is constructed so that its characters *disagree* with the corresponding characters that lie along the *diagonal* of the matrix. If the n^{th} character in the n^{th} string is *zero*, then $\delta(n)$ is defined to be *one*. Conversely, if that character is a *one*, then $\delta(n)$ is set to *zero*.

***Corollary* 8.3.**
Let $\mathcal{A}$ be a set with $|\mathcal{A}| \geqslant 2$. Then, $\left|\{f \mid f : \mathbb{N} \to \mathcal{A}\}\right| > \aleph_0$. Further, if $|\mathcal{A}| \geqslant \aleph_0$, there are uncountably many infinite strings over $\mathcal{A}$. 推論

[1] As a reminder: if $f : X \to Y$ is a function, then $f(x) = y \;:\Leftrightarrow\; (x,y) \in f$. If we have another function $g : X \to Y$ with the same domain and codomain, then $f = g$ means the two *sets* have the same elements by the *axiom of extensionality*, so f and g contain the same ordered pairs $(\forall x \in X)(\forall y \in Y)((x,y) \in f \Leftrightarrow (x,y) \in g)$. This means precisely that f and g have the same output on every given input. $(\forall x \in X)(f(x) = g(x))$.

The Four Horsemen

Theorem* 8.10 *(Cantor's Theorem).
$\forall \mathcal{X}\Big(|\mathcal{X}| < \big|\mathbb{P}(\mathcal{X})\big|\Big)$. 定理

Proof. Let $\mathcal{X}$ be a set and suppose that $|\mathcal{X}| \geqslant |\mathbb{P}(\mathcal{X})|$ towards a contradiction. We then know there exists a surjection $f : \mathcal{X} \twoheadrightarrow \mathbb{P}(\mathcal{X})$. Consider the set $\Delta := \{x \in \mathcal{X} \mid x \notin f(x)\}$. We know Δ exists by the *axiom of separation*, and we can clearly see that $\Delta \subseteq \mathcal{X}$, so $\Delta \in \mathbb{P}(\mathcal{X})$. Thus, since f is surjective, we know there exists $\delta \in \mathcal{X}$ such that $f(\delta) = \Delta$. We can now ask the simple question: is $\delta \in \Delta$ or is $\delta \notin \Delta$?

> *Case 1:*
> If $\delta \in \Delta$, then $\delta \notin f(\delta)$ by definition. However, $f(\delta) = \Delta$. Thus, $\delta \notin \Delta$. ↯
>
> *Case 2:*
> If $\delta \notin \Delta$, then we know $\neg(\delta \notin f(\delta))$ by definition, so that $\delta \in f(\delta)$. Recalling that $f(\delta) = \Delta$, this tells us $\delta \in \Delta$. ↯

In either case, we have forced a contradiction. Therefore, $|\mathcal{X}| < \big|\mathbb{P}(\mathcal{X})\big|$.

Q.E.D.

Theorem* 8.11 *(Cantor's Theorem – Taylor's Version).
$\forall \mathcal{X}\Big(\big|\mathbb{P}(\mathcal{X})\big| > |\mathcal{X}|\Big)$. 定理

Theorem* 8.12 *(Cantor's Theorem – Johnstone's Version).
If $\mathcal{X}$ is a set, then $\mathbb{P}(\mathcal{X}) \neq \mathcal{X}/R$ for any equivalence relation R. 定理

Theorem* 8.13 *(Cantor's Theorem – Lawvere's Version).
Let S and V be sets such that a surjection $\varphi : S \twoheadrightarrow \{f \mid f : S \to V\}$ exists. Then, every function $\psi : V \to V$ has a *fixed point*, which means $(\exists v \in V)(\psi(v) = v)$. 定理

9

Modern Number Theory

> *"I don't know why we are here, but I'm pretty sure that it is not in order to enjoy ourselves."*
>
> – Ludwig Wittgenstein

9.1 A Different Point of View

Definition* 9.1 *(Modular Congruence).

$a \equiv b \pmod n$ Let $n \in \mathbb{N}_+$. Given two integers $a, b \in \mathbb{Z}$, we write $a \equiv b \pmod n$ to mean that *a is congruent to b modulo n* as defined formally below.

$$a \equiv b \pmod n \quad :\Leftrightarrow \quad n \mid a - b$$

In this expression, n is referred to as the *modulus* since this is the number according to which we are measuring the *residues* a and b. 定義

***Lemma* 9.1.**

Consider a modulus $n \in \mathbb{N}_+$ and take two arbitrary residues $x, y \in \mathbb{Z}$ such that $x \equiv y \pmod n$. Then, for any $k \in \mathbb{Z}$, we know the following.

$$\begin{aligned} x + k &\equiv y + k \pmod n \\ k \cdot x &\equiv k \cdot y \pmod n \end{aligned}$$

This means that adding and multiplying by an integer on both sides of a given congruence *maintains congruence* modulo n. 引理

***Corollary* 9.1.**

For any modulus $n \in \mathbb{N}_+$ and $x \in \mathbb{Z}$, we have $x \equiv x + n \pmod n$. 推論

Given a modulus $n \in \mathbb{N}_+$, congruence modulo n defines a *relation* on $\mathbb{Z}$, which we will denote $n\mathbb{Z} := \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x \equiv y \pmod n\}$.[2] As it happens, this happens to be a very *nice* kind of relation. First of all, every integer $x \in \mathbb{Z}$ is related to itself, so this relation is *reflexive*.

$$(n \cdot 0 = 0) \Rightarrow (n \mid 0) \Rightarrow (n \mid x - x) \Rightarrow x \equiv x \pmod n$$

[2] This is not the conventional way this notation is used; $n\mathbb{Z}$ is typically used in algebra to refer to something called a *"coset"* of the group $\mathbb{Z}$. Instead, we are using $n\mathbb{Z}$ to refer to a *relation*. Although this is technically abusing notation, there *is* a fundamental correspondence between these two concepts, and our use of the notation is *in the same spirit* given the definition we are about to introduce.

Further, $(y, x) \in n\mathbb{Z}$ whenever $(x, y) \in n\mathbb{Z}$, so this relation is *symmetric*.

$$\begin{aligned}
x \equiv y \pmod{n} &\Rightarrow n \mid x - y \\
&\Rightarrow (\exists k \in \mathbb{Z})(nk = x - y) \\
&\Rightarrow (\exists k \in \mathbb{Z})(n(-k) = y - x) \\
&\Rightarrow n \mid y - x \\
&\Rightarrow y \equiv x \pmod{n}
\end{aligned}$$

Finally, every time we have two legs $(x, y) \in n\mathbb{Z}$ and $(y, z) \in n\mathbb{Z}$ of a triangle, we can always close the triangle with $(x, z) \in n\mathbb{Z}$.

$$\begin{aligned}
x \equiv y \pmod{n} &\Rightarrow n \mid x - y \\
&\Rightarrow nk_1 = x - y \text{ for some } k_1 \in \mathbb{Z} \\
y \equiv z \pmod{n} &\Rightarrow n \mid y - z \\
&\Rightarrow nk_2 = y - z \text{ for some } k_2 \in \mathbb{Z} \\
(nk_1 = x - y) \wedge (nk_2 = x - y) &\Rightarrow nk_1 - nk_2 = (x - y) - (y - z) \\
&\Rightarrow n(k_1 - k_2) = x - z \\
&\Rightarrow n \mid x - z \\
&\Rightarrow x \equiv z \pmod{n}
\end{aligned}$$

Therefore, $n\mathbb{Z}$ is an *equivalence relation*, so we can define *equivalence classes* under this relation. Because these classes relate specifically to the *"congruence modulo n"* relation, we sometimes call them *residue classes* and define them as follows for each integer $x \in \mathbb{Z}$ below.

$[x]_n$

$$[x]_n := \{ y \in \mathbb{Z} \mid (x, y) \in n\mathbb{Z} \} = \{ y \in \mathbb{Z} \mid x \equiv y \pmod{n} \}$$

These classes *partition* $\mathbb{Z}$ into a collection of nonempty, disjoint subsets whose union covers all of the integers. The fact that $x \equiv x + n \pmod{n}$ for every $x \in \mathbb{Z}$ tells us that there are *exactly* n such equivalence classes.

$\mathbb{Z}/n\mathbb{Z}$

$$\mathbb{Z}/n\mathbb{Z} := \left\{ [x]_n \;\middle|\; x \in \mathbb{Z} \right\} = \left\{ [0]_n, [1]_n, \ldots, [n-1]_n \right\}$$

Each of the possible remainders $r \in \{0, 1, \ldots n - 1\}$ after division by n produces an equivalence class $[r]_n$ that contains *all* of the integers whose remainder is r after dividing them by n.

***Theorem* 9.1.**
Let $n \in \mathbb{N}_+$ be a modulus and consider a remainder $r \in \{0, 1, \ldots, n - 1\}$. Then, for any $x \in \mathbb{Z}$, we have $(\exists q \in \mathbb{Z})(x = qn + r) \iff x \in [r]_n$. 定理

***Corollary* 9.2.**
For any $n \in \mathbb{N}_+$, we have $|\mathbb{Z}/n\mathbb{Z}| = n$. 推論

9.2 *The Algebraic Perspective*

We can now notice something interesting. Take two integers $x, y \in \mathbb{Z}$ with remainders $r_x, r_y \in \{0, 1, \ldots, n-1\}$ respectively, so that $x \in [r_x]_n$ and $y \in [r_y]_n$. This implies that $x \equiv r_x \pmod{n}$ and $y \equiv r_y \pmod{n}$, showing us $x + y \equiv r_1 + r_2 \pmod{n}$. But then $x + y \in [r_x + r_y]_n$ tells us that the sum $x + y$ has remainder equal to the sum of the remainders of x and y individually. It's easy to verify that $xy \in [r_x r_y]_n$ also holds. So, we can use the algebra of $\mathbb{Z}$ to *induce* an *algebraic structure* on $\mathbb{Z}/n\mathbb{Z}$.

Definition* 9.2 *(Modular Arithmetic).
Let $n \in \mathbb{N}_+$ and let $[x]_n$ and $[y]_n$ be two arbitrary residue classes in $\mathbb{Z}/n\mathbb{Z}$. We define *modular addition* between $[x]_n$ and $[y]_n$ as follows.

$$[x]_n + [y]_n \coloneqq [x + y]_n$$

We define *modular multiplication* between $[x]_n$ and $[y]_n$ as follows.

$$[x]_n \cdot [y]_n \coloneqq [x \cdot y]_n$$

The fact that $\mathbb{Z}/n\mathbb{Z}$ partitions $\mathbb{Z}$ assures us these operations are functions from $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}) \to \mathbb{Z}/n\mathbb{Z}$ and that they are well-defined. 定義

***Lemma* 9.2.**
Let $n \in \mathbb{N}_+$ be a modulus and consider any three residues $x, y, z \in \mathbb{Z}$.

$$\begin{aligned} x + y \equiv z \pmod{n} \quad &\Leftrightarrow \quad [x]_n + [y]_n = [z]_n \\ x \cdot y \equiv z \pmod{n} \quad &\Leftrightarrow \quad [x]_n \cdot [y]_n = [z]_n \\ x \equiv y \pmod{n} \quad &\Leftrightarrow \quad [x]_n = [y]_n \end{aligned}$$

This shows *congruences* over $\mathbb{Z}$ are equivalent to *equations* over $\mathbb{Z}/n\mathbb{Z}$. 引理

We have already encountered an example of a commutative ring—namely, the set of integers $\mathbb{Z}$ with the usual addition and multiplication. $\mathbb{Z}/n\mathbb{Z}$, however, is the first *finite* algebraic structure we've come across. Does it behave like the *infinite* structure $\mathbb{Z}$ its operations derived from?

Addition on $\mathbb{Z}/n\mathbb{Z}$ is *associative*, *commutative*, and there is an *identity* element $[0]_n$ satisfying $[x]_n + [0]_n = [x]_n$ for every $[x]_n \in \mathbb{Z}/n\mathbb{Z}$. The same three properties hold true about *multiplication*, with the identity element being $[1]_n$ satisfying $[x]_n[1]_n = [x]_n$ for all $[x]_n \in \mathbb{Z}/n\mathbb{Z}$. Further, multiplication *distributes* over addition just as it does for numbers. So far, this means $\mathbb{Z}/n\mathbb{Z}$ has the all of the algebraic properties $\mathbb{N}$ does.

We can now ask: does $\mathbb{Z}/n\mathbb{Z}$ contain *additive inverses* for all of its elements? More precisely, is the following statement *true?*

$$\Big(\forall [x]_n \in \mathbb{Z}/n\mathbb{Z}\Big)\Big(\exists [y]_n \in \mathbb{Z}/n\mathbb{Z}\Big)\Big([x]_n + [y]_n = [0]_n\Big)$$

The answer here is clearly *yes!* Given $[x]_n \in \mathbb{Z}/n\mathbb{Z}$, simply observe that $[x]_n + [-x]_n = [x - x]_n = [0]_n$. With this observation, we now see $\mathbb{Z}/n\mathbb{Z}$ has inherited all of the algebraic properties of $\mathbb{Z}$. This also tells us that we can always *solve* congruences of the following form for $x \in \mathbb{Z}$.

$$x + \alpha \equiv \beta \pmod{n}$$

Narrow Field of View

However, there is one more distinctive thing about $\mathbb{Z}$ that distinguishes it from $\mathbb{Q}$ and $\mathbb{R}$: the only non-zero integer with a *multiplicative inverse* is 1, the multiplicative identity. Is the same true about $\mathbb{Z}/n\mathbb{Z}$? More precisely, for any given $[x]_n \in \mathbb{Z}/n\mathbb{Z}$, when is the statement below *true?*

$$\Big(\exists [y]_n \in \mathbb{Z}/n\mathbb{Z}\Big)\Big([x]_n \cdot [y]_n = [1]_n\Big)$$

An equivalent way to formulate this question is: for what values $x \in \mathbb{Z}$ does the following congruence have at least one integer solution $y \in \mathbb{Z}$?

$$xy \equiv 1 \pmod{n}$$

To answer this question, let's fix $x \in \mathbb{Z}$ and observe the following.

$$\begin{aligned}
(\exists y \in \mathbb{Z})\big(xy \equiv 1 \pmod{n}\big) &\Leftrightarrow (\exists y \in \mathbb{Z})\big(n \mid xy - 1\big) \\
&\Leftrightarrow (\exists y_1 \in \mathbb{Z})(\exists y_2 \in \mathbb{Z})\big(ny_2 = xy_1 - 1\big) \\
&\Leftrightarrow (\exists y_1 \in \mathbb{Z})(\exists y_2 \in \mathbb{Z})\big(ny_2 = 1 - xy_1\big) \\
&\Leftrightarrow (\exists y_1 \in \mathbb{Z})(\exists y_2 \in \mathbb{Z})\big(xy_1 + ny_2 = 1\big) \\
&\Leftrightarrow \gcd(x, n) = 1
\end{aligned}$$

Figure 9.1: Διόφαντος ὁ Ἀλεξανδρεύς

The last equivalence above follows from *Bézout's identity*—which states that the greatest common divisor of x and n can always be expressed as an integer linear combination of x and n—and the fact that the greatest common divisor divides any linear combination of x and n.[1] We summarize this result with the following theorem.

***Theorem* 9.2.**
For any $n \in \mathbb{N}_+$ and $[x]_n \in \mathbb{Z}/n\mathbb{Z}$, the following equivalence holds.

$$\Big(\exists [y]_n \in \mathbb{Z}/n\mathbb{Z}\Big)\Big([x]_n \cdot [y]_n = [1]_n\Big) \Leftrightarrow \gcd(x, n) = 1$$

As a consequence, the congruence $xy \equiv 1 \pmod{n}$ has a solution $y \in \mathbb{Z}$ if and only if x and n are relatively prime. 定理

Even more interestingly, the multiplicative inverse for x that we've been looking for will precisely be given by *its coefficient* in the linear combination, highlighted in *red* above. We can effectively *compute* these coefficients with a modified version of the Euclidean division algorithm.

[1] As a reminder: if $a, b \in \mathbb{Z}$, then Bézout tells us that there exist $x, y \in \mathbb{Z}$ such that $\gcd(a, b) = ax + by$.

Algorithm 9.1 (Extended Euclidean Division).
Given $a, b \in \mathbb{Z}$, we compute $\gcd(a, b)$ at the same time that we find coefficients $s, t \in \mathbb{Z}$ for which $as + bt = \gcd(a, b)$ guaranteed by Bézout.

$$\texttt{egcd}(a,b) := \begin{cases} (a,1,0) & \text{if } b = 0 \\ (d,t,s-qt) & \text{if } b \neq 0 \text{, where } \begin{cases} (d,s,t) = \texttt{egcd}(b,r) \\ a = qb + r \\ 0 \leqslant r < |b| \\ q, r \in \mathbb{Z} \end{cases} \end{cases}$$

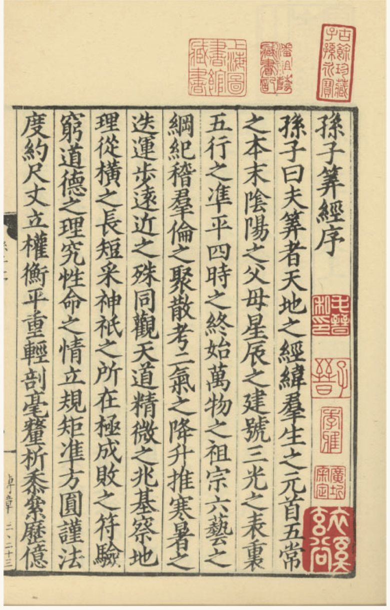
This recursive algorithm returns an ordered triple $\texttt{egcd}(a,b) = (d,s,t)$. The first coordinate is the greatest common divisor $d = \gcd(a,b)$. The second and third coordinates satisfy $as + bt = \gcd(a,b)$. 演算法

The terms a, b, and s/t in the extended Euclidean division algorithm are color-coded to match the previous derivation of the fact that $xy \equiv 1 \pmod{n}$ is equivalent to $\gcd(a,b) = 1$.

With this knowledge in hand, we now know precisely *when* congruences of the following form are solvable over the integers.

$$\alpha x + \beta \equiv \gamma \pmod{n}$$

These kinds of congruences are actually *linear Diophantine equations* in disguise: equations of the form $ax + by = c$ with $a, b, c, x, y \in \mathbb{Z}$. Extending our analysis, we have known when and how to find solutions to *systems* of *special kinds* of linear Diophantine equations since 400 AD. This astounding, ancient result is called the *Chinese remainder theorem*.



孫子筭經序

孫子曰夫筭者天地之經緯羣生之元首五常之本末陰陽之父母星辰之建號三光之表裏五行之準平四時之終始萬物之祖宗六藝之綱紀稽羣倫之聚散考二氣之降升推寒暑之迭運步遠近之殊同觀天道精微之兆基察地理從橫之長短采神祇之所在極成敗之符驗窮道德之理究性命之情立規矩準方圓謹法度約尺丈立權衡平重輕剖毫釐析黍絫歷億

Figure 9.2: The mathematician 孙子, whose identity is lost to time, first wrote down this theorem in the 孙子算经, one of the *Ten Computational Canons* of the Tang dynasty, between 200 and 400 AD.

Theorem 9.3 (Chinese Remainder Theorem).
Let $k \in \mathbb{N}_+$ and consider k moduli $n_0, n_1, \ldots, n_{k-1} \in \mathbb{N}_+$ such that $\gcd(n_i, n_j) = 1$ whenever $i \neq j$ for all $i, j \in k$. Then, for any choice of residues $a_0, a_1, \ldots, a_{k-1} \in \mathbb{Z}$, there exists a solution $x \in \mathbb{Z}$ to the following system of modular congruences.

$$\begin{aligned} x &\equiv a_0 \pmod{n_0} \\ x &\equiv a_1 \pmod{n_1} \\ &\vdots \\ x &\equiv a_{k-1} \pmod{n_{k-1}} \end{aligned}$$

Further, any other solution y is congruent to x modulo $\prod_{i=0}^{k-1} n_i$. 定理

Proof. We will prove the *existence* of a solution to the system of linear congruences. We leave proving *uniqueness* of the solution to the reader.

Let $k \in \mathbb{N}_+$ and consider moduli $n_0, n_1, \ldots, n_{k-1} \in \mathbb{N}_+$ that are pairwise relatively prime, which means $(\forall i, j \in k)(i \neq j \Rightarrow \gcd(n_i, n_j) = 1)$. Recall this implies each n_j is multiplicatively invertible modulo n_i whenever $i \neq j$. For each $j \neq i$, define $\overline{n_{j,i}}$ to be the *unique* multiplicative inverse of n_j modulo n_i in the range $\{0, 1, \ldots n_i - 1\}$, and let $\overline{n_{i,i}} := 0$.[1]

[1] To the concerned reader: despite there being many choices for *"the"* multiplicative inverse, this is well-defined. Since there must be an inverse for n_j, we can find z in the range $0 \leqslant z < n_i$ such that $z \equiv n_j \pmod{n_i}$ and verify that the rest of the proof will hold for that z.

Now, let $a_0, a_1, \ldots, a_{k-1} \in \mathbb{Z}$ and define the following the integer.

$$x := \sum_{i=0}^{k-1} a_i \prod_{j=0}^{k-1} n_j \overline{n_{j,i}}$$

We obtain x by taking each target residue a_i and multiplying it by *all of the moduli* in the system of congruences *except for its own modulus.* The idea is that, for each ℓ, this will force all of the terms in the sum except a_ℓ to be divisible by n_ℓ—and thus congruent to 0 modulo n_ℓ—yielding $x \equiv a_\ell \pmod{n_\ell}$. We demonstrate this below. Let $\ell \in \{0, 1, \ldots, k-1\}$.[1]

$$\begin{aligned}
x &\equiv \sum_{i=0}^{k-1} a_i \prod_{j=0}^{k-1} n_j \overline{n_{j,i}} && \pmod{n_\ell} \\
&\equiv \sum_{i=0}^{k-1} a_i \prod_{\substack{j=0\\ j\neq i}}^{k-1} n_j \overline{n_{j,i}} && \pmod{n_\ell} \\
&\equiv a_\ell \prod_{\substack{j=0\\ j\neq \ell}}^{k-1} n_j \overline{n_{j,\ell}} + \sum_{\substack{i=0\\ i\neq \ell}}^{k-1} a_i \prod_{\substack{j=0\\ j\neq i}}^{k-1} n_j \overline{n_{j,i}} && \pmod{n_\ell} \\
&\equiv a_\ell \prod_{\substack{j=0\\ j\neq \ell}}^{k-1} n_j \overline{n_{j,\ell}} + \sum_{\substack{i=0\\ i\neq \ell}}^{k-1} a_i a_\ell n_\ell \overline{n_{\ell,i}} \prod_{\substack{j=0\\ j\neq i\\ j\neq \ell}}^{k-1} a_i n_j \overline{n_{j,i}} && \pmod{n_\ell} && \text{commuting out the } a_\ell n_\ell \overline{n_{\ell,i}} \text{ factors} \\
&\equiv a_\ell \prod_{\substack{j=0\\ j\neq \ell}}^{k-1} n_j \overline{n_{j,\ell}} + n_\ell \sum_{\substack{i=0\\ i\neq \ell}}^{k-1} a_i a_\ell \overline{n_{\ell,i}} \prod_{\substack{j=0\\ j\neq i\\ j\neq \ell}}^{k-1} a_i n_j \overline{n_{j,i}} && \pmod{n_\ell} && \text{factoring out } n_\ell \text{ from each term} \\
&\equiv a_\ell \prod_{\substack{j=0\\ j\neq \ell}}^{k-1} n_j \overline{n_{j,\ell}} + 0 \sum_{\substack{i=0\\ i\neq \ell}}^{k-1} a_i a_\ell \overline{n_{\ell,i}} \prod_{\substack{j=0\\ j\neq \ell}}^{k-1} a_i n_j \overline{n_{j,i}} && \pmod{n_\ell} && \text{because } n_\ell \equiv 0 \pmod{n_\ell} \\
&\equiv a_\ell \prod_{\substack{j=0\\ j\neq i\\ j\neq \ell}}^{k-1} n_j \overline{n_{j,\ell}} + 0 && \pmod{n_\ell} && \text{since } 0z \equiv 0 \pmod{n_\ell} \text{ for every } z \in \mathbb{Z} \\
&\equiv a_\ell \prod_{\substack{j=0\\ j\neq i\\ j\neq \ell}}^{k-1} n_j \overline{n_{j,\ell}} && \pmod{n_\ell} && \text{since } z + 0 \equiv z \pmod{n_\ell} \text{ for every } z \in \mathbb{Z} \\
&\equiv a_\ell \prod_{\substack{j=0\\ j\neq i\\ j\neq \ell}}^{k-1} 1 && \pmod{n_\ell} && \text{since } n_j \cdot \overline{n_{j,\ell}} \equiv 1 \pmod{n_\ell} \text{ by definition} \\
&\equiv a_\ell && \pmod{n_\ell} && \text{since } 1z \equiv z \pmod{n_\ell} \text{ for every } z \in \mathbb{Z}
\end{aligned}$$

Since ℓ was arbitrary, x solves the system of congruences. Q.E.D.

[1] *A note to the student:* this is an example of a situation that sometimes occurs in mathematics where a simple idea turns into a syntactically monstrous proof because of the need to keep track of a lot of small details. Paradoxically, we can obtain an *elegant* and much more *intuitive* proof of the *Chinese remainder theorem* by *generalizing* the statement to a much broader, more abstract class of objects (namely, *groups*) rather than focussing on elements of $\mathbb{Z}$ specifically.

Peripheral Vision

As we saw, solving congruences modulo n often involves finding an inverse for an element in $\mathbb{Z}/n\mathbb{Z}$. Although the *extended Euclidean division algorithm* gives us an efficient way of computing these inverses when they exist, it's far too inconvenient for a human working by-hand.

Theorem* 9.4 *(Férmat's Little Theorem).
Let p be prime. The following congruence is then *true* for any $a \in \mathbb{Z}$.

$$a^p \equiv a \pmod{p}$$

Further, for any $a \in \mathbb{Z}$ such that $\gcd(a, p) = 1$, the following is *true.*

$$a^{p-1} \equiv 1 \pmod{p}$$

This is equivalent to saying $[a]_p^{p-1} = [1]_p$ for every $[a]_p \neq [0]_p$. 定理

Figure 9.3: Leonhard Euler is the namesake for the totient function φ_e, among a litany of other mathematical concepts, definitions, theorems, and constructions.

We define the *totient* of $n \in \mathbb{N}$ as the amount of naturals below n that are coprime with n. Formally, $\varphi_e(n) := \big|\{x \in \mathbb{N}_+ \mid x \leqslant n \wedge \gcd(x, n) = 1\}\big|$, where $\varphi_e : \mathbb{N} \to \mathbb{N}$, known as *Euler's totient function.* We now see an important connection between *Fermat's little theorem* and Euler's totient.

***Lemma* 9.3.**
If p is a prime number, then $\varphi_e(p) = p - 1$. 引理

As it turns out, this is exactly counts the elements of $\mathbb{Z}/n\mathbb{Z}$ that are *multiplicatively invertible.* Since $\varphi_e(p) = p - 1$ when p is prime, this gives us some insight into *Fermat's little theorem:* when $a \not\equiv 0 \pmod{p}$, then multiplying a by itself for as many times as there are multiplicatively invertible elements in $\mathbb{Z}/n\mathbb{Z}$ produces a number congruent to 1 modulo p. In other words, we know $a^{\varphi_e(p)} \equiv 1 \pmod{p}$ when $\gcd(a, p) = 1$. Does this remarkable observation generalize? *Yes, it does!*

Theorem* 9.5 *(Euler's Theorem).
For any $n \in \mathbb{N}_+$ and $a \in \mathbb{Z}$ such that $\gcd(a, n) = 1$, the following is *true.*

$$a^{\varphi_e(n)} \equiv 1 \pmod{n}$$

This is equivalent to saying $[a]_n^{\varphi_e(n)} = [1]_n$ whenever $[a]_n$ is invertible. 定理

Euler's totient function has a few interesting and beautiful properties, but none is more important than the fact that it *splits multiplicatively* over the prime power divisors of its input.

***Theorem* 9.6.**
If $a, b \in \mathbb{N}_+$ such that $\gcd(a, b) = 1$, then $\varphi_e(ab) = \varphi_e(a)\varphi_e(b)$. 定理

There is a deeper truth underlying this theorem. When a and b are coprime, then $\mathbb{Z}/ab\mathbb{Z}$ has the *same algebraic structure*[1] as $(\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z})$ if we extend the definitions of modular addition and multiplication to ordered pairs by adding or multiplying their respective coordinates.[2] In spirit, this says that moving around on the integer number line from the perspective of ab is equivalent to moving around on a 2-dimensional integer grid, where one of the axes behaves like $\mathbb{Z}/a\mathbb{Z}$ and the other behaves like $\mathbb{Z}/b\mathbb{Z}$. This idea can be used to further generalize the *Chinese remainder theorem* to $\mathbb{Z}/n\mathbb{Z}$, and to *groups* even more generally.

9.3 *Asymmetric Cryptography*

The RSA cryptosystem is an algorithm for performing *asymmetric encryption*, also known as *public key encryption*. Its security is reliant on two key observations related to factoring $n \in \mathbb{N}$ into a product of primes.

1. The fastest known algorithm for factoring n is $\mathcal{O}(e^{\sqrt[3]{64/9}(\ln n)^{1/3}(\ln \ln n)^{2/3}})$.
2. The fastest known way to find the k^{th} root of $[x]_n$ is by factoring n.

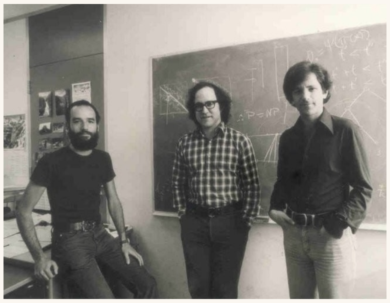


Figure 9.4: RSA cryptography gets its name from Rivest, Shamir, and Adleman, the coauthors of the original 1977 paper.

Suppose that Gaius Julius Caesar, currently on campaign in Transalpine Gaul, wants to securely receive messages from his general Marcus Antonius in Rome about the brewing civil war. The algorithm works in two stages, involving ***private data*** that must ***remain secret*** or be ***destroyed*** and ***public data*** that can be shared through ***insecure channels*** without compromising the security of the system.

```
def is_prime(x):
  for n in range(2, int(sqrt(x) + 1)):
    if x % n == 0:
      return False
  return True
```

Figure 9.5: A simple Python function for recursively deciding whether an integer x is prime in $\mathcal{O}(\sqrt{x})$ time and $\mathcal{O}(1)$ space.

Key Generation

1. Caesar picks two large prime numbers $\boldsymbol{p}$ and $\boldsymbol{q}$.
2. He then defines $\boldsymbol{n} := \boldsymbol{pq}$.
3. He now computes $\boldsymbol{\varphi_e(n)} = (\boldsymbol{p}-1)(\boldsymbol{q}-1)$.
   (a) $\varphi_e(n) = \varphi_e(pq) = \varphi_e(p)\varphi_e(q) = (p-1)(q-1)$ by *theorem* 9.6.
4. He then picks $\boldsymbol{d}$ such that $1 < \boldsymbol{d} < \boldsymbol{\varphi_e(n)}$ and $\gcd(\boldsymbol{d}, \boldsymbol{\varphi_e(n)}) = 1$.
   (a) Caesar verifies $\gcd(d, \varphi_e(n)) = 1$ with the *extended Euclidean algorithm*, simultaneously obtaining $\boldsymbol{e}$ such that $\boldsymbol{ed} \equiv 1 \pmod{\boldsymbol{\varphi_e(n)}}$.

$\boldsymbol{n}$ is the ***public modulus***.

$\boldsymbol{\varphi_e(n)}$ is the ***private modulus***.

$\boldsymbol{d}$ is the ***private decryption key***.

$\boldsymbol{e}$ is the ***public encryption key***.

[1] When two sets $\mathcal{G}$ and $\mathcal{H}$ have the same *algebraic structure*, we say that they are *isomorphic* and use the notation $\mathcal{G} \cong \mathcal{H}$.

[2] Given sets $\mathcal{G}$ and $\mathcal{H}$ with operations $\star_{\mathcal{G}}$ and $\star_{\mathcal{H}}$ respectively, we can *induce* an algebraic structure on $\mathcal{G} \times \mathcal{H}$ by defining $(g_1, h_1) \star (g_2, h_2) := (g_1 \star_{\mathcal{G}} g_2, h_1 \star_{\mathcal{H}} h_2)$.

```python
def mult_inv(e, phi, s=None, t=None):
    s = [1, 0] if s is None else s
    t = [0, 1] if t is None else t

    e, phi = (min(e, phi), max(e, phi))

    q = 1
    while phi >= e * q:
        q += 1
    q -= 1
    r = phi - e*q

    if r == 0:
        return t[1]
    else:
        s = [s[1], s[0] - q*s[1]]
        t = [t[1], t[0] - q*t[1]]
        return mult_inv(r, e, s=s, t=t)
```

Figure 9.6: A recursive `Python` implementation of finding the multiplicative inverse of an integer `e` modulo `phi` using the *extended Euclidean division algorithm.*

Julius Caesar now has a ***public key*** (e, n) and a ***private key*** (d, n). He transmits (e, n) to Marcus Antonius in Rome in plain text via messenger, keeping (d, n) securely hidden. The secrets p, q, and $\varphi_e(n)$ are all *immediately destroyed* to minimize his vulnerability to attack.

Encryption

1. Having received (e, n), Marcus prepares a message m—a binary string—and chunks it into substrings $m = m_0 \mathbin{+\!\!+} m_1 \mathbin{+\!\!+} \cdots \mathbin{+\!\!+} m_{k-1}$ such that $(\forall i \in k)(0 < m_i < n \wedge \gcd(m_i, n) = 1)$.[1]
2. Marcus encrypts each chunk m_i by computing $c_i := {m_i}^e - \lfloor {m_i}^e / n \rfloor n$.
   (a) This guarantees that $c_i \equiv {m_i}^e \pmod{n}$ and $0 < c_i < n$.
3. Marcus now sends the cypher $c := c_0 \mathbin{+\!\!+} c_1 \mathbin{+\!\!+} \cdots \mathbin{+\!\!+} c_{k-1}$ to Caesar.

```python
def mod_exp(a, b, n, exp=1):
    if b <= 0:
        return exp
    else:
        return mod_exp(a, b - 1, n, exp=(exp*a % n))
```

Figure 9.7: An efficient `Python` algorithm for recursively computing $\texttt{a}^{\texttt{b}}$ modulo `n` in $\mathcal{O}(b)$ time and $\mathcal{O}(1)$ space.

[1] If these conditions are not ensured, then information will be lost during the encryption and decryption processes.

Decryption

1. Caesar receives the encrypted message $c = c_0 \mathbin{+\!\!+} c_1 \mathbin{+\!\!+} \cdots \mathbin{+\!\!+} c_{k-1}$.
2. He now decrypts each chunk c_i by computing $\mu_i := {c_i}^d - \lfloor {c_i}^d / n \rfloor n$.
   (a) This guarantees that $\mu_i \equiv {c_i}^d \pmod{n}$ and $0 < \mu_i < n$.
3. The fully decrypted message is then $\mu := \mu_0 \mathbin{+\!\!+} \mu_1 \mathbin{+\!\!+} \cdots \mathbin{+\!\!+} \mu_{k-1}$.

The decrypted chunks μ_i each have the following remarkable property.

$$\mu_i \equiv m_i \pmod{n}$$

This fact, along with the constraint $0 < \mu_i < n$ enforced for each chunk, confirms that $\mu = \mu_0 \mathbin{+\!\!+} \mu_1 \mathbin{+\!\!+} \cdots \mathbin{+\!\!+} \mu_{k-1} = m_0 \mathbin{+\!\!+} m_1 \mathbin{+\!\!+} \cdots \mathbin{+\!\!+} m_{k-1} = m$, ensuring the RSA algorithm *correctly* encrypts and decrypts messages.

Theorem 9.7 (Correctness of the RSA Algorithm).
Let $n := pq$ for two distinct primes $p \neq q$ and suppose $e, d \in \mathbb{Z}$ satisfy $ed \equiv 1 \pmod{\varphi_e(n)}$. The following then holds for any message $M \in \mathbb{N}$.

$$\left(M^e\right)^d \equiv M \pmod{n}$$

This guarantees the correctness of the RSA algorithm. 定理

Proof. Assume the conditions provided above and recall the following.

$$\varphi_e(n) = \varphi_e(pq) = \varphi_e(p)\varphi_e(q) = (p-1)(q-1)$$

Since $ed \equiv 1 \pmod{\varphi_e(n)}$, we know $(p-1)(q-1) \mid ed - 1$, so that $p - 1 \mid ed - 1$ and $q - 1 \mid ed - 1$. There then exist $k, \ell \in \mathbb{Z}$ as follows.

$$(p-1)k + 1 = ed \qquad \text{and} \qquad (q-1)\ell + 1 = ed$$

We will now show $\left(M^e\right)^d \equiv M \pmod{p}$. There are two cases.

Case 1:
Assume $M \equiv 0 \pmod{p}$. Clearly then $M^{ed} \equiv 0^{ed} \equiv 0 \pmod{p}$.

Case 2:
Assume $M \not\equiv 0 \pmod{p}$. Since p is prime, we then know $\gcd(p, M) = 1$. *Férmat's little theorem* hence requires $(M^k)^{p-1} \equiv 1 \pmod{p}$. Observe.

$$\begin{aligned} M^{ed} &\equiv M^{(p-1)k+1} && \pmod{p} \\ &\equiv M^{(p-1)k} M && \pmod{p} \\ &\equiv (M^k)^{p-1} M && \pmod{p} \\ &\equiv 1 \cdot M && \pmod{p} \\ &\equiv M && \pmod{p} \end{aligned}$$

Therefore, $\left(M^e\right)^d \equiv M \pmod{p}$.

Mutatis mutandis, we have that $\left(M^e\right)^d \equiv M \pmod{q}$. We therefore conclude $M^{ed} \equiv M \pmod{pq}$ by the *Chinese remainder theorem*. Q.E.D.

Index