## COURSE PRELIMINARIES

# Foundations: Logic, Sets, Functions, and the Craft of Proof

MATH S4061 | Introduction to Modern Analysis I

Logical and notational prerequisites — assuming no prior experience with proofs

*The only way to learn mathematics is to do mathematics.*

Paul R. Halmos

Contents of these preliminaries



**Overview.** These preliminaries are the on-ramp to the course. They assume you have never written a proof and have never met set notation, and they build—slowly and from the ground up—everything the lectures take for granted: how to read and write mathematical statements (0.1), the quantifiers that power every definition in analysis, the language of sets, relations, and functions, and, at its centre, the *craft of proof*: how a proof is built, the handful of standard strategies (which are exactly the Modes of Argument tagged throughout this book), and how to find one when you are stuck. We close with a worked, classified problem set. Read these preliminaries actively, with pencil in hand; nothing here is meant to be watched go by.

## 0.1 The Language of Mathematics

Mathematics is written in declarative sentences that are either true or false, and a proof is a chain of such sentences in which each link is forced by the ones before it. Before we can build or follow such a chain, we have to be able to read and write its links *exactly*. That is the whole purpose of this first section: not to prove anything deep, but to fix the grammar—statements and the words "not", "and", "or", "if…then", and "if and only if"—so precisely that later there is never any doubt about what a theorem claims or what a proof must deliver.

**Definition 0.1.1**

### Statement

A *statement* (or *proposition*) is a declarative sentence that is definitely true or definitely false—never both, and never neither. Its *truth value* is T (true) or F (false).

**Example 0.1.2**

*What is and isn't a statement*

"$2+2=4$" is a statement (true); "7 is even" is a statement (false). But "$x+1=3$" is *not* a statement as it stands—its truth depends on the unspecified $x$, so it has no fixed truth value; such a sentence is called an *open sentence*, and it becomes a statement only once $x$ is pinned down or quantified (0.2). "This sentence is false" is not a statement either: assuming it true makes it false and vice versa, so it has no consistent truth value. Questions and commands ("Is 7 prime?", "Add 3.") are never statements.

We build complicated statements from simple ones using five *connectives*. The first three are the everyday words *not*, *and*, *or*; we record their meaning in a *truth table*, which simply lists the truth value of the compound for every combination of truth values of its parts.

**Definition 0.1.3**

### Negation, conjunction, disjunction

Let $P$ and $Q$ be statements.

- the *negation* $\neg P$ ("not $P$") is true exactly when $P$ is false;
- the *conjunction* $P \wedge Q$ ("$P$ and $Q$") is true exactly when both are true;
- the *disjunction* $P \vee Q$ ("$P$ or $Q$") is true exactly when at least one is true.

| $P$ | $\neg P$ |
|---|---|
| T | F |
| F | T |

| $P$ | $Q$ | $P \wedge Q$ | $P \vee Q$ |
|---|---|---|---|
| T | T | T | T |
| T | F | F | T |
| F | T | F | T |
| F | F | F | F |

**Remark 0.1.4**

*"Or" is inclusive*

In ordinary speech "or" often means one or the other but not both ("soup or salad"). In mathematics "or" is always *inclusive*: $P \vee Q$ is true when $P$ is true, when $Q$ is true, *and* when both are true—only

the last row of the table, both false, makes it false. When we genuinely mean "exactly one," we say so.

The fourth connective, *implication*, is the engine of every theorem, and it is the one beginners find most surprising. An implication does not assert that its hypothesis holds; it only promises a *link*—that whenever the hypothesis holds, the conclusion does too.

**Definition 0.1.5**

## Implication

The *implication* $P \Rightarrow Q$ ("if $P$ then $Q$", or "$P$ implies $Q$") is false in exactly one situation: when $P$ is true and $Q$ is false. In every other case it is true.

| $P$ | $Q$ | $P \Rightarrow Q$ |
|---|---|---|
| T | T | T |
| T | F | F |
| F | T | T |
| F | F | T |

Here $P$ is the *hypothesis* (or *antecedent*) and $Q$ the *conclusion* (or *consequent*).

**Remark 0.1.6**

*Why a false hypothesis makes the implication true (vacuous truth)*

The last two rows of the table are the ones to dwell on: when $P$ is false, $P \Rightarrow Q$ is counted *true* no matter what $Q$ is. This is called *vacuous truth*, and it is forced on us by what an implication promises. Read $P \Rightarrow Q$ as a promise: "whenever $P$ holds, $Q$ holds." The only way to *break* such a promise is to exhibit a case where $P$ holds yet $Q$ fails—the second row. If $P$ never holds, the promise is never put to the test, so it cannot have been broken, and we call it true by default. A promise like "if you score 100, I will buy you dinner" is not a lie on a day you scored 60; it simply was not triggered. So "if $0 = 1$, then I am the Pope" is a true statement: its hypothesis is false, so the implication holds vacuously—it tells you nothing about the Pope. We will lean on vacuous truth constantly; for instance, "every element of the empty set is even" is true precisely because there is no element to check (0.3).

From an implication $P \Rightarrow Q$ we can form three close relatives by swapping and negating. Two of them are traps for the unwary.

**Definition 0.1.7**

## Converse, contrapositive, inverse

Given $P \Rightarrow Q$, its

- *converse* is $Q \Rightarrow P$;
- *contrapositive* is $\neg Q \Rightarrow \neg P$;
- *inverse* is $\neg P \Rightarrow \neg Q$.

An implication and its contrapositive always have the same truth value—they are *logically equivalent*, and proving one proves the other (this is the basis of *contrapositive proof*, 0.5).

An implication and its converse are *not* equivalent: the converse may be true or false independently, and confusing the two is among the most common errors in a first proof course.

**Example 0.1.8**

*The converse can fail*

Let $P$ be "$n$ is divisible by 4" and $Q$ be "$n$ is even." Then $P \Rightarrow Q$ is true (a multiple of 4 is certainly even). Its converse $Q \Rightarrow P$—"every even number is divisible by 4"—is false ($n = 6$ is even but not a multiple of 4). Its contrapositive "if $n$ is odd then $n$ is not divisible by 4" is true, as it must be, being equivalent to the original. Proving $P \Rightarrow Q$ tells you nothing about whether $Q \Rightarrow P$ holds; that is a separate question.

The fifth connective ties an implication to its converse.

**Definition 0.1.9**

## Biconditional; necessary and sufficient

The *biconditional* $P \Leftrightarrow Q$ ("$P$ if and only if $Q$", abbreviated "$P$ iff $Q$") is true exactly when $P$ and $Q$ have the same truth value. It is the conjunction of an implication and its converse: $P \Leftrightarrow Q$ means $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$. Correspondingly one says $P$ is *sufficient* for $Q$ (because $P \Rightarrow Q$) and $P$ is *necessary* for $Q$ (because $Q \Rightarrow P$, i.e. $Q$ cannot hold without $P$). Proving a biconditional therefore requires proving *both* directions, usually labelled ($\Rightarrow$) and ($\Leftarrow$).

## 0.2 Quantifiers

In 0.1.2 we met *open sentences* such as "$x + 1 = 3$": sentences that are neither true nor false until the variable is pinned down. *Quantifiers* are the two phrases that pin a variable down by declaring *how many* of its values make the sentence true—"for all" and "there exists." They are not a side topic. Every definition in this course—convergence, continuity, the least-upper-bound property—is a short tower of stacked quantifiers, and the single most useful skill these preliminaries can give you is reading, building, and *negating* such towers fluently.

**Definition 0.2.1**

### Predicate and domain of discourse

A *predicate* (or *open sentence*) $P(x)$ is a sentence containing a variable $x$ that becomes a statement once $x$ is assigned a value from a specified set $D$, called the *domain* (or *universe*) *of discourse*. For instance, with $P(x)$ the sentence "$x^2 = 2$" on the domain $D = \mathbb{R}$, the value $x = \sqrt{2}$ makes $P(x)$ true and $x = 1$ makes it false. A predicate may involve several variables, $P(x, y)$, each ranging over its own domain.

**Definition 0.2.2**

### The universal and existential quantifiers

Let $P(x)$ be a predicate on a domain $D$.

- the *universal* statement $\forall x \in D,\ P(x)$ ("for all $x$ in $D$, $P(x)$") is true exactly when $P(x)$ holds for *every* value of $x$ in $D$;
- the *existential* statement $\exists x \in D,\ P(x)$ ("there exists $x$ in $D$ such that $P(x)$") is true exactly when $P(x)$ holds for *at least one* value of $x$ in $D$.

Once quantified, $x$ is a *bound* variable—a placeholder, so that $\forall x\, P(x)$ and $\forall t\, P(t)$ say the very same thing—and the quantified sentence is a genuine statement, with a fixed truth value that no longer depends on $x$. A variable left unquantified is *free*, and a sentence with a free variable is an open sentence, not a statement (0.1.2).

**Example 0.2.3**

*Reading the quantifiers*

Each line below is a complete statement; its truth value follows.

- $\forall x \in \mathbb{R},\ x^2 \geq 0$ (true: a square is never negative);
- $\exists x \in \mathbb{R},\ x^2 = 2$ (true: $x = \sqrt{2}$ is a witness);
- $\exists x \in \mathbb{Q},\ x^2 = 2$ (false: no rational number squares to 2; we prove this in 0.5);
- $\forall n \in \mathbb{N},\ n + 1 > n$ (true).

Over an *empty* domain the conventions follow vacuous truth (0.1.6): $\forall x \in \emptyset$, $P(x)$ is true (there is no $x$ to violate it) and $\exists x \in \emptyset$, $P(x)$ is false (there is no $x$ to witness it).

**Remark 0.2.4**

*Proving versus disproving each quantifier*

The two quantifiers call for opposite kinds of work, and recognising which you face is half of finding a proof.

- To *prove* $\forall x \in D,\ P(x)$ you must treat an *arbitrary* $x$: you write "fix $x \in D$" and argue for that nameless $x$ using nothing special about it—checking examples, however many, never suffices. To *disprove* it you need only one *counterexample*: a single $x \in D$ for which $P(x)$ is false.
- To *prove* $\exists x \in D,\ P(x)$ you exhibit one *witness*: a specific $x$ (often constructed) for which $P(x)$ holds. To *disprove* it you must show that *every* $x$ fails, i.e. prove $\forall x \in D,\ \neg P(x)$.

Universals need an arbitrary element; existentials need a witness. This asymmetry shapes nearly every proof you will write, and we return to it in earnest in 0.5.

The most mechanical—and most valuable—fact about quantifiers is how they behave under negation. It lets you compute, with no cleverness at all, exactly what it means for a definition to *fail*.

**Definition 0.2.5**

## Negating a quantifier

For any predicate $P$ on a domain $D$,

$$\neg\big(\forall x \in D,\ P(x)\big) \ \equiv\ \exists x \in D,\ \neg P(x), \qquad \neg\big(\exists x \in D,\ P(x)\big) \ \equiv\ \forall x \in D,\ \neg P(x).$$

In words: "not every $x$ satisfies $P$" means "some $x$ fails $P$," and "no $x$ satisfies $P$" means "every $x$ fails $P$." To negate a whole string of quantifiers, sweep it left to right, turning each $\forall$ into $\exists$ and each $\exists$ into $\forall$, and finally negate the predicate at the end. This rule is the engine of mode A11 (0.5)—unfolding the failure of a definition by negating it term by term.

**Example 0.2.6**

*Negation in action—a preview of convergence*

You are not expected to follow the analysis here; watch only the mechanics. The statement "$a_n \to L$" is defined by a tower of three quantifiers,

$$\forall\, \varepsilon > 0,\ \ \exists\, N,\ \ \forall\, n \geq N,\ \ |a_n - L| < \varepsilon.$$

Negating mechanically—flip each quantifier, negate the inside—gives

$$\exists\, \varepsilon > 0,\ \ \forall\, N,\ \ \exists\, n \geq N,\ \ |a_n - L| \geq \varepsilon.$$

In words: $a_n$ *fails* to converge to $L$ when there is some positive $\varepsilon$ such that, however far out you place the threshold $N$, some later term $a_n$ still lies at least $\varepsilon$ away from $L$. The point is that we produced this by a rule, not by insight; when the definitions get hard, this is how you will always know precisely what must be shown.

When quantifiers of different kinds are stacked, their *order* is part of the meaning; swapping a $\forall$ past an $\exists$ can turn a truth into a falsehood.

**Definition 0.2.7**

## Nested quantifiers; order matters

Read a stacked statement left to right, as a dialogue between you and an adversary: each $\forall$ is a value handed to you by the adversary, and each $\exists$ to its right is a value *you* supply, allowed to depend on everything already named. Thus

$$\forall x \in \mathbb{R},\ \exists y \in \mathbb{R},\quad y > x$$

is *true*—handed any $x$, you answer $y = x + 1$—while the swap

$$\exists y \in \mathbb{R},\ \forall x \in \mathbb{R},\quad y > x$$

is *false*: now you must commit to a single $y$ *before* any $x$ is named, and no fixed real number exceeds every real number. Same four symbols, opposite truth values; only the order differs.

**Remark 0.2.8**

*The dependence is the whole game*

In $\forall x\, \exists y$ the witness $y$ may depend on $x$; in $\exists y\, \forall x$ it may not. Every $\varepsilon$–$N$ and $\varepsilon$–$\delta$ definition in this course is an "$\forall\exists$" statement in which the threshold $N$ (or the radius $\delta$) is permitted to depend on $\varepsilon$—and, later, the difference between ordinary and *uniform* convergence is nothing but a deliberate change in that order of dependence. Getting the order right is not pedantry; it is the mathematics.

**Definition 0.2.9**

## Unique existence

The statement $\exists!\, x \in D,\ P(x)$ ("there exists a *unique* $x$ in $D$ such that $P(x)$") abbreviates

$$\exists x \in D,\ \Big(P(x)\ \wedge\ \forall y \in D,\ \big(P(y) \Rightarrow y = x\big)\Big)\,:$$

at least one $x$ satisfies $P$, and any two that do are equal. Proving it therefore has two separate parts—*existence* (exhibit one $x$ that works) and *uniqueness* (assume $P(x)$ and $P(y)$ both hold and deduce $x = y$).

## 0.3 Sets

Almost every object in this course—a sequence, a function, an interval, the real line itself—is, underneath, a *set*: a collection of things considered as a single whole. The language of sets is the notation in which every later definition is written, so before convergence or continuity can be stated we need to be able to name a collection, say what belongs to it, compare two collections, and combine them. None of this is deep; what it asks of you is precision, and the one new habit it demands is the pair of proof moves for comparing sets—showing one sits inside another, and showing two are equal—which we introduce here and lean on for the rest of the book.

**Definition 0.3.1**

### Set, element, membership

A *set* is a collection of objects, considered as a single object in its own right. The objects in the collection are its *elements* (or *members*). If $x$ is an element of the set $A$ we write $x \in A$ ("$x$ belongs to $A$"); if it is not, we write $x \notin A$. A set is determined *entirely* by which objects belong to it—nothing else about it matters, not how its elements are listed, described, or ordered, and not whether any are named twice.

That last sentence is the whole content of the idea, so it is worth saying again plainly: a set is fixed by its membership and by nothing else. Two descriptions that admit exactly the same objects describe the same set, however different they look on the page. We make that principle official in 0.3.5; first we need ways to write sets down.

**Definition 0.3.2**

### Roster and set-builder notation

There are two standard ways to specify a set.

- *Roster (list) notation* names the elements between braces: $\{1, 2, 3\}$ is the set whose members are 1, 2, and 3. Because only membership matters, $\{1, 2, 3\}$, $\{3, 2, 1\}$, and $\{1, 1, 2, 3, 3\}$ are the *same* set—order and repetition carry no information. A one-element set such as $\{x\}$ is called a *singleton*; the braces are not optional, since $\{x\}$ is a *set* whose lone member is $x$, a different object from $x$ itself. A list may trail off in a clear pattern, as in $\{0, 1, 2, 3, \dots\}$, but only when the pattern is genuinely unambiguous.
- *Set-builder notation* carves a set out of a known domain $D$ using a predicate $P(x)$ (0.2.1):

$$\{\, x \in D : P(x) \,\}$$

  is read "the set of all $x$ in $D$ such that $P(x)$," and its members are exactly those $x \in D$ for which $P(x)$ is true. Thus $\{\, x \in \mathbb{R} : x^2 < 4 \,\}$ is the open interval of reals strictly between $-2$ and 2. The colon is sometimes written as a vertical bar, $\{x \in D \mid P(x)\}$; the two are interchangeable.

**Remark 0.3.3**

*Set-builder* is *a quantifier in disguise*

Set-builder notation is the bridge from 0.2 to this section: "$y \in \{x \in D : P(x)\}$" means nothing more nor less than "$y \in D$ and $P(y)$." Whenever you must decide whether some object lies in a set defined this way, that is the translation to reach for—membership in a set-builder set is a predicate to be checked. Always state the domain $D$. Writing $\{x : P(x)\}$ with no domain at all invites the trouble of 0.3.18, so in this course every set is built inside one already in hand. (Two later constructions stand apart and rightly need no ambient domain: the power set 0.3.15 gathers *all* subsets of a given set, and the union or intersection of a family 0.3.22 ranges over the family itself.)

One collection is so important, and so easy to overlook, that it gets its own name and symbol: the collection with no members at all.

**Definition 0.3.4**

## The empty set

The *empty set* is the set with no elements; we write it $\varnothing$ (or $\{\,\}$). For every object $x$, the statement $x \in \varnothing$ is false. There is only *one* empty set: a set is fixed by its members (0.3.1), and any two sets with no members have exactly the same members (namely none), so they are the same set. We therefore speak of *the* empty set.

The empty set is where vacuous truth (0.1.6) earns its keep. "Every element of $\varnothing$ is even" is true—not because we checked, but because there is no element to check, so the claim cannot fail. Any sentence beginning "every element of $\varnothing\ldots$" is true, and any beginning "some element of $\varnothing\ldots$" is false. Hold onto this; it is exactly why the empty set will turn out to sit inside every set whatsoever.

**Definition 0.3.5**

## Equality of sets (extensionality)

Two sets $A$ and $B$ are *equal*, written $A = B$, when they have exactly the same elements: for every object $x$,

$$x \in A \iff x \in B.$$

This principle—that a set is determined by its members alone—is called *extensionality*.[1] It is the only way two sets are ever shown equal, and it is the reason $\{1, 2, 3\} = \{3, 2, 1\}$.

Equality compares membership in both directions at once. Most of the time we want the one-directional comparison: every member of one set is also a member of another.

**Definition 0.3.6**

## Subset and proper subset

A set $A$ is a *subset* of a set $B$, written $A \subseteq B$, when every element of $A$ is also an element of $B$:

$$A \subseteq B \quad \text{means} \quad \forall x,\ (x \in A \Rightarrow x \in B).$$

We also say $A$ is *contained in* $B$, or $B$ *contains* $A$. If in addition $A \neq B$—so $B$ has at least one element outside $A$—we call $A$ a *proper* subset and write $A \subsetneq B$. Comparing the

[1] The name contrasts with an *intensional* view, where the *description* would matter. Sets are extensional: only the extension, the actual collection of members, counts. "Even prime" and "{2}" describe the same set.

definition with 0.3.5 shows the link we will use constantly: $A = B$ holds exactly when $A \subseteq B$ *and* $B \subseteq A$.

**Remark 0.3.7**

*Two proof moves to memorise now*

This definition seeds the two most-used techniques in the book, both unfolded properly in 0.5; meet them here so they are familiar when the analysis starts.

- *To prove* $A \subseteq B$. The claim is a universal implication, so you prove it the way 0.2.4 prescribes: *fix* an arbitrary $x \in A$, then argue—using only that $x \in A$—that $x \in B$. The argument must work for a nameless element, never for examples. The skeleton is always "Let $x \in A$. … Hence $x \in B$, so $A \subseteq B$."
- *To prove* $A = B$. Prove $A \subseteq B$ and $B \subseteq A$ separately. This is *double inclusion*, and it is how essentially every set identity in this course is established: show each side contains the other.

Reach for these two moves automatically. The moment a problem mentions $\subseteq$ or $=$ between sets, you already know the first line of your proof.

**Proposition 0.3.8**

## $\varnothing \subseteq A$ and $A \subseteq A$, for every set $A$

For every set $A$, the empty set is a subset of $A$, and $A$ is a subset of itself.

**Proof 0.3.8**

*Proof by Unwinding the Definition of Subset.*

(1) To show $\varnothing \subseteq A$, we must show $\forall x,\ (x \in \varnothing \Rightarrow x \in A)$. Fix any $x$. Its hypothesis $x \in \varnothing$ is false (0.3.4), so the implication $x \in \varnothing \Rightarrow x \in A$ is true vacuously (0.1.6)—there is no $x$ that could break it. As $x$ was arbitrary, $\varnothing \subseteq A$.

(2) To show $A \subseteq A$, fix $x \in A$; then $x \in A$, which is what was to be shown. Hence $A \subseteq A$.

■

[Direct]

With the comparisons in place we name the sets this whole course is built on. Their careful *construction*—building each from the one before, and pinning down what makes the reals complete—is the business of the first lectures; here we only fix names and symbols.

**Definition 0.3.9**

## The standard number sets

We write, throughout the book,

$$\mathbb{N} = \{0, 1, 2, 3, \dots\}, \quad \mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}, \quad \mathbb{Q} = \left\{ \tfrac{p}{q} : p \in \mathbb{Z},\ q \in \mathbb{Z},\ q \neq 0 \right\},$$

the *natural numbers*, the *integers*, and the *rational numbers*, and $\mathbb{R}$ for the *real numbers*. By the convention of this course $0 \in \mathbb{N}$. These nest,

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

and each inclusion is proper. How $\mathbb{N}$ is founded and induction justified (1.1), how $\mathbb{Z}$ and $\mathbb{Q}$ are constructed (1.2), why $\mathbb{Q}$ leaves gaps that force us to $\mathbb{R}$ (1.4), and how $\mathbb{R}$ is built to fill them (1.6) are all taken up later in the course; for now they are names with which to write examples.

Sets become useful once we can *combine* them. The three basic operations mirror the logical connectives of 0.1 exactly: "and" becomes intersection, "or" becomes union, "not" becomes complement. Read the definitions with that correspondence in mind and they need no memorising.

**Definition 0.3.10**

## Union, intersection, difference, complement

Let $A$ and $B$ be sets, and let everything in sight be drawn from a fixed *universe* (or *universal set*) $U$. We define

$$A \cup B = \{\, x \in U : x \in A \text{ or } x \in B \,\}, \qquad A \cap B = \{\, x \in U : x \in A \text{ and } x \in B \,\},$$

the *union* and the *intersection* (the "or" here is inclusive, 0.1.4); the *difference*

$$A \setminus B = \{\, x \in U : x \in A \text{ and } x \notin B \,\}$$

("$A$ minus $B$," the elements of $A$ left after removing those in $B$); and, relative to the universe $U$, the *complement*

$$A^c = U \setminus A = \{\, x \in U : x \notin A \,\}.$$

The complement depends on the chosen $U$, so $U$ must be fixed before $A^c$ has a meaning.

**Example 0.3.11**

*The operations on small sets*

Let $A = \{1,2,3,4\}$ and $B = \{3,4,5\}$ inside the universe $U = \{1,2,3,4,5,6\}$. Then $A \cup B = \{1,2,3,4,5\}$, $A \cap B = \{3,4\}$, $A \setminus B = \{1,2\}$, $B \setminus A = \{5\}$, and $A^c = \{5,6\}$. The difference is one-sided: $A \setminus B \neq B \setminus A$ in general. For a nonexample of intersection, $\{1,2\} \cap \{3,4\} = \varnothing$—two sets can perfectly well share no element, and then their intersection is the empty set.

**Definition 0.3.12**

## Disjoint and pairwise disjoint

Two sets $A$ and $B$ are *disjoint* when $A \cap B = \varnothing$—they share no element. A collection of sets is *pairwise disjoint* when any two *distinct* sets from it are disjoint. Thus $\{1,2\}$, $\{3\}$, and $\{4,5\}$ are pairwise disjoint, while $\{1,2\}$, $\{2,3\}$, $\{4\}$ are not (the first two meet in 2).

A picture fixes all of this at once. A *Venn diagram* draws the universe as a rectangle and each set as a region inside it; the operations are then the regions you shade.

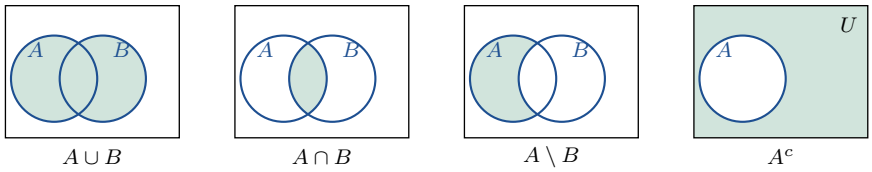


**Figure 0.3.13.** THE FOUR OPERATIONS AS SHADED REGIONS. In each panel the universe $U$ is the rectangle and $A, B$ are the discs; the shaded region is the named set. Union shades either disc; intersection, only the overlap; difference $A \setminus B$, the part of $A$ outside $B$; complement $A^c$, everything in $U$ outside $A$.

The correspondence between set operations and logical connectives is not a coincidence to admire and forget; it is a working tool. Every law the connectives obey in 0.1 becomes a law the operations obey, and the proofs are translations. Two families of such laws come up constantly.

**Proposition 0.3.14**

## Distributive and De Morgan laws

For all sets $A$, $B$, $C$, and for $A$, $B$ inside a universe $U$,

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C), \qquad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

*(the distributive laws)*, and

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

*(De Morgan's laws)*. In words for the last pair: to be outside a union is to be outside both; to be outside an intersection is to be outside at least one. We prove the first De Morgan law below; the first distributive law is worked the same way, by double inclusion, in 0.E.18.

**Proof 0.3.14**

*Proof by Double Inclusion of the First De Morgan Law.*

(1) We prove $(A \cup B)^c = A^c \cap B^c$ by showing each side is a subset of the other (0.3.7). For the forward inclusion $\subseteq$, fix $x \in (A \cup B)^c$. Then $x \in U$ and $x \notin A \cup B$, so it is not the case that $x \in A$ or $x \in B$. The negation of an "or" is an "and" of negations, which the truth tables of 0.1.3 make plain, so $x \notin A$ and $x \notin B$. With $x \in U$ this gives $x \in A^c$ and $x \in B^c$, that is,

$$x \in A^c \cap B^c.$$

Hence $(A \cup B)^c \subseteq A^c \cap B^c$.

(2) For the reverse inclusion $\supseteq$, fix $x \in A^c \cap B^c$. Then $x \in U$ with $x \notin A$ and $x \notin B$,

so neither $x \in A$ nor $x \in B$ holds; therefore $x \notin A \cup B$. With $x \in U$ this says

$$x \in (A \cup B)^c,$$

so $A^c \cap B^c \subseteq (A \cup B)^c$.

(3) Both inclusions hold, so by double inclusion the two sets are equal. ■

[Direct]; the other three are identical translations of the truth tables of 0.1.3.

Every set so far has had numbers, or points, for elements. Nothing stops the elements *themselves* from being sets, and one such construction is indispensable: the set of all subsets of a given set.

**Definition 0.3.15**

## Power set

The *power set* of a set $S$, written $\mathcal{P}(S)$, is the set whose elements are all the subsets of $S$:

$$\mathcal{P}(S) = \{\, A : A \subseteq S \,\}.$$

Thus "$A \in \mathcal{P}(S)$" means precisely "$A \subseteq S$." Because $\varnothing \subseteq S$ and $S \subseteq S$ for every $S$ (0.3.8), both $\varnothing$ and $S$ are always elements of $\mathcal{P}(S)$.

**Example 0.3.16**

*The power set of a two-element set*

For $S = \{a, b\}$ the subsets are: the empty set, the two singletons, and $S$ itself, so

$$\mathcal{P}(\{a, b\}) = \{\, \varnothing,\ \{a\},\ \{b\},\ \{a, b\} \,\},$$

a set with *four* elements. The braces matter: $\{a\}$, the singleton, is an element of $\mathcal{P}(S)$, whereas $a$ is not—$a$ is an element of $S$, not a subset of it. Counting subsets in general: to build a subset of an $n$-element set you decide, independently, "in or out" for each of the $n$ elements, which is 2 choices made $n$ times. So a finite set with $n$ elements has exactly $2^n$ subsets, and $|\mathcal{P}(S)| = 2^{|S|}$. Here $n = 2$ gives $2^2 = 4$, matching the list.

**Remark 0.3.17**

*$\varnothing \in \mathcal{P}(S)$ versus $\varnothing \subseteq S$—a classic confusion*

These two true statements look almost identical and mean different things; keeping them apart is a rite of passage. The symbol $\in$ relates an *element* to a set; the symbol $\subseteq$ relates a *set* to a set. Both

$$\varnothing \subseteq S \qquad \text{and} \qquad \varnothing \in \mathcal{P}(S)$$

are true *for every* $S$, and they are really the same fact wearing two hats: $\varnothing$ is a *subset* of $S$ (0.3.8), and therefore $\varnothing$ is an *element* of the power set, because elements of $\mathcal{P}(S)$ *are* the subsets of $S$. But $\varnothing \in S$ is a different claim entirely, usually false: it asserts that the empty set is one of the actual members of $S$, and for $S = \{1, 2\}$ it plainly is not. The test is mechanical: ask whether the thing on the left is being offered as a *member* ($\in$) or as a sub-collection ($\subseteq$), and check the right object against

the matching definition. A symptom of the confusion is $\varnothing = \{\varnothing\}$; these are unequal, since the left has no elements and the right has exactly one (namely $\varnothing$).

**Remark 0.3.18**

*Why there is no "set of all sets"*

Set-builder notation feels as though it should let us form "the set of all $x$ with property $P$" for *any* property $P$ and any reach we like. It does not, and the reason is worth seeing once, because it explains the insistence in 0.3.3 on always naming a domain. Suppose we allowed an unrestricted $R = \{\, x : x \notin x \,\}$, the set of all sets that are not members of themselves. Ask whether $R \in R$. If $R \in R$, then $R$ meets its own defining condition, so $R \notin R$; and if $R \notin R$, then $R$ satisfies the condition, so $R \in R$. Either answer contradicts itself—this is *Russell's paradox*. The lesson is not that mathematics is broken; it is that you may not conjure a set from a property out of thin air. You carve new sets *out of sets already in hand*, with set-builder applied to a known domain $D$, exactly as we have done throughout. Do that, and no paradox can arise; the heavy machinery that guarantees this is the subject of axiomatic set theory, which the course will not need.

To build the plane, and later every space in the course, we need to pair elements in a way that, unlike a set, *remembers order*. The set $\{a, b\}$ forgets which came first; an *ordered pair* does not.

**Definition 0.3.19**

## Ordered pair

An *ordered pair* $(a, b)$ is the pairing of a *first* coordinate $a$ with a *second* coordinate $b$, in that order. Its defining property is the equality rule

$$(a, b) = (c, d) \quad \Longleftrightarrow \quad a = c \ \text{ and } \ b = d :$$

two ordered pairs are equal exactly when they agree in the first coordinate and in the second. In particular order counts—$(1, 2) \neq (2, 1)$, although $\{1, 2\} = \{2, 1\}$—and a coordinate may repeat, as in $(7, 7)$, which no two-element set could express.

**Definition 0.3.20**

## Cartesian product

The *Cartesian product* of sets $A$ and $B$ is the set of all ordered pairs with first coordinate from $A$ and second from $B$:

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

The plane is the leading example: $\mathbb{R} \times \mathbb{R}$, written $\mathbb{R}^2$, is the set of all coordinate pairs $(x, y)$ of real numbers. More generally, for finitely many sets $A_1, \ldots, A_n$ the product

$$A_1 \times \cdots \times A_n = \{\, (a_1, \ldots, a_n) : a_i \in A_i \text{ for each } i \,\}$$

collects the ordered $n$-tuples, with $\mathbb{R}^n = \mathbb{R} \times \cdots \times \mathbb{R}$ ($n$ factors) the space in which the course's metric geometry (2.2) will eventually live.

**Example 0.3.21**

*A product is a grid; for finite sets, sizes multiply*

With $A = \{1, 2, 3\}$ and $B = \{x, y\}$,

$$A \times B = \big\{(1, x), (1, y), (2, x), (2, y), (3, x), (3, y)\big\},$$

six pairs—a 3-by-2 grid of choices. In general $|A \times B| = |A| \cdot |B|$ for finite $A, B$, since each of the $|A|$ first coordinates may be matched with any of the $|B|$ second coordinates. Order in the product matters too: $A \times B$ and $B \times A$ are different sets here, the first holding $(1, x)$ and the second holding $(x, 1)$.

Union and intersection were defined for two sets, but analysis routinely combines *infinitely many*—one set for each natural number, or one for each real radius. We index the sets by a label drawn from an *index set* and take the union or intersection over all labels at once.

**Definition 0.3.22**

## Indexed family; arbitrary union and intersection

An *indexed family* of sets is an assignment $\alpha \mapsto A_\alpha$ of a set $A_\alpha$ to each $\alpha$ in an *index set* $I$; we write it $\{A_\alpha\}_{\alpha \in I}$. Its union and intersection are

$$\bigcup_{\alpha \in I} A_\alpha = \{\, x : x \in A_\alpha \text{ for } \textit{some } \alpha \in I \,\}, \qquad \bigcap_{\alpha \in I} A_\alpha = \{\, x : x \in A_\alpha \text{ for } \textit{every } \alpha \in I \,\}.$$

The union collects everything that lands in at least one member of the family; the intersection, only what lands in all of them. The index set $I$ may be finite, or infinite—this is exactly what lets us combine infinitely many sets in a single stroke. The quantifier inside each definition is the one to keep your eye on: "some $\alpha$" for $\bigcup$, "every $\alpha$" for $\bigcap$.

**Example 0.3.23**

*An intersection over an infinite index set*

Index by the positive integers $I = \{\, n \in \mathbb{N} : n \geq 1 \,\}$, and let $A_n = \big[\, 0,\ \tfrac{1}{n} \,\big]$, the closed interval from 0 to $1/n$. As $n$ grows the intervals shrink toward the single point 0. Their union is just the largest, $\bigcup_{n \in I} A_n = [0, 1]$ (since $A_1 = [0, 1]$ contains all the others). Their intersection is

$$\bigcap_{n \in I} A_n = \{0\}.$$

Certainly $0 \in A_n$ for every $n$, so 0 is in the intersection. And no positive $x$ survives: given $x > 0$, some $1/n < x$ (the Archimedean property, 1.7), so $x \notin A_n = [0, 1/n]$ for that $n$, hence $x$ fails the "every $\alpha$" test. The intersection of infinitely many nonempty sets can thus collapse to a single point—a phenomenon at the heart of the nested-interval arguments to come.

## 0.4 Relations and Functions

Sets on their own are inert collections; analysis comes alive only once we can speak of how their elements stand to one another and how one set is sent into another. "3 is less than 5," "2 divides 6," "$f$ sends $x$ to $x^2$"—each pairs up elements, and each is captured by the same single idea, a *relation*: a set of ordered pairs. From that one notion we will carve out the object this whole course turns on, the *function*, and then the two refinements of it that every later definition leans on: the way a function can be *injective* or *surjective*, and the way an *equivalence relation* sorts a set into clean disjoint pieces. We build all of it from the sets of 0.3, with the quantifier discipline of 0.2 doing the real work.

**Definition 0.4.1**

### Ordered pair and Cartesian product

We recall two notions from 0.3.19–0.3.20, now as the substrate on which relations are built. The *ordered pair* $(a, b)$ records two objects *in order*: $(a, b) = (c, d)$ exactly when $a = c$ and $b = d$, so $(1, 2)$ and $(2, 1)$ are different pairs even though the sets $\{1, 2\}$ and $\{2, 1\}$ are equal. Given sets $A$ and $B$, their *Cartesian product* is the set of all such pairs,

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

We write $A^2$ for $A \times A$. Thus $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ is the familiar plane of coordinate pairs, and $\{1, 2\} \times \{x, y\} = \{(1, x), (1, y), (2, x), (2, y)\}$ has $2 \cdot 2 = 4$ elements.

A relation is simply a choice of *which* pairs we want to single out from this product.

**Definition 0.4.2**

### Relation

A *relation* from $A$ to $B$ is a subset $R \subseteq A \times B$. We write $a\ R\ b$ (read "$a$ is related to $b$") to mean $(a, b) \in R$, and $a \not R\ b$ when $(a, b) \notin R$. When $A = B$ we call $R$ a relation *on* $A$. The *domain* of $R$ is the set of first coordinates that actually occur, and the *range* the set of second coordinates,

$$\operatorname{dom} R = \{\, a \in A : \exists\, b \in B,\ a\ R\ b \,\}, \qquad \operatorname{ran} R = \{\, b \in B : \exists\, a \in A,\ a\ R\ b \,\}.$$

**Example 0.4.3**

*Two relations you already know*

The order relation "$\leq$" on $\mathbb{R}$ is the relation $R = \{(a, b) \in \mathbb{R}^2 : a \leq b\}$; writing $a\ R\ b$ is exactly writing $a \leq b$, so the familiar symbol *is* the set of pairs it picks out. Its domain and range are both all of $\mathbb{R}$. The relation "divides" on $\mathbb{N}$ is $D = \{(m, n) : \exists\, k \in \mathbb{N},\ n = mk\}$; here $2\ D\ 6$ (take $k = 3$) but $4 \not D\ 6$. These two examples already display the structure we chase below: $\leq$ is an *order*, and—once we adjust it—a relation like "$m - n$ is even" will be an *equivalence*.

Most relations are too loose to compute with. A function is the special, disciplined kind in which every input has *exactly one* output—no input left unanswered, and none answered twice. That

single phrase, "exactly one," is the unique-existence quantifier of 0.2.9, and it is the heart of the definition.

**Definition 0.4.4**

## Function

A *function* (or *map*) $f\colon A \to B$ is a relation $f \subseteq A \times B$ such that for every $a \in A$ there is exactly one $b \in B$ with $(a, b) \in f$:

$$\forall\, a \in A, \quad \exists!\, b \in B, \quad (a, b) \in f.$$

That unique $b$ is written $f(a)$, the *value* of $f$ at $a$. The set $A$ is the *domain*, $B$ the *codomain*, and the *image* (or *range*) is the set of values actually hit,

$$f(A) = \{\, f(a) : a \in A \,\} \subseteq B.$$

Two functions are equal when they have the same domain, the same codomain, and agree at every point—$f(a) = g(a)$ for all $a \in A$.

**Remark 0.4.5**

*Well-definedness: the two ways to fail*

The defining clause "exactly one $b$" is really two demands, and a candidate rule can break either. It must hand back *at least* one output for each input—a rule with no value at some $a$ (such as $a \mapsto 1/a$ offered as a map on all of $\mathbb{R}$, which says nothing at $a = 0$) is not a function on that domain. And it must hand back *at most* one—a rule assigning two values to a single input is not a function at all. The square-root "rule" $r$ on $\mathbb{R}_{\geq 0}$ that returns *both* $+\sqrt{x}$ and $-\sqrt{x}$ fails here: 4 would be related to both 2 and $-2$, so $(4, 2)$ and $(4, -2)$ both lie in $r$ and the output is not determined. When a definition presents an output through some choice—"pick a representative, then…"—checking that the answer does not depend on the choice is exactly the chore called *verifying $f$ is well defined*, and we meet it head-on with equivalence classes in 0.4.16.

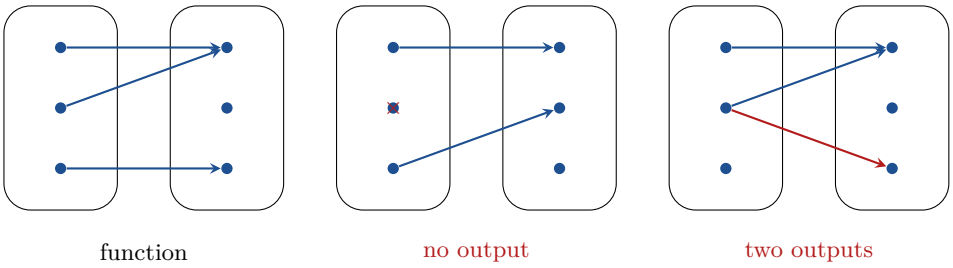


**Figure 0.4.6.** A function versus two non-functions. In a function every left dot fires exactly one arrow; the middle picture leaves an input unanswered, the right picture answers one input twice.

A function moves whole *sets* around, forwards and backwards. The forward motion sends a subset of the domain to the set of its values; the backward motion—defined for *any* function, invertible or not—collects every input that lands in a target set.

**Definition 0.4.7**

## Image and preimage of a set

Let $f\colon A \to B$, let $S \subseteq A$ and $T \subseteq B$. The *image* of $S$ and the *preimage* (or *inverse image*) of $T$ are

$$f(S) = \{\, f(a) : a \in S \,\} \subseteq B, \qquad f^{-1}(T) = \{\, a \in A : f(a) \in T \,\} \subseteq A.$$

The symbol $f^{-1}(T)$ is a set, read off the rule $f$ alone; it carries *no* claim that $f$ has an inverse function. For instance, with $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$, we have $f^{-1}(\{4\}) = \{-2, 2\}$ and $f^{-1}\big((-\infty, 0)\big) = \emptyset$, even though $f$ is nowhere invertible.

**Proposition 0.4.8**

## Preimage respects the set operations

For any $f\colon A \to B$ and any subsets $T, U \subseteq B$,

$$f^{-1}(T \cap U) = f^{-1}(T) \cap f^{-1}(U), \qquad f^{-1}(T \cup U) = f^{-1}(T) \cup f^{-1}(U).$$

For any $S, S' \subseteq A$, the forward image is weaker: $f(S \cap S') \subseteq f(S) \cap f(S')$ always holds, but the reverse inclusion can fail.

**Proof 0.4.8**

*Direct Proof by Membership-Chasing that the Preimage Respects Intersection.*

(1) An element-of statement is proved by translating each side into its membership condition and checking the two conditions are the very same sentence. Fix $a \in A$. By the definition of preimage,

$$a \in f^{-1}(T \cap U) \iff f(a) \in T \cap U \iff \big(f(a) \in T \text{ and } f(a) \in U\big).$$

(2) The right-hand clause is, again by the definition of preimage, exactly "$a \in f^{-1}(T)$ and $a \in f^{-1}(U)$," which is to say $a \in f^{-1}(T) \cap f^{-1}(U)$. Since $a$ was arbitrary, the two sets have the same elements and are therefore equal (0.3).

(3) For the forward image the inclusion $f(S \cap S') \subseteq f(S) \cap f(S')$ holds because any $f(a)$ with $a \in S \cap S'$ lies in both $f(S)$ and $f(S')$. The reverse fails for $f(x) = x^2$ with $S = \{1\}$, $S' = \{-1\}$: then $S \cap S' = \emptyset$ gives $f(S \cap S') = \emptyset$, yet $f(S) \cap f(S') = \{1\} \cap \{1\} = \{1\}$.

■

[Direct] the union rule is identical with "and" replaced by "or".

Two questions decide how much a function can be reversed. Does it ever *collapse* two inputs to one output? Does it *reach* every point of the codomain? A "no" to the first and a "yes" to the second are the properties *injective* and *surjective*; together they make a function perfectly reversible. Each property is a quantified sentence, and—this is the part to internalise—each

comes with a fixed recipe for how its proof must open.

**Definition 0.4.9**

## Injective, surjective, bijective

A function $f\colon A \to B$ is

- *injective* (*one-to-one*) if distinct inputs give distinct outputs: $\forall\, x, y \in A,\ (f(x) = f(y) \Rightarrow x = y)$;
- *surjective* (*onto*) if every point of the codomain is hit: $\forall\, b \in B,\ \exists\, a \in A,\ f(a) = b$, that is, $f(A) = B$;
- *bijective* (a *one-to-one correspondence*) if it is both injective and surjective.

**Remark 0.4.10**

*How each proof must begin*

The quantifier shape of each property dictates the first line of its proof—learn these openings and you will never stare at a blank page on this kind of problem.

- To prove $f$ *injective*, the cleanest route is the equality form of the definition: *assume* $f(x) = f(y)$ for arbitrary $x, y \in A$, and *deduce* $x = y$. (One may instead assume $x \neq y$ and derive $f(x) \neq f(y)$, but the equation form is almost always easier to manipulate.)
- To prove $f$ *surjective*, it is a $\forall\exists$ statement (0.2.7): *fix an arbitrary* $b \in B$ and *construct a witness*—produce a specific $a \in A$, usually by solving $f(a) = b$ for $a$, and then verify $f(a) = b$.
- To *disprove* injectivity, exhibit one collision $x \neq y$ with $f(x) = f(y)$; to disprove surjectivity, exhibit one $b \in B$ that no input reaches.

**Example 0.4.11**

*The same rule, four different verdicts*

Whether a function is injective or surjective depends on the chosen domain and codomain, not on the formula alone. Take the rule $x \mapsto x^2$.

- $f\colon \mathbb{R} \to \mathbb{R}$ is neither: $f(-1) = f(1) = 1$ kills injectivity, and no input gives $-1$, killing surjectivity.
- $g\colon \mathbb{R} \to [0, \infty)$ is surjective (every $b \geq 0$ is $g(\sqrt{b})$) but still not injective.
- $h\colon [0, \infty) \to [0, \infty)$ is bijective: injective because $x^2 = y^2$ with $x, y \geq 0$ forces $x = y$, and surjective as before.

The successor map $s\colon \mathbb{N} \to \mathbb{N}$, $s(n) = n + 1$, is injective (if $n + 1 = m + 1$ then $n = m$) but not surjective: nothing maps to 0, since 0 is the least natural number. This is the first hint that an infinite set can match a *proper* subset of itself—a theme we take up under "same size" below and pursue in 2.1.

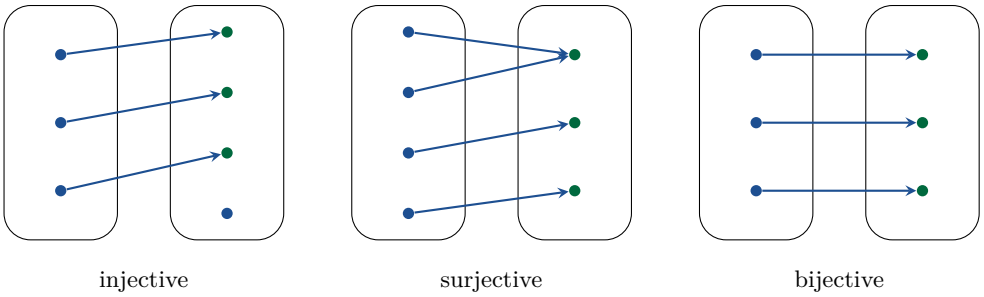


**Figure 0.4.12.** INJECTIVE, SURJECTIVE, BIJECTIVE. Injective: no two arrows share a head. Surjective: every right dot is hit. Bijective: a perfect pairing, no misses and no collisions.

Functions chain: feed the output of one into the next. This chaining, *composition*, is how complicated maps are assembled from simple ones, and it is the setting in which "reversing" a function gets its precise meaning.

**Definition 0.4.13**

## Composition and the identity

Given $f\colon A \to B$ and $g\colon B \to C$, the *composition* $g \circ f\colon A \to C$ is the function defined by

$$(g \circ f)(a) = g(f(a)), \qquad a \in A.$$

(The codomain of $f$ must match the domain of $g$, or the right-hand side is meaningless.) For each set $A$ the *identity function* $\mathrm{id}_A\colon A \to A$ is $\mathrm{id}_A(a) = a$. Composition is *associative*—$(h \circ g) \circ f = h \circ (g \circ f)$, since both send $a$ to $h(g(f(a)))$—and the identity is neutral: $f \circ \mathrm{id}_A = f = \mathrm{id}_B \circ f$.

**Definition 0.4.14**

## Inverse function

A function $f\colon A \to B$ is *invertible* if there is a function $g\colon B \to A$ with

$$g \circ f = \mathrm{id}_A \qquad \text{and} \qquad f \circ g = \mathrm{id}_B,$$

that is, $g(f(a)) = a$ for all $a \in A$ and $f(g(b)) = b$ for all $b \in B$. Such a $g$, when it exists, is unique and is written $f^{-1}$.[2]

**Theorem 0.4.15**

## A function is invertible iff it is bijective

A function $f\colon A \to B$ is invertible if and only if it is bijective.

**Proof 0.4.15**

*Direct Proof that Invertible Equals Bijective by Constructing the Inverse.*

[2]This $f^{-1}$, the inverse *function*, exists only when $f$ is bijective; the preimage $f^{-1}(T)$ of 0.4.7 is a set defined for *every* $f$. The shared notation is standard and harmless once you know which object is meant: $f^{-1}$ alone is a function, $f^{-1}(\,\cdot\,)$ applied to a *set* is a preimage.

(1) For the forward direction, suppose $f$ is invertible with inverse $g$. To see $f$ is injective, take $x, y \in A$ with $f(x) = f(y)$; applying $g$ and using $g \circ f = \mathrm{id}_A$,

$$x = g\big(f(x)\big) = g\big(f(y)\big) = y.$$

To see $f$ is surjective, fix $b \in B$ and set $a = g(b)$; then $f(a) = f(g(b)) = (f \circ g)(b) = b$, so $b$ is hit. Hence $f$ is bijective.

(2) For the converse, suppose $f$ is bijective. We must *build* a function $g\colon B \to A$. Fix $b \in B$. Surjectivity gives at least one $a \in A$ with $f(a) = b$; injectivity makes it the only one, for if $f(a) = f(a') = b$ then $a = a'$. So there is exactly one such $a$, and defining $g(b)$ to be that $a$ assigns one output to each input—$g$ is a genuine function (0.4.4).

(3) This $g$ inverts $f$ on both sides. For $a \in A$, the unique preimage of $f(a)$ is $a$ itself, so $g(f(a)) = a$, giving $g \circ f = \mathrm{id}_A$. For $b \in B$, $g(b)$ is by construction the input with $f(g(b)) = b$, giving $f \circ g = \mathrm{id}_B$. Thus $f$ is invertible.

■

[Direct] cf. 0.2.9 (unique existence) and 0.4.9.

We now return to relations on a single set to isolate the kind that behaves like *equality of some feature*—"same remainder on division by $n$," "same length," "same direction." Such a relation does not merely compare elements; it sorts the whole set into groups of mutually-related elements, and those groups will turn out to tile the set with no gaps and no overlaps. This sorting mechanism is the engine behind the construction of the integers and the rationals (1.2) and, later, the completion that builds the reals.

**Definition 0.4.16**

## Equivalence relation and equivalence class

A relation $\sim$ on a set $A$ is an *equivalence relation* if it is

- *reflexive*: $\forall\, a \in A,\ a \sim a$;
- *symmetric*: $\forall\, a, b \in A,\ (a \sim b \Rightarrow b \sim a)$;
- *transitive*: $\forall\, a, b, c \in A,\ (a \sim b \text{ and } b \sim c \Rightarrow a \sim c)$.

For $a \in A$ the *equivalence class* of $a$ is the set of everything related to it,

$$[a] = \{\, x \in A : x \sim a \,\} \subseteq A,$$

and any $x \in [a]$ is called a *representative* of that class. The set of all classes is the *quotient* $A/\!\sim\, = \{\, [a] : a \in A \,\}$.

**Example 0.4.17**

*Congruence modulo n*

Fix $n \in \mathbb{N}$ with $n \geq 1$. On $\mathbb{Z}$ declare $a \equiv b \pmod{n}$ to mean $n$ divides $a - b$. This is an equivalence relation: it is reflexive because $n \mid 0 = a - a$; symmetric because $n \mid (a - b)$ forces $n \mid (b - a)$; transitive because if $n \mid (a - b)$ and $n \mid (b - c)$ then $n$ divides their sum $(a - b) + (b - c) = a - c$. Its classes are the *residue classes*: for $n = 3$ they are

$$[0] = \{\dots, -3, 0, 3, 6, \dots\}, \quad [1] = \{\dots, -2, 1, 4, 7, \dots\}, \quad [2] = \{\dots, -1, 2, 5, 8, \dots\},$$

three disjoint sets whose union is all of $\mathbb{Z}$. Every integer lands in exactly one—precisely the partition phenomenon we now prove in general.

**Theorem 0.4.18**

## Equivalence classes partition the set

Let $\sim$ be an equivalence relation on a nonempty set $A$. Then the distinct equivalence classes form a *partition* of $A$: each class is nonempty, any two classes are either identical or disjoint, and the classes together cover $A$. Conversely, every partition of $A$ arises from exactly one equivalence relation, namely "$a \sim b$ iff $a$ and $b$ lie in the same piece."

**Proof 0.4.18**

*Direct Proof that Equivalence Classes Partition the Set.*

(1) Each class is nonempty and the classes cover $A$: reflexivity gives $a \sim a$, so $a \in [a]$; thus no class is empty, and every $a \in A$ sits in the class $[a]$, so the union of all classes is $A$.

(2) The key step is that two classes overlap only by coinciding. Suppose $[a] \cap [b] \neq \emptyset$ and pick $c$ in the intersection, so $c \sim a$ and $c \sim b$. For any $x \in [a]$ we have $x \sim a$; chaining with $a \sim c$ (symmetry) and $c \sim b$ (transitivity, twice) gives $x \sim b$, hence $x \in [b]$. So $[a] \subseteq [b]$, and the symmetric argument gives $[b] \subseteq [a]$; therefore $[a] = [b]$. Any two classes are thus equal or disjoint, and with the previous step the classes partition $A$.

(3) For the converse, let $\mathcal{P}$ be a partition—a family of nonempty, pairwise-disjoint subsets of $A$ with union $A$—and define $a \sim b$ to mean $a, b$ belong to a common piece $P \in \mathcal{P}$. This is reflexive (each $a$ lies in some piece, since the pieces cover $A$), symmetric (the condition is unordered in $a, b$), and transitive (if $a, b$ share a piece $P$ and $b, c$ share a piece $Q$, then $b \in P \cap Q$ forces $P = Q$ by disjointness, so $a, c \in P$). Its classes are exactly the pieces of $\mathcal{P}$, and no other equivalence relation yields this partition, since the relation is forced by "same piece."

■

[Direct] the whole proof runs on the three axioms of 0.4.16.

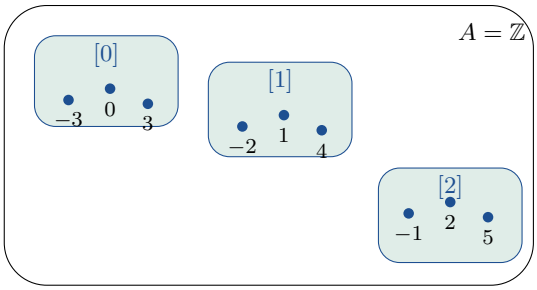


**Figure 0.4.19.** A partition into equivalence classes. The relation $\sim$ carves $A$ into non-overlapping cells, here the three residue classes $[0], [1], [2]$ of congruence modulo 3 on a patch of $\mathbb{Z}$. Every element sits in exactly one cell; the cells meet nowhere and together cover all of $A$.

**Remark 0.4.20**

*Why "well defined on classes" is the recurring worry*

Once a set is cut into classes, one constantly wants to define operations on the classes by working with a representative: "to add $[a]$ and $[b]$, add $a$ and $b$ and take $[a+b]$." The danger is that the answer might depend on *which* representatives you grabbed. Showing it does not—that $a \sim a'$ and $b \sim b'$ imply $a+b \sim a'+b'$, so $[a+b] = [a'+b']$—is the well-definedness check of 0.4.5, and it is unavoidable: skip it and the operation is simply not defined. Every quotient construction in 1.2—the integers from pairs of naturals, the rationals from pairs of integers—hinges on exactly this verification.

A bijection does something striking: it pairs the elements of two sets perfectly, one for one, with none left over on either side. That is precisely what it should mean for two sets to have *equally many* elements—and it is the only definition that survives the jump to infinite sets, where counting is impossible.

**Definition 0.4.21**

## Equinumerous sets; finite and infinite

Two sets $A$ and $B$ are *equinumerous* (have the *same cardinality*), written $A \approx B$, if there exists a bijection $f\colon A \to B$. A set $A$ is *finite* if $A \approx \{0, 1, \ldots, n-1\}$ for some $n \in \mathbb{N}$ (and then $A$ has $n$ elements), and *infinite* otherwise; here $n = 0$ gives the empty set $\{0, \ldots, -1\} = \emptyset$, so the empty set is finite with 0 elements, and $n = 1$ gives the one-element set $\{0\}$. Equinumerosity is itself reflexive, symmetric, and transitive—witnessed by the identity, the inverse of a bijection, and the composition of two bijections—so it behaves like an equivalence relation comparing sizes.

**Remark 0.4.22**

*The surprise of the infinite*

For *finite* sets this matches ordinary counting and a proper subset is always strictly smaller. Infinite sets break that intuition: the successor map $n \mapsto n+1$ from 0.4.11 is a bijection from $\mathbb{N}$ onto $\mathbb{N} \setminus \{0\}$, so an infinite set can be equinumerous with a proper subset of itself. This is not a paradox but the *definition* of infinite at work, and it opens the door to a genuine hierarchy of infinities—countable versus uncountable—which we develop in earnest in 2.1. We plant only the seed here.

**Definition 0.4.23**

## Partial and total order

A relation $\leq$ on a set $A$ is a *partial order* if it is reflexive, *antisymmetric* ($a \leq b$ and $b \leq a$ imply $a = b$), and transitive. It is a *total* (or *linear*) order if in addition any two elements are comparable: $\forall\, a, b \in A,\ (a \leq b \text{ or } b \leq a)$. The usual $\leq$ on $\mathbb{R}$ is a total order, and that comparability is exactly what makes the real line a *line*; the subset relation $\subseteq$ on the subsets of a set is a partial order that is not total, since $\{1\}$ and $\{2\}$ are incomparable. The order axioms of $\mathbb{R}$, and the supremum property that distinguishes it from $\mathbb{Q}$, are the subject of 1.3 and 1.5.

With relations and functions in hand—image and preimage, the injective/surjective/bijective trichotomy, composition and inverse, and the equivalence-class machinery—we have the vocabulary every later definition is phrased in. What remains is to learn to *wield* it: to turn these definitions into proofs. That craft is 0.5.

## 0.5 The Craft of Proof

Everything so far has been preparation. We fixed the language of statements (0.1), the quantifiers that turn open sentences into claims (0.2), and the sets and functions the claims are about (0.3, 0.4). Now we come to the act the whole course is built on: proving. A proof is not a different kind of writing reserved for geniuses; it is a disciplined habit of justifying every assertion, and it runs on a small, learnable stock of strategies—the very *Modes of Argument* tagged on every proof in this book. This section lays out that stock, one strategy at a time, each with a worked proof in the house style, and ends with the question every beginner actually asks: when you are staring at a blank page, how do you *find* the proof?

**Concept 0.5.1**

*What a proof is*

A *proof* of a statement $P$ is a finite chain of statements ending in $P$, in which every link is one of: an axiom, a definition, a hypothesis we are allowed to assume, a result proved earlier, or a statement that follows from earlier links by a valid rule of logic (0.1). *Rigour* means exactly that no link is skipped—a careful reader, granting only the axioms and definitions, can check each step without having to guess. The standard we hold to in this course is concrete: a proof is finished when a competent reader could read it line by line and object to nothing.

**Concept 0.5.2**

*Before you prove: name the hypotheses and the goal*

The most common reason a beginner is stuck is that they have not written down, precisely, what they may *assume* and what they must *show*. Do this first, and translate each into the language of 0.1–0.2 by *unfolding the definitions*. To prove "$f$ is injective," for instance, replace the word by its definition and you are no longer staring at a vague adjective but at a concrete target with a known shape (0.4):

$$\text{show:}\quad \forall x, y \in A,\quad f(x) = f(y) \;\Rightarrow\; x = y.$$

A universal goal tells you to fix an arbitrary $x, y$; the inner implication tells you to assume $f(x) = f(y)$ and drive toward $x = y$. Half of most proofs is just this honest restatement.

We now catalogue the strategies.[3] The first is the one every other strategy falls back on.

**Definition 0.5.3**

### Direct proof

A *direct proof* of an implication $P \Rightarrow Q$ assumes $P$ and reaches $Q$ by a forward chain of definitions and known results, with no special device. It is the default; reach for something cleverer only when the direct route stalls.

**Proof 0.5.3**

*Direct proof that the product of two odd integers is odd.*

[3] The worked examples lean on the elementary arithmetic of the integers, taken as known throughout: even and odd numbers, divisibility ($d \mid m$ means $m = dq$ for some integer $q$), prime and composite numbers, and the fact that every integer is even or odd.

(1) Suppose $m$ and $n$ are odd. By definition of oddness there are integers $j, k$ with $m = 2j + 1$ and $n = 2k + 1$.

(2) Multiply and regroup:

$$mn = (2j + 1)(2k + 1) = 4jk + 2j + 2k + 1 = 2(2jk + j + k) + 1.$$

(3) Since $2jk+j+k$ is an integer, $mn$ has the form 2(integer)+1, which is the definition of an odd integer. Hence $mn$ is odd.

■

[Direct]

**Definition 0.5.4**

## Proof by contrapositive

A *proof by contrapositive* of $P \Rightarrow Q$ proves the equivalent statement $\neg Q \Rightarrow \neg P$ instead (0.1.7): assume $\neg Q$ and derive $\neg P$. It is the right move when "$\neg Q$" is a more concrete handle than "$P$"—typically when $Q$ is itself a negation or an existence claim that is awkward to use directly.

**Proof 0.5.4**

*Proof by contrapositive that if $n^2$ is even then $n$ is even.*

(1) The hypothesis "$n^2$ even" is hard to use directly—it tells us little about $n$ itself. So we prove the contrapositive: *if $n$ is odd, then $n^2$ is odd.*

(2) Assume $n$ is odd, say $n = 2k + 1$. Then

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1,$$

which is odd.

(3) This establishes $\neg(n \text{ even}) \Rightarrow \neg(n^2 \text{ even})$, and by 0.1.7 that is logically the same as the claim "$n^2$ even $\Rightarrow$ $n$ even."

■

[A9]

**Definition 0.5.5**

## Proof by contradiction

A *proof by contradiction* of a statement $P$ assumes its negation $\neg P$ and derives an *absurdity*—some statement $R$ together with its negation $\neg R$. Since a true assumption can never lead to a contradiction, $\neg P$ must be false, so $P$ is true. It is the natural weapon against statements of the form "there is no ..." or "... is impossible."

**Proof 0.5.5**

*Proof by contradiction that $\sqrt{2}$ is irrational.*

(1) Suppose, for contradiction, that $\sqrt{2}$ is rational. Then $\sqrt{2} = p/q$ for integers $p, q$ with $q \neq 0$, and we may take the fraction in lowest terms, so that $p$ and $q$ are not both even.

(2) Squaring and clearing denominators, $p^2 = 2q^2$, so $p^2$ is even; by 0.5.4, $p$ is even, say $p = 2r$.

(3) Substitute: $4r^2 = 2q^2$, hence $q^2 = 2r^2$, so $q^2$ is even, and again by 0.5.4 $q$ is even.

(4) But now $p$ and $q$ are both even, contradicting the choice of lowest terms. The assumption was impossible, so $\sqrt{2}$ is irrational.

■

[A9]; the existence gap behind 1.4.

**Remark 0.5.6**

*Contrapositive or contradiction?*

The two are cousins, and beginners often blur them. A contrapositive proof is the disciplined special case: it proves $P \Rightarrow Q$ by assuming exactly $\neg Q$ and producing exactly $\neg P$—a single clean target. A contradiction proof is freer: it assumes $\neg P$ and may derive *any* absurdity at all. Prefer the contrapositive when your goal is an implication and the negated conclusion is the better foothold; save full contradiction for statements that are not implications, like an irrationality or a nonexistence. When a "contradiction" proof of $P \Rightarrow Q$ only ever uses $\neg Q$ to build $\neg P$, it was secretly a contrapositive—write it as one.

**Definition 0.5.7**

## Proof by cases, and "without loss of generality"

A *proof by cases* splits the hypothesis into finitely many exhaustive alternatives and proves the goal in each; since the cases cover every possibility, the goal holds always. When two cases are interchangeable—the argument for one becomes the argument for the other by renaming—we prove just one and write "*without loss of generality*" (WLOG) to record that the symmetry disposes of the rest.

**Proof 0.5.7**

*Proof by cases that $n^2 + n$ is even for every integer $n$.*

(1) Every integer is even or odd; take the two cases.

(2) If $n$ is even, $n = 2k$, then $n^2 + n = 4k^2 + 2k = 2(2k^2 + k)$ is even.

(3) If $n$ is odd, $n = 2k+1$, then $n^2+n = n(n+1) = (2k+1)(2k+2) = 2(2k+1)(k+1)$ is even.

(4) The two cases exhaust the integers, so $n^2 + n$ is even in all cases. (One could instead note $n^2 + n = n(n + 1)$ is a product of consecutive integers, one of which is even—a shorter route, but the case split is the method on display.)

■

[A12]

**Concept 0.5.8**

*Proving and disproving quantified statements*

The grammar of the goal dictates the proof's skeleton (0.2.4).

- To prove $\forall x \in D,\ P(x)$: write "*fix an arbitrary* $x \in D$" and argue for that nameless $x$, using nothing particular about it. To *dis*prove it, produce one *counterexample*—a single $x$ with $P(x)$ false.
- To prove $\exists x \in D,\ P(x)$: *construct* or exhibit a specific witness $x$ and check $P(x)$. To *dis*prove it, prove the universal $\forall x \in D,\ \neg P(x)$.

For example, $\forall n \in \mathbb{N},\ n^2 \geq n$ is proved by fixing an arbitrary $n$: if $n = 0$ it reads $0 \geq 0$; if $n \geq 1$ then multiplying $n \geq 1$ by $n \geq 0$ gives $n^2 \geq n$. By contrast "every prime is odd" is destroyed by the single counterexample $p = 2$.

**Concept 0.5.9**

*Proving "if and only if," and uniqueness*

A biconditional $P \Leftrightarrow Q$ is two implications (0.1.9), and a proof must supply *both*: the forward direction ($\Rightarrow$) and the backward direction ($\Leftarrow$), often by different strategies. Thus "$n$ is even iff $n^2$ is even" is a one-line direct argument in one direction ($n = 2k$ gives $n^2 = 2(2k^2)$, even) and the contrapositive of 0.5.4 in the other (an odd $n$ has an odd square); it is worked in full at 0.E.36. A *uniqueness* claim, "there is exactly one $x$ with $P(x)$" (0.2.9), is likewise two jobs: *existence* (exhibit one) and *uniqueness* (assume $P(x)$ and $P(y)$ and deduce $x = y$).

**Concept 0.5.10**

*Proving statements about sets*

Set claims reduce to logic about membership, and two patterns cover almost everything (0.3). To prove a containment $A \subseteq B$, "*fix* $x \in A$" and show $x \in B$ (*element-chasing*). To prove an equality $A = B$, prove $A \subseteq B$ and $B \subseteq A$ separately (*double inclusion*). For instance, transitivity of inclusion—if $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$—is one element-chase: fix $x \in A$; then $x \in B$ because $A \subseteq B$, and so $x \in C$ because $B \subseteq C$.

**Remark 0.5.11**

*Negate to discover what you must produce*

When a goal is itself a negation or a failure—"$f$ is *not* continuous," "the sequence does *not* converge," "no $x$ satisfies $P$"—do not argue in fog. Negate the definition mechanically by the rule of 0.2.5, flipping every quantifier, until the negation sits on a plain predicate; what remains is a positive thing to build. This is mode A11, and in analysis it is the difference between being lost and knowing exactly which $\varepsilon$, or which point, you are on the hook to produce (the worked negation of continuity is 0.E.8).

**Remark 0.5.12**

*The Modes of Argument, in one map*

The strategies above are the general-purpose core, and they are the front-matter Modes of Argument by another name: Direct (0.5.3), A9 contradiction and contrapositive (0.5.4, 0.5.5), A12 cases and WLOG (0.5.7), A11 negating a quantifier (0.5.11), and A10 induction, important enough to get its own treatment next (0.6). The remaining tags name the moves special to analysis, which the lectures will exemplify in place: A1 forcing a nonnegative quantity below every $\varepsilon$ to be zero, A2 and A3 the $\varepsilon$–$N$ and $\varepsilon$–$\delta$ arguments, A4 the triangle inequality with an added-and-subtracted middle term, A5

supremum and infimum arguments, A6 passing from an open cover to a finite subcover, A7 bisection and nested intervals, and A8 subsequence extraction and diagonalisation. Every one is a specialisation of the habits in this section; none is magic.

**Concept 0.5.13**

*How to find a proof when you are stuck*

Knowing the strategies is not the same as knowing which to use, and the honest answer is that finding a proof is a craft sharpened by practice, not a formula. Still, when the page is blank, this checklist almost always breaks the logjam.

(1) *Understand the statement exactly.* Unfold every definition and quantifier (0.5.2); write down precisely what is assumed and what is wanted. Most "hard" problems dissolve here.

(2) *Compute small and extreme cases.* Try $n = 0, 1, 2$; try the empty set; try the trivial function. Examples reveal the mechanism and often hand you the general argument.

(3) *Work from both ends.* Push forward from the hypotheses and backward from the goal until the two chains meet in the middle.

(4) *Find a relative.* Ask which theorem mentions *both* the hypothesis and the goal; recall a solved problem of the same shape and reuse its method.

(5) *Switch strategy deliberately.* If a universal resists a direct attack, try the contrapositive or contradiction; if you need existence, try to construct the object, or to derive an absurdity from its absence.

(6) *Separate finding from writing.* Discover the idea on scratch paper, then write the proof cleanly from the top—a finished proof rarely shows the false starts that produced it.

None of this substitutes for doing the work: as the epigraph insists, the only way to learn this is to prove things yourself. The exercises that follow are where the craft is actually acquired.

## 0.6 Mathematical Induction

A great many statements in this course read " $P(n)$ holds for every natural number $n$ "—a formula that sums the first $n$ integers, an inequality that holds for all $n$ past some point, a property shared by every member of an unending list. We cannot check infinitely many cases by hand, and 0.2.4 warned that for a universal statement no finite pile of examples will do. *Mathematical induction* is the engine built precisely for this situation: a single argument that, in two short moves, establishes $P(n)$ for all $n$ at once. It is mode A10, and it rests on one structural fact about the naturals, which we state first.

**Theorem 0.6.1**

### Well-ordering of the naturals

Every nonempty subset of $\mathbb{N}$ has a *least element*: if $S \subseteq \mathbb{N}$ and $S \neq \emptyset$, then there is some $m \in S$ with $m \leq s$ for every $s \in S$.

We take well-ordering as a defining feature of $\mathbb{N} = \{0, 1, 2, \dots\}$; later in the course the naturals are built instead from the successor and induction axioms (1.1), and well-ordering is then a theorem rather than a starting point.[4] What makes it powerful is that it forbids an infinite *descent*: you cannot keep stepping to a strictly smaller natural number forever, because any set of the numbers you would visit would have a bottom. That single prohibition is exactly what licenses induction.

**Theorem 0.6.2**

### The principle of mathematical induction

Fix an integer $n_0$, and let $P(n)$ be a predicate defined for every integer $n \geq n_0$. Suppose

- *(base case)* $P(n_0)$ is true; and
- *(inductive step)* for every integer $k \geq n_0$, the implication $P(k) \Rightarrow P(k+1)$ is true.

Then $P(n)$ is true for every integer $n \geq n_0$.

The picture to hold in your head is a line of dominoes. The base case is your hand knocking over the first one; the inductive step is the guarantee that each domino, when it falls, topples its neighbour. Grant both and every domino falls, however long the line—not because you pushed each one, but because the two moves together force the whole cascade. The inductive step does *not* assert $P(k)$; it only promises the link from $P(k)$ to $P(k+1)$, exactly the conditional promise of 0.1.6. The assumption "$P(k)$ is true," made temporarily inside the step so as to reach $P(k+1)$, has a name worth knowing.

**Concept 0.6.3**

*The inductive hypothesis*

Inside the inductive step you fix an arbitrary $k \geq n_0$ and *assume* $P(k)$; this working assumption is the *inductive hypothesis*. Your task in the step is to use it to derive $P(k+1)$. It is not something

[4] The same statement is false for $\mathbb{Z}$ (which has no least element) and for the nonnegative rationals (the set of positive rationals has no least element—between any two there is another). Well-ordering is special to $\mathbb{N}$.

you are claiming outright—it is the antecedent of the conditional you are proving, granted to you for the length of the step and discharged the moment you reach the conclusion. A proof by induction therefore has a fixed two-part shape: verify the base case outright, then prove the conditional "if $P(k)$ then $P(k+1)$" for an arbitrary $k$.

Why is the principle true? Well-ordering supplies a clean answer through the back door: if induction could fail, a *least* failure would have to exist, and we show it cannot.

**Proof 0.6.2**

*Proof that well-ordering implies the principle of induction.*

(1) Suppose, for contradiction, that the base case and inductive step both hold yet $P(n)$ fails for some integer $n \geq n_0$. Collect the failures into

$$S = \{\, n \in \mathbb{Z} : \ n \geq n_0 \text{ and } P(n) \text{ is false} \,\}.$$

The shift $n \mapsto n - n_0$ carries $S$ onto a subset of $\mathbb{N}$, and it preserves order, so a least element of $S$ corresponds to a least element of that image and vice versa. By assumption $S$ is nonempty, hence so is its image; well-ordering (0.6.1) gives the image a least element, and pulling back, $S$ itself has a least element $m$.

(2) The base case says $P(n_0)$ is true, so $m \neq n_0$; hence $m > n_0$, and $m-1$ is an integer with $m - 1 \geq n_0$. Because $m$ is the *least* member of $S$, the smaller number $m - 1$ is not in $S$, so $P(m-1)$ is true.

(3) Apply the inductive step with $k = m - 1$: from $P(m-1)$ true we get $P(m)$ true. But $m \in S$ means $P(m)$ is false—a contradiction.

(4) No least failure can exist, so $S$ is empty: $P(n)$ holds for every integer $n \geq n_0$.

■

[A9] via a least counterexample.

This is one of two honest routes to the same principle. Here well-ordering is the given and induction is the theorem; when the naturals are constructed later (1.1), it is induction that is taken as an axiom and well-ordering that is derived. The two derivations run in opposite directions and neither is circular—they simply choose different members of the same family (0.6.13) as the foundation. With the principle secured, the rest of the section is practice—and induction is a craft learned only by watching it run and then running it yourself. We begin with the identity that is, by tradition, everyone's first.

**Proposition 0.6.4**

## The sum of the first $n$ integers

For every integer $n \geq 1$,

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

**Proof 0.6.4**

*Proof by Induction on $n$ of the closed form for $1 + \cdots + n$.*

(1) Write $P(n)$ for the equation $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$, to be proved for all $n \geq 1$. For the base case $n = 1$ the left side is 1 and the right side is $\frac{1 \cdot 2}{2} = 1$, so $P(1)$ holds.

(2) Fix an arbitrary $k \geq 1$ and assume the inductive hypothesis $P(k)$:

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

To reach $P(k+1)$, add the next term $k+1$ to both sides:

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

(3) The right-hand end is $\frac{(k+1)\big((k+1)+1\big)}{2}$, which is exactly the statement $P(k+1)$. Thus $P(k) \Rightarrow P(k+1)$ for every $k \geq 1$, and by 0.6.2 the identity holds for all $n \geq 1$.

■

[A10] cf. the Gauss pairing picture of 1.1.

**Remark 0.6.5**

*What induction proves and what it hides*

The proof above is airtight, yet it gives no hint of *where* the formula $\frac{n(n+1)}{2}$ came from—induction verifies a guess but never produces one. The young Gauss is said to have found it by pairing $1+2+\cdots+n$ with the same sum written backwards, $n + (n-1) + \cdots + 1$; the $n$ columns each total $n+1$, so twice the sum is $n(n+1)$. That argument is the rectangle picture you will meet later (1.1): two copies of the staircase $1 + 2 + \cdots + n$ interlock into an $n \times (n+1)$ grid. The picture *discovers* the answer; induction then *certifies* it. Keep both in view: the explanatory argument tells you why, the induction tells you that it never fails.

The next two are run with less commentary; the shape is by now the point. Watch how each inductive step reduces the case $k+1$ to the case $k$ by isolating a single extra term.

**Proposition 0.6.6**

## Two further identities

For every integer $n \geq 1$,

**(a)** $1 + 3 + 5 + \cdots + (2n-1) = n^2$, **(b)** $1 + 2 + 2^2 + \cdots + 2^{n-1} = 2^n - 1$.

**Proof 0.6.6**

*Proof by Induction of the odd-number and geometric sums.*

(1) For **(a)**, let $P(n)$ be "$1 + 3 + \cdots + (2n-1) = n^2$." The base case $n = 1$ reads $1 = 1^2$, true. Assume $P(k)$, namely $1 + 3 + \cdots + (2k-1) = k^2$; the $(k+1)$st odd

number is $2(k+1)-1 = 2k+1$, so

$$1 + 3 + \cdots + (2k-1) + (2k+1) = k^2 + (2k+1) = (k+1)^2,$$

which is $P(k+1)$. Hence (a) holds for all $n \geq 1$.

(2) For **(b)**, let $Q(n)$ be "$1 + 2 + \cdots + 2^{n-1} = 2^n - 1$." The base case $n = 1$ reads $1 = 2^1 - 1$, true. Assume $Q(k)$; the next term is $2^k$, so

$$(1 + 2 + \cdots + 2^{k-1}) + 2^k = (2^k - 1) + 2^k = 2 \cdot 2^k - 1 = 2^{k+1} - 1,$$

which is $Q(k+1)$. Hence (b) holds for all $n \geq 1$. The pattern in (a) is worth a second look: the running totals $1, 4, 9, 16, \ldots$ of consecutive odd numbers are exactly the perfect squares.

■

[A10]

Induction is not confined to equalities. An *inequality* that holds from some point on is proved the same way, with the inductive step doing a little estimation rather than exact algebra. The next result also shows why the base case need not be $n = 0$ or $n = 1$: the inequality is simply false for small $n$, so we start where it first becomes true. (The gentlest such fact is $2^n > n$, true for every $n \in \mathbb{N}$ and a clean first exercise; we prove the harder $2^n > n^2$, which needs a later starting point.)

**Proposition 0.6.7**

## An exponential outgrows a square

For every integer $n \geq 5$, $2^n > n^2$.

**Proof 0.6.7**

*Proof by Induction of* $2^n > n^2$ *for* $n \geq 5$.

(1) Let $P(n)$ be "$2^n > n^2$." Small values fail—$2^4 = 16 = 4^2$ is not strict, and $2^3 = 8 < 9$; the inequality first holds at $n = 5$, where $2^5 = 32 > 25 = 5^2$. So the base case is $P(5)$.

(2) Fix $k \geq 5$ and assume $P(k)$: $2^k > k^2$. Doubling, $2^{k+1} = 2 \cdot 2^k > 2k^2$. It now suffices to show $2k^2 \geq (k+1)^2$, for then $2^{k+1} > 2k^2 \geq (k+1)^2$ and $P(k+1)$ follows.

(3) Expanding, $2k^2 \geq (k+1)^2$ is the same as $k^2 \geq 2k + 1$. Since $k \geq 5$ we have $k^2 \geq 5k = 2k + 3k > 2k + 1$, so the needed inequality holds.

(4) Chaining the two estimates gives $2^{k+1} > (k+1)^2$, which is $P(k+1)$. By 0.6.2, $2^n > n^2$ for all $n \geq 5$.

■

[A10] the base case is $n_0 = 5$, not 0.

A divisibility statement is induction in yet another costume. Here "$d$ divides $m$," written $d \mid m$, means $m = d \cdot q$ for some integer $q$. The trick in the step is always to write the $(k+1)$st quantity in terms of the $k$th plus a remainder you can see is divisible.

**Proposition 0.6.8**

## A divisibility fact

For every $n \in \mathbb{N}$, $3 \mid (n^3 - n)$.

**Proof 0.6.8**

*Proof by Induction that* $3 \mid (n^3 - n)$.

(1) Let $P(n)$ be "$3 \mid (n^3 - n)$." The base case $n = 0$ gives $0^3 - 0 = 0 = 3 \cdot 0$, divisible by 3, so $P(0)$ holds.

(2) Fix $k \geq 0$ and assume $P(k)$: there is an integer $q$ with $k^3 - k = 3q$. Expand the next quantity and group it around $k^3 - k$:

$$(k+1)^3 - (k+1) = \big(k^3 + 3k^2 + 3k + 1\big) - (k+1) = \big(k^3 - k\big) + 3\big(k^2 + k\big).$$

(3) The first bracket is $3q$ by hypothesis and the second is $3(k^2 + k)$, so

$$(k+1)^3 - (k+1) = 3q + 3\big(k^2 + k\big) = 3\big(q + k^2 + k\big),$$

a multiple of 3. Thus $P(k+1)$ holds, and by 0.6.2 the claim holds for every $n \in \mathbb{N}$. ■

[A10]

Each proof so far reached $P(k+1)$ from its *immediate* predecessor $P(k)$. Sometimes one step back is not enough—the case $n$ naturally breaks into pieces that are *several*, or an unknown number of, steps smaller. For these we need a sturdier form that hands us *all* earlier cases at once.

**Theorem 0.6.9**

## Strong (complete) induction

Fix an integer $n_0$ and let $P(n)$ be a predicate for $n \geq n_0$. Suppose that for every integer $k \geq n_0$,

$$\Big(P(j) \text{ holds for all } j \text{ with } n_0 \leq j < k\Big) \implies P(k).$$

Then $P(n)$ holds for every integer $n \geq n_0$. (Taking $k = n_0$, there are no integers $j$ with $n_0 \leq j < n_0$, so the antecedent is the empty conjunction—vacuously true (0.1.6)—and the implication forces $P(n_0)$ outright, so the base case is genuinely built in.)

**Remark 0.6.10**

*When you need the strong form*

The only difference from 0.6.2 is the inductive hypothesis: ordinary induction lends you $P(k)$, strong induction lends you the entire run $P(n_0), \ldots, P(k)$. Reach for the strong form whenever building case

$k+1$ sends you back to a case that is *not* the immediate predecessor—a recursion like $a_n = a_{n-1}+a_{n-2}$ that looks two steps back, or an argument that factors $k+1$ into smaller pieces of unpredictable size. The two principles are not rivals: anything provable one way is provable the other, and strong induction is itself a theorem of well-ordering by the same least-counterexample argument as 0.6.2. Use whichever makes the step honest.

The classic place where one step back fails is factoring a number into primes: knowing that $k$ has a prime factorization tells you nothing about $k+1$, but breaking a composite $k+1 = ab$ sends you to the *smaller* factors $a$ and $b$, and those are the cases strong induction makes available.

**Theorem 0.6.11**

## Existence of prime factorizations

Every integer $n \geq 2$ is a product of (one or more) prime numbers.

**Proof 0.6.11**

*Proof by Strong Induction of the existence of a prime factorization.*

(1) Let $P(n)$ be "$n$ is a product of primes," to be proved for all $n \geq 2$; here a single prime counts as a product of one factor. Fix $k \geq 2$ and assume the strong inductive hypothesis: $P(j)$ holds for every $j$ with $2 \leq j < k$. We must prove $P(k)$.

(2) Split into two cases. If $k$ is prime, then $k$ is itself a product of one prime and $P(k)$ holds with nothing further to do.

(3) If $k$ is not prime, then by definition $k = a \cdot b$ for some integers $a, b$ with $2 \leq a < k$ and $2 \leq b < k$. Both $a$ and $b$ are smaller than $k$ and at least 2, so the inductive hypothesis applies to each: $a$ is a product of primes and $b$ is a product of primes.

(4) Concatenating those two lists of prime factors expresses $k = a \cdot b$ as a product of primes, so $P(k)$ holds. In either case $P(k)$ follows from the cases below it, and by 0.6.9 every integer $n \geq 2$ has a prime factorization.

■

[A10+A12]

**Remark 0.6.12**

*Ordinary induction would stall here*

Try to run 0.6.11 with the ordinary form and you will feel the wall: to factor $k+1$ you would need a factorization of $k$, but there is no way to turn one into the other—$k$ and $k+1$ share no factors. The honest reduction is to the divisors $a, b$ of $k+1$, whose only guaranteed property is that they are *smaller*. That is precisely the gap strong induction fills, and recognising it is the whole skill: when the natural sub-problem is "some smaller case," not "the previous case," use 0.6.9.

Three principles—ordinary induction, strong induction, and well-ordering—keep reappearing, and it is worth knowing they are interchangeable.

**Remark 0.6.13**

*Three statements of one idea*

Over the naturals, well-ordering (0.6.1), the principle of induction (0.6.2), and strong induction (0.6.9) are *logically equivalent*: assume any one and you can derive the other two. We have already gone halfway—well-ordering gave us induction (0.6.2) and strong induction (0.6.10); the return trip, deriving well-ordering from induction, is set as 0.E.46. So the choice among them is one of convenience, never of strength. A proof that "descends to a smaller counterexample" (well-ordering), one that "adds one to climb" (induction), and one that "reduces to smaller pieces" (strong induction) are three dialects of the same underlying fact about $\mathbb{N}$.

Induction is delicate in one specific way, and the failure mode is worth meeting head-on, because it is invisible until you look for it: *a flawless inductive step proves nothing without a true base case*, and a step that quietly fails at one early value sinks the whole argument. The most famous illustration is a deliberately false "theorem."

**Counterexample 0.6.14**

## All horses are the same colour

*False claim.* In any group of $n$ horses, all $n$ have the same colour. The bogus "induction" runs as follows. Base case $n = 1$: a single horse trivially matches itself. Inductive step: assume any $k$ horses share a colour, and take a group of $k + 1$ horses $h_1, \ldots, h_{k+1}$. The first $k$ of them, $h_1, \ldots, h_k$, are a group of $k$, hence one colour; the last $k$ of them, $h_2, \ldots, h_{k+1}$, are also a group of $k$, hence one colour. The two overlapping groups force all $k + 1$ horses to the common colour—"therefore" all horses are the same colour.

FAILS: The inductive step is valid for every $k \geq 2$ but *breaks at* $k = 1$: passing from 1 horse to 2, the two groups of size $k = 1$ are $\{h_1\}$ and $\{h_2\}$, which do *not overlap*, so nothing links the colour of $h_1$ to that of $h_2$. The chain $P(1) \Rightarrow P(2)$ is the one missing link, and with it gone the dominoes past the first never fall.

**Remark 0.6.15**

*The lesson: check the step at the very first transition*

The horse argument is seductive precisely because the inductive step *looks* uniform—it seems to work "for all $k$"—while in truth it silently requires the two sub-groups to overlap, which needs $k \geq 2$. The argument proves $P(k) \Rightarrow P(k + 1)$ for $k \geq 2$ and proves $P(1)$, but it never proves $P(1) \Rightarrow P(2)$, so the cascade is severed at the start. Two habits inoculate you. First, always verify the base case explicitly; an induction with a false or missing base proves nothing (the step "$P(k) \Rightarrow P(k+1)$ for all $k$" is consistent with $P$ being false everywhere). Second, test the inductive step at its *first* instance—here $k = 1$—where hidden size assumptions surface. Most flawed inductions die at exactly that first transition.

A picture makes the mechanism plain: the base case lights the first domino, the step is the spacing that lets each fall onto the next, and a single missing tile—like the broken $P(1) \Rightarrow P(2)$ above—halts the cascade.

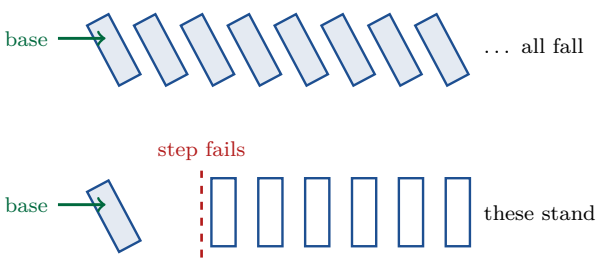


**Figure 0.6.16.** The domino cascade, and the gap that stops it. Top: base case plus uniform step topple the whole line. Bottom: the step fails at the very first transition, so every later domino stands.

With the mechanism, the two forms, and the pitfall in hand, you have mode A10 in full. The exercises that follow drill the shape on identities, inequalities, divisibility, and a recursion where only the strong form will do; treat the first few as warm-ups and the last as the real test of whether you have internalised *which* earlier case the step truly needs.

# 0.E Exercises

These are the foundations exercises, gathered here and grouped by topic. Each is worked in full; treat the solution as a model of how much detail a written proof is expected to carry, but try every problem yourself before reading on—reading a solution is no substitute for the struggle that makes it stick.

### Statements and logic

**Exercise 0.E.1** [excluded middle]

Prove that $P \vee \neg P$ is true regardless of the truth value of $P$. (This law is called the *law of the excluded middle*.)

SOLUTION.

Whatever value $P$ takes, exactly one of $P$ and $\neg P$ is true, so their disjunction has a true disjunct and is therefore true. The truth table records both cases:

| $P$ | $\neg P$ | $P \vee \neg P$ |
|---|---|---|
| T | F | T |
| F | T | T |

The final column is T in every row, so $P \vee \neg P$ is true for all $P$. A statement true under every assignment of truth values to its parts, like this one, is called a *tautology*.

■

**Exercise 0.E.2** [contrapositive]

Show that an implication and its contrapositive are logically equivalent: $P \Rightarrow Q$ and $\neg Q \Rightarrow \neg P$ have the same truth value in every case.

SOLUTION.

Compare the two final columns:

| $P$ | $Q$ | $P \Rightarrow Q$ | $\neg Q \Rightarrow \neg P$ | agree? |
|---|---|---|---|---|
| T | T | T | T | ✓ |
| T | F | F | F | ✓ |
| F | T | T | T | ✓ |
| F | F | T | T | ✓ |

For $\neg Q \Rightarrow \neg P$: it is false only when its hypothesis $\neg Q$ is true and its conclusion $\neg P$ is false, that is, when $Q$ is false and $P$ is true—exactly the one case where $P \Rightarrow Q$ is false. The two columns therefore agree in all four rows, so the statements are logically equivalent. This is what licenses proving "if $P$ then $Q$" by instead assuming $\neg Q$ and deriving $\neg P$ (0.5).

■

**Exercise 0.E.3** [De Morgan for connectives]

Prove that $\neg(P \wedge Q)$ and $\neg P \vee \neg Q$ are logically equivalent, and state the companion law for $\neg(P \vee Q)$.

Solution.

The two are equivalent; compare the third and sixth columns.

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

They agree in every row, so $\neg(P \wedge Q) \equiv \neg P \vee \neg Q$: the negation of "both" is "at least one fails." The companion law is $\neg(P \vee Q) \equiv \neg P \wedge \neg Q$, the negation of "at least one" being "both fail." These are the logical source of the set-theoretic De Morgan laws of 0.3.14.

■

**Exercise 0.E.4** [implication as "not-or"]

Show that $P \Rightarrow Q$ is logically equivalent to $\neg P \vee Q$.

Solution.

Equivalent, by the truth table.

| $P$ | $Q$ | $P \Rightarrow Q$ | $\neg P \vee Q$ |
|---|---|---|---|
| T | T | T | T |
| T | F | F | F |
| F | T | T | T |
| F | F | T | T |

The two final columns match in all four rows. The equivalence is worth keeping: an implication asserts nothing more than "the hypothesis fails or the conclusion holds," which is why a false hypothesis makes $P \Rightarrow Q$ true outright—the vacuous truth of 0.1.6 read straight off the disjunction. Negating both sides gives $\neg(P \Rightarrow Q) \equiv P \wedge \neg Q$: an implication fails exactly when its hypothesis holds and its conclusion does not.

■

**Exercise 0.E.5** [converse and inverse]

Show that the converse $Q \Rightarrow P$ and the inverse $\neg P \Rightarrow \neg Q$ of an implication $P \Rightarrow Q$ are logically equivalent to each other. Give an example where the original is true yet both fail.

SOLUTION.

The inverse is the contrapositive of the converse: contraposing $Q \Rightarrow P$ swaps and negates its parts to give $\neg P \Rightarrow \neg Q$, and a statement and its contrapositive always agree (0.1.7). So converse and inverse share a truth value in every case—which is why the warning against "assuming the converse" is the same warning against the inverse.

For the example, let $P$ be "$n$ is a multiple of 4" and $Q$ be "$n$ is even." Then $P \Rightarrow Q$ is true, the converse "every even $n$ is a multiple of 4" is false ($n = 6$), and so its equivalent inverse "if $n$ is not a multiple of 4 then $n$ is odd" is false as well ($n = 6$ again). The original can hold while both converse and inverse fail.

■

**Exercise 0.E.6** [necessary and sufficient]

Rewrite each as an implication and decide whether it is true: (a) "$6 \mid n$ is sufficient for $n$ to be even"; (b) "$n$ being even is necessary for $6 \mid n$."

SOLUTION.

Both encode the same true implication $6 \mid n \Rightarrow 2 \mid n$. By 0.1.9, "$A$ is sufficient for $B$" means $A \Rightarrow B$, so (a) is "$6 \mid n \Rightarrow n$ even"; and "$B$ is necessary for $A$" also means $A \Rightarrow B$ (without $B$, $A$ cannot hold), so (b) is again "$6 \mid n \Rightarrow n$ even." The implication is true: if $n = 6k$ then $n = 2(3k)$ is even. The point is that "sufficient" and "necessary" name the two ends of one arrow, and reading the arrow the right way round is half of reading a theorem.

■

## Quantifiers

**Exercise 0.E.7** [order of quantifiers]

For the predicate $P(x, y)$ given by "$x + y = 0$" on $\mathbb{R}$, decide the truth value of each of $\forall x\, \exists y\, P(x, y)$ and $\exists y\, \forall x\, P(x, y)$, with proof.

SOLUTION.

The first is true and the second is false.

For $\forall x\, \exists y\, (x + y = 0)$: fix an arbitrary $x \in \mathbb{R}$ and take $y = -x$; then $x + y = x + (-x) = 0$, so the inner existential holds. Since $x$ was arbitrary, the universal holds.

For $\exists y\, \forall x\, (x + y = 0)$: suppose some fixed $y \in \mathbb{R}$ satisfied $x + y = 0$ for every $x$. Taking $x = 0$ forces $y = 0$; taking $x = 1$ then forces $1 + 0 = 0$, which is false. No such $y$ exists, so

the statement is false. The two statements differ only in the order of the quantifiers, and that reversal flips the truth value—exactly the phenomenon of 0.2.7.

■

**Exercise 0.E.8** [negating a definition]

Using only the mechanical rule of 0.2.5, write the negation of

$$\forall\, \varepsilon > 0,\ \ \exists\, \delta > 0,\ \ \forall x,\ \ \big(|x - a| < \delta \ \Rightarrow\ |f(x) - f(a)| < \varepsilon\big),$$

moving every negation inward until it sits on the innermost predicate.

Solution.

Sweep left to right, flipping each quantifier, and finally negate the implication. The negation of an implication $A \Rightarrow B$ is $A \wedge \neg B$—it fails exactly when the hypothesis holds and the conclusion does not (0.1.5)—so $\neg(|x - a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon)$ becomes $|x - a| < \delta \ \wedge\ |f(x) - f(a)| \geq \varepsilon$. Hence the negation is

$$\exists\, \varepsilon > 0,\ \ \forall\, \delta > 0,\ \ \exists x,\ \ \big(|x - a| < \delta \ \wedge\ |f(x) - f(a)| \geq \varepsilon\big).$$

In words: some $\varepsilon > 0$ resists every $\delta$—for each $\delta$ there is a point within $\delta$ of $a$ whose image is at least $\varepsilon$ away from $f(a)$. This is precisely what it means for $f$ to be *discontinuous* at $a$, and we obtained it with no picture at all, purely by the negation rule.

■

**Exercise 0.E.9** [negation and counterexample]

Write the negation of "$\forall n \in \mathbb{N},\ (n \text{ is prime} \Rightarrow n \text{ is odd})$," and decide whether the statement or its negation is true.

Solution.

The negation is $\exists n \in \mathbb{N},\ (n \text{ is prime and } n \text{ is even})$, and *it* is the true one. Negating the universal turns it existential and negates the inside (0.2.5); the inner $\neg(P \Rightarrow Q)$ is $P \wedge \neg Q$ (0.1.5), here "$n$ prime and $n$ not odd," i.e. prime and even. The witness is $n = 2$: prime and even, so the negation holds and the original universal is false. A single even prime settles it—the counterexample pattern of 0.2.4.

■

**Exercise 0.E.10** [unique existence]

Prove that there is exactly one positive real number $x$ with $x^3 = x$.

Solution.

The unique such $x$ is 1; existence and uniqueness are separate jobs (0.2.9). Existence: $1^3 = 1$, so $x = 1$ works. Uniqueness: if $x > 0$ and $x^3 = x$, then $x^3 - x = x(x-1)(x+1) = 0$, so $x \in \{0, 1, -1\}$, of which only 1 is positive. Hence $x = 1$ is the sole positive solution, and $\exists!\, x > 0,\ x^3 = x$.

■

**Exercise 0.E.11** [quantifier order]

Decide, with proof, the truth value of each (taking $n \geq 1$): (a) $\forall \varepsilon > 0,\ \exists n \in \mathbb{N},\ \frac{1}{n} < \varepsilon$; (b) $\exists n \in \mathbb{N},\ \forall \varepsilon > 0,\ \frac{1}{n} < \varepsilon$.

SOLUTION.

Statement (a) is true and (b) is false—the same symbols in the opposite order.

For (a), fix an arbitrary $\varepsilon > 0$; by the Archimedean property (1.7) there is an integer $n \geq 1$ with $n > 1/\varepsilon$, and then $\frac{1}{n} < \varepsilon$. The witness $n$ may depend on $\varepsilon$, which is the whole point (0.2.8).

For (b), one $n$ would have to serve every $\varepsilon > 0$ at once. Given any fixed $n \geq 1$, take $\varepsilon = \frac{1}{n} > 0$; then $\frac{1}{n} < \varepsilon$ reads $\frac{1}{n} < \frac{1}{n}$, false. So no $n$ survives and (b) fails. Reversing the quantifiers turned a truth into a falsehood (0.2.7)—the structure underneath every $\varepsilon$–$N$ argument to come.

■

**Exercise 0.E.12** [negating boundedness]

A sequence $(a_n)$ is *bounded* if $\exists M > 0,\ \forall n,\ |a_n| \leq M$. Write, by the mechanical rule, what it means for $(a_n)$ to be *un*bounded.

SOLUTION.

Unbounded means $\forall M > 0,\ \exists n,\ |a_n| > M$. Negating the definition flips each quantifier and negates the inside (0.2.5): $\neg\exists M$ becomes $\forall M$, $\neg\forall n$ becomes $\exists n$, and $\neg(|a_n| \leq M)$ is $|a_n| > M$. In words: no bound $M$ works, because for every proposed $M$ some term overshoots it. This is the same mechanical negation that unfolds the failure of any definition built from stacked quantifiers.

■

## Sets

**Exercise 0.E.13** [membership vs. subset]

Decide, with a one-line reason for each, whether the following are true or false: (a) $2 \in \{1, 2, 3\}$; (b) $\{2\} \in \{1, 2, 3\}$; (c) $\{2\} \subseteq \{1, 2, 3\}$; (d) $\varnothing \in \{1, 2, 3\}$; (e) $\varnothing \subseteq \{1, 2, 3\}$; (f) $2 \subseteq \{1, 2, 3\}$.

Solution.

The verdicts are: (a) true, (b) false, (c) true, (d) false, (e) true, (f) ill-formed—not a true-or-false statement at all.

For (a), 2 is one of the listed members, so $2 \in \{1, 2, 3\}$. For (b), the elements of $\{1, 2, 3\}$ are the numbers 1, 2, 3; the *set* $\{2\}$ is not among them, so $\{2\} \notin \{1, 2, 3\}$. For (c), $\{2\} \subseteq \{1, 2, 3\}$ asks whether every element of $\{2\}$ lies in $\{1, 2, 3\}$; the only element is 2, which does, so the inclusion holds. For (d), $\varnothing$ is not one of the listed members $1, 2, 3$, so $\varnothing \notin \{1, 2, 3\}$. For (e), $\varnothing \subseteq \{1, 2, 3\}$ is true by 0.3.8: the empty set is a subset of every set. For (f), "$2 \subseteq \{1, 2, 3\}$" compares a number against a set with $\subseteq$, which only relates a set to a set; 2 is not a set, so the statement is malformed—it has no truth value, and "ill-formed" is itself the answer. The whole point of the exercise is the $\in$ versus $\subseteq$ distinction of 0.3.17: $\in$ asks for membership, $\subseteq$ asks that every member be shared.

■

**Exercise 0.E.14** [vacuous truth]

Prove that for every $x \in \varnothing$, one has $x^2 = 9$.

Solution.

The statement is true, vacuously. Written out, the claim is the universal implication $\forall x,\ (x \in \varnothing \Rightarrow x^2 = 9)$. Fix any $x$. Its hypothesis $x \in \varnothing$ is false, because the empty set has no elements (0.3.4), so the implication is true by vacuous truth (0.1.6)—there is no $x$ in $\varnothing$ that could make it fail. Since $x$ was arbitrary, the universal statement holds. Nothing about the number 9 entered the argument: the same proof shows every element of $\varnothing$ has any property whatsoever, which is exactly why $\varnothing \subseteq A$ for all $A$.

■

**Exercise 0.E.15** [empty set in a power set]

Let $S = \{\varnothing, \{\varnothing\}\}$. Determine $|S|$, list $\mathcal{P}(S)$ in full, and state $|\mathcal{P}(S)|$.

Solution.

$S$ has two elements, so $|S| = 2$ and $|\mathcal{P}(S)| = 2^2 = 4$.

The two elements of $S$ are the empty set $\varnothing$ and the one-element set $\{\varnothing\}$; these are distinct, since the first has no elements and the second has exactly one (0.3.17), so $|S| = 2$. The subsets of $S$ are the empty set, the two singletons, and $S$ itself:

$$\mathcal{P}(S) = \Big\{\ \varnothing,\ \{\varnothing\},\ \{\{\varnothing\}\},\ \{\varnothing, \{\varnothing\}\}\ \Big\}.$$

This has 4 elements, matching $2^{|S|} = 2^2$ from 0.3.16. The first two entries deserve a glance: $\varnothing$ appears *as a subset* of $S$ (so $\varnothing \in \mathcal{P}(S)$), while $\{\varnothing\}$ appears once as an *element* of $S$

and again, wrapped in braces as $\{\{\varnothing\}\}$, as a singleton subset—the nesting is genuine, not a typo.

■

**Exercise 0.E.16** [$\varnothing$ as a power-set member]

Prove that $\varnothing \in \mathcal{P}(S)$ for every set $S$.

SOLUTION.

The statement holds for every $S$. By definition of the power set, $\varnothing \in \mathcal{P}(S)$ means exactly $\varnothing \subseteq S$ (0.3.15)—the elements of $\mathcal{P}(S)$ are precisely the subsets of $S$. And $\varnothing \subseteq S$ holds for every set $S$ by 0.3.8: every element of the empty set lies in $S$, vacuously, since there are no elements of the empty set to check (0.1.6). Therefore $\varnothing \in \mathcal{P}(S)$. The exercise is really 0.3.17 in action: the subset fact about $\varnothing$ becomes a membership fact about $\mathcal{P}(S)$.

■

**Exercise 0.E.17** [absorbing/identity laws]

Let $A$ be any set. Prove that $A \cap \varnothing = \varnothing$ and $A \cup \varnothing = A$.

SOLUTION.

Both identities hold for every $A$, and each is proved by double inclusion (0.3.7).

For $A \cap \varnothing = \varnothing$: the inclusion $\varnothing \subseteq A \cap \varnothing$ is automatic from 0.3.8. Conversely, fix $x \in A \cap \varnothing$; then $x \in \varnothing$, which is impossible, so there is no such $x$ and $A \cap \varnothing \subseteq \varnothing$ holds vacuously. Both inclusions give $A \cap \varnothing = \varnothing$.

For $A \cup \varnothing = A$: fix $x \in A \cup \varnothing$. Then $x \in A$ or $x \in \varnothing$; the second disjunct is impossible, so $x \in A$, giving $A \cup \varnothing \subseteq A$. Conversely, if $x \in A$ then $x \in A$ or $x \in \varnothing$, so $x \in A \cup \varnothing$, giving $A \subseteq A \cup \varnothing$. Both inclusions give $A \cup \varnothing = A$. (Velleman §1.4 collects these among the basic set identities.)

■

**Exercise 0.E.18** [distributive law]

Prove the distributive law $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ for all sets $A$, $B$, $C$.

SOLUTION.

The identity holds, and we prove it by double inclusion (0.3.7), translating the distributive law for "and" over "or" from 0.1.

For $\subseteq$, fix $x \in A \cap (B \cup C)$. Then $x \in A$, and $x \in B \cup C$, so $x \in B$ or $x \in C$. In the first case $x \in A$ and $x \in B$, so $x \in A \cap B$; in the second $x \in A$ and $x \in C$, so $x \in A \cap C$. Either

way

$$x \in (A \cap B) \cup (A \cap C),$$

so $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

For $\supseteq$, fix $x \in (A \cap B) \cup (A \cap C)$, so $x \in A \cap B$ or $x \in A \cap C$. In both cases $x \in A$, and in the first $x \in B$ while in the second $x \in C$, so in either case $x \in B$ or $x \in C$, i.e. $x \in B \cup C$. Hence $x \in A$ and $x \in B \cup C$, that is $x \in A \cap (B \cup C)$, giving $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. Both inclusions hold, so the sets are equal. The engine throughout is the logical equivalence "$P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$," which one reads straight off the truth tables of 0.1.3; the set proof is its faithful shadow.

■

**Exercise 0.E.19** [subset and complement]

Let $A, B$ be subsets of a universe $U$. Prove that $A \subseteq B$ if and only if $B^c \subseteq A^c$.

Solution.

The biconditional holds; we prove both directions, and each is a contrapositive in disguise.

Assume $A \subseteq B$, and fix $x \in B^c$, so $x \in U$ and $x \notin B$. Were $x \in A$, then $A \subseteq B$ would force $x \in B$, a contradiction; so $x \notin A$, hence $x \in A^c$. As $x$ was arbitrary, $B^c \subseteq A^c$.

Conversely assume $B^c \subseteq A^c$. Fix $x \in A$, so $x \in U$. Were $x \notin B$, then $x \in B^c$, and the hypothesis would give $x \in A^c$, i.e. $x \notin A$, contradicting $x \in A$; so $x \in B$. As $x$ was arbitrary, $A \subseteq B$. Both directions hold, so $A \subseteq B \iff B^c \subseteq A^c$. This is the set-theoretic form of contrapositive equivalence (0.1.7): passing to complements reverses an inclusion, just as contraposition reverses an implication.

■

**Exercise 0.E.20** [De Morgan for an indexed family]

Let $\{A_\alpha\}_{\alpha \in I}$ be an indexed family of subsets of a universe $U$, with $I \neq \varnothing$. Prove the infinite De Morgan law

$$\Big(\bigcup_{\alpha \in I} A_\alpha\Big)^c = \bigcap_{\alpha \in I} A_\alpha^c.$$

Solution.

The identity holds for any index set $I$, finite or infinite; the proof is double inclusion (0.3.7), driven by the quantifier negation rule of 0.2.5.

For $\subseteq$, fix $x \in \big(\bigcup_\alpha A_\alpha\big)^c$, so $x \in U$ and $x \notin \bigcup_\alpha A_\alpha$. By definition of the indexed union (0.3.22), $x \in \bigcup_\alpha A_\alpha$ says "$\exists\, \alpha \in I,\ x \in A_\alpha$"; its negation is "$\forall\, \alpha \in I,\ x \notin A_\alpha$" (0.2.5). So $x \notin A_\alpha$ for every $\alpha$, i.e. $x \in A_\alpha^c$ for every $\alpha$, which is exactly $x \in \bigcap_\alpha A_\alpha^c$.

For $\supseteq$, fix $x \in \bigcap_\alpha A_\alpha^c$, so $x \in U$ and $x \in A_\alpha^c$ for every $\alpha$, that is $x \notin A_\alpha$ for every $\alpha$. Then no $\alpha$ puts $x$ in $A_\alpha$, so $x \notin \bigcup_\alpha A_\alpha$, hence $x \in \left(\bigcup_\alpha A_\alpha\right)^c$. Both inclusions hold, so the sets are equal. This is the two-set law of 0.3.14 with "not-or" upgraded to "not-some": negating the existential that defines a union produces the universal that defines an intersection, which is precisely 0.2.5.

■

## Relations and functions

**Exercise 0.E.21** [injectivity from a formula]

Let $f\colon \mathbb{R} \to \mathbb{R}$ be $f(x) = 3x - 7$. Prove that $f$ is injective and that it is surjective, and write down its inverse.

SOLUTION.

The map is a bijection with inverse $f^{-1}(y) = (y + 7)/3$.

For injectivity, take $x, y \in \mathbb{R}$ with $f(x) = f(y)$, that is $3x - 7 = 3y - 7$. Adding 7 and dividing by 3 gives $x = y$, which is the defining condition of 0.4.9.

For surjectivity, fix an arbitrary $b \in \mathbb{R}$ and look for a witness by solving $3x - 7 = b$; this forces $x = (b + 7)/3$, a genuine real number. Then $f\big((b + 7)/3\big) = 3 \cdot \frac{b+7}{3} - 7 = b$, so $b$ is hit. Being injective and surjective, $f$ is bijective, hence invertible (0.4.15). The witness just constructed is exactly the inverse rule: $f^{-1}(y) = (y + 7)/3$, and one checks $f^{-1}(f(x)) = \frac{(3x-7)+7}{3} = x$ and $f(f^{-1}(y)) = 3 \cdot \frac{y+7}{3} - 7 = y$.

■

**Exercise 0.E.22** [a collision]

Let $g\colon \mathbb{R} \to \mathbb{R}$ be $g(x) = x^2 - 4x$. Decide whether $g$ is injective and whether it is surjective, with proof.

SOLUTION.

It is neither injective nor surjective.

To break injectivity, exhibit one collision. Completing the square, $g(x) = (x - 2)^2 - 4$, so $g$ is symmetric about $x = 2$: $g(0) = 0$ and $g(4) = 16 - 16 = 0$, hence $g(0) = g(4)$ while $0 \neq 4$. A single such pair defeats the universal in 0.4.9.

To break surjectivity, find a target no input reaches. Since $(x - 2)^2 \geq 0$ for every real $x$, we have $g(x) = (x - 2)^2 - 4 \geq -4$, so the value $-5$ is never attained; the existential $\exists\, x,\ g(x) = -5$ is false. Either failure alone settles the question, and both hold here.

■

**Exercise 0.E.23** [composition of injections]

Let $f\colon A \to B$ and $g\colon B \to C$ be injective. Prove that $g \circ f\colon A \to C$ is injective. Then show by example that $g \circ f$ can be injective while $g$ is not.

Solution.

The composition of injections is injective.

Take $x, y \in A$ with $(g \circ f)(x) = (g \circ f)(y)$, that is $g(f(x)) = g(f(y))$. Injectivity of $g$ applied to the inputs $f(x), f(y) \in B$ gives $f(x) = f(y)$; injectivity of $f$ then gives $x = y$. So $g \circ f$ satisfies 0.4.9.

The converse property fails: $g$ need not be injective even when $g \circ f$ is. Take $A = \{0\}$, $B = \{0, 1\}$, $C = \{0\}$, with $f(0) = 0$ and $g$ the constant map $g(0) = g(1) = 0$. Here $g$ collapses 0 and 1, so it is not injective, yet $g \circ f\colon \{0\} \to \{0\}$ is trivially injective, having only one input. The injectivity of a composite constrains the *first* map applied, not the second.

■

**Exercise 0.E.24** [preimage of a union]

Let $f\colon A \to B$ and let $T, U \subseteq B$. Prove $f^{-1}(T \cup U) = f^{-1}(T) \cup f^{-1}(U)$.

Solution.

The two sets are equal, proved by showing each element of one lies in the other.

Fix $a \in A$. Unwinding the preimage from 0.4.7,

$$a \in f^{-1}(T \cup U) \iff f(a) \in T \cup U \iff \big(f(a) \in T \text{ or } f(a) \in U\big).$$

The final clause is, again by 0.4.7, the statement "$a \in f^{-1}(T)$ or $a \in f^{-1}(U)$," which is exactly $a \in f^{-1}(T) \cup f^{-1}(U)$. Each step is a biconditional, so the two sets have identical membership conditions and are equal. The argument is the union twin of 0.4.8; the only change is "and" becoming "or," reflecting that union is built from disjunction.

■

**Exercise 0.E.25** [forward image can grow]

Let $f\colon A \to B$ and $S, S' \subseteq A$. Prove $f(S \cup S') = f(S) \cup f(S')$, and give an example where $f(S \cap S') \neq f(S) \cap f(S')$.

Solution.

The image distributes over unions but not over intersections.

For the union, a point $b$ lies in $f(S \cup S')$ exactly when $b = f(a)$ for some $a \in S \cup S'$, i.e. for

some $a \in S$ or some $a \in S'$; that is precisely $b \in f(S)$ or $b \in f(S')$, namely $b \in f(S) \cup f(S')$. Both inclusions hold, so the sets are equal.

For the intersection the equality can fail. Take $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$, with $S = \{1\}$ and $S' = \{-1\}$. Then $S \cap S' = \emptyset$ gives $f(S \cap S') = \emptyset$, while $f(S) \cap f(S') = \{1\} \cap \{1\} = \{1\}$. The obstruction is exactly the collapsing that injectivity forbids: when $f$ is injective the intersection equality is restored, since distinct inputs then keep distinct images.

■

**Exercise 0.E.26** [verify an equivalence relation]

On $\mathbb{R}$ define $x \sim y$ to mean $x - y \in \mathbb{Z}$. Prove that $\sim$ is an equivalence relation and describe the equivalence class $[x]$.

SOLUTION.

The relation is an equivalence relation, and $[x] = \{\, x + k : k \in \mathbb{Z} \,\}$.

It satisfies the three axioms of 0.4.16. Reflexive: $x - x = 0 \in \mathbb{Z}$, so $x \sim x$. Symmetric: if $x - y \in \mathbb{Z}$ then $y - x = -(x - y) \in \mathbb{Z}$, since the integers are closed under negation, so $y \sim x$. Transitive: if $x - y \in \mathbb{Z}$ and $y - z \in \mathbb{Z}$, then their sum $(x - y) + (y - z) = x - z \in \mathbb{Z}$, so $x \sim z$.

For the class, $y \in [x]$ means $x - y \in \mathbb{Z}$, that is $y = x - k$ for some integer $k$; as $k$ ranges over $\mathbb{Z}$ so does $-k$, so $[x] = \{\, x + k : k \in \mathbb{Z} \,\}$, the integer translates of $x$. Each class meets the half-open interval $[0, 1)$ in exactly one point, the fractional part of $x$, so $[0, 1)$ is a complete set of class representatives and the quotient $\mathbb{R}/\!\sim$ may be pictured as a circle of circumference one (gluing 0 to 1).

■

**Exercise 0.E.27** [a relation that just misses]

On $\mathbb{R}$ define $x \; R \; y$ to mean $|x - y| \leq 1$. Show $R$ is reflexive and symmetric but not transitive, so it is *not* an equivalence relation.

SOLUTION.

The relation has the first two properties but fails the third.

Reflexive: $|x - x| = 0 \leq 1$, so $x \; R \; x$ for every $x$. Symmetric: $|x - y| = |y - x|$, so $|x - y| \leq 1$ holds iff $|y - x| \leq 1$, giving $x \; R \; y \Rightarrow y \; R \; x$.

Transitivity fails, and one counterexample is enough to deny the universal in 0.4.16. Take $x = 0$, $y = 1$, $z = 2$: then $|0 - 1| = 1 \leq 1$ and $|1 - 2| = 1 \leq 1$, so $0 \; R \; 1$ and $1 \; R \; 2$, yet $|0 - 2| = 2 > 1$, so $0 \not R \; 2$. Closeness within a fixed tolerance does not chain, which is why "approximately equal" is never an equivalence relation—the very obstruction that forces

analysis to work with genuine limits rather than "small enough" differences.

■

**Exercise 0.E.28** [a two-sided inverse forces bijectivity]

Let $f\colon A \to B$ and suppose there is $g\colon B \to A$ with $g \circ f = \mathrm{id}_A$ and $f \circ g = \mathrm{id}_B$. Prove $f$ is bijective *without* quoting 0.4.15, by arguing each property directly.

Solution.

The function $f$ is injective and surjective.

For injectivity, suppose $f(x) = f(y)$ with $x, y \in A$. Apply $g$ to both sides and use $g \circ f = \mathrm{id}_A$:

$$x = g\big(f(x)\big) = g\big(f(y)\big) = y,$$

so distinct inputs cannot share an output.

For surjectivity, fix $b \in B$ and set $a = g(b) \in A$. Then $f \circ g = \mathrm{id}_B$ gives $f(a) = f(g(b)) = b$, so $b$ has the preimage $a$. Holding for every $b$, this is the existential of 0.4.9. Hence $f$ is bijective. The point worth keeping is that injectivity used only the left inverse and surjectivity only the right inverse—each side of the inverse equation carries exactly one of the two properties.

■

**Exercise 0.E.29** [a bijection between intervals]

Construct an explicit bijection $f\colon (0,1) \to (a,b)$ for real numbers $a < b$, and prove it is one. Conclude that any two bounded open intervals are equinumerous.

Solution.

The affine map $f(t) = a + (b-a)\,t$ is a bijection from $(0,1)$ onto $(a,b)$.

First it lands in the target: for $t \in (0,1)$, multiplying the strict inequalities $0 < t < 1$ by the positive number $b - a$ and adding $a$ gives $a < a + (b-a)t < b$, so $f(t) \in (a,b)$. It is injective because $f(s) = f(t)$ means $a + (b-a)s = a + (b-a)t$; cancelling $a$ and dividing by $b - a \neq 0$ gives $s = t$. It is surjective because, given any $y \in (a,b)$, the value $t = (y-a)/(b-a)$ satisfies $0 < t < 1$ (divide $a < y < b$ by $b - a > 0$ after subtracting $a$) and $f(t) = a + (b-a) \cdot \frac{y-a}{b-a} = y$.

So $f$ is a bijection, and by 0.4.21 the intervals $(0,1)$ and $(a,b)$ are equinumerous. Since this holds for every choice of $a < b$, and equinumerosity is symmetric and transitive (0.4.21), any two bounded open intervals $(a,b)$ and $(c,d)$ are equinumerous, each being equinumerous with $(0,1)$. This finite-looking statement already foreshadows the surprises of 2.1: a comparable trick stretches a bounded interval onto the whole line.

■

## The craft of proof

**Exercise 0.E.30** [direct proof]

Prove that the sum of any two odd integers is even.

SOLUTION.

Let $m$ and $n$ be odd, so $m = 2j + 1$ and $n = 2k + 1$ for integers $j, k$. Then

$$m + n = (2j + 1) + (2k + 1) = 2(j + k + 1),$$

and since $j + k + 1$ is an integer, $m + n$ is twice an integer, hence even.

■

**Exercise 0.E.31** [contrapositive]

Let $n$ be an integer. Prove that if $3n + 2$ is odd, then $n$ is odd.

SOLUTION.

We prove the contrapositive: if $n$ is even, then $3n + 2$ is even. Suppose $n = 2k$. Then $3n + 2 = 6k + 2 = 2(3k + 1)$, which is even. By 0.1.7 the contrapositive is equivalent to the original implication, so "$3n + 2$ odd $\Rightarrow$ $n$ odd" is proved. (A direct attack stalls: "$3n + 2$ odd" is awkward to use, while "$n$ even" is an immediate handle—the cue to switch to the contrapositive.)

■

**Exercise 0.E.32** [contradiction]

Prove that there is no smallest positive real number.

SOLUTION.

Suppose, for contradiction, that there were a smallest positive real number, say $x > 0$, so that $x \leq y$ for every positive real $y$. Consider $x/2$. Since $x > 0$ we have $x/2 > 0$, so $x/2$ is itself a positive real; and $x/2 < x$ because $x > 0$. Thus $x/2$ is a positive real strictly smaller than $x$, contradicting that $x$ was the smallest. No such smallest positive real exists.

■

**Exercise 0.E.33** [contradiction]

Prove that $\sqrt{3}$ is irrational. (You may first prove the lemma: for an integer $p$, if 3 divides $p^2$ then 3 divides $p$.)

Solution.

First the lemma, by contrapositive: if $3 \nmid p$, then $p$ leaves remainder 1 or 2 on division by 3, i.e. $p = 3k+1$ or $p = 3k+2$. In the first case $p^2 = 9k^2+6k+1 = 3(3k^2+2k)+1$, and in the second $p^2 = 9k^2+12k+4 = 3(3k^2+4k+1)+1$; either way $p^2$ leaves remainder 1, so $3 \nmid p^2$. Hence $3 \mid p^2 \Rightarrow 3 \mid p$.

Now suppose, for contradiction, that $\sqrt{3} = p/q$ with $p, q$ integers in lowest terms, $q \neq 0$. Then $p^2 = 3q^2$, so $3 \mid p^2$, and by the lemma $3 \mid p$, say $p = 3r$. Substituting, $9r^2 = 3q^2$, so $q^2 = 3r^2$, whence $3 \mid q^2$ and, by the lemma again, $3 \mid q$. But then 3 divides both $p$ and $q$, contradicting lowest terms. Therefore $\sqrt{3}$ is irrational.

■

**Exercise 0.E.34** [counterexample]

Disprove: for all real numbers $a$ and $b$, $(a+b)^2 = a^2 + b^2$.

Solution.

The statement is false; one counterexample suffices to disprove a universal (0.5.8). Take $a = b = 1$: then $(a+b)^2 = 2^2 = 4$, while $a^2+b^2 = 1+1 = 2$, and $4 \neq 2$. (The identity fails for any $a, b$ with $ab \neq 0$, since $(a+b)^2 = a^2+b^2+2ab$; a single instance is all a disproof needs.)

■

**Exercise 0.E.35** [cases]

Prove that $n^3 - n$ is divisible by 6 for every integer $n$.

Solution.

Factor $n^3 - n = (n-1)\,n\,(n+1)$, a product of three consecutive integers. Among any two consecutive integers one is even, so the product is divisible by 2; among any three consecutive integers one is divisible by 3, so the product is divisible by 3. Being divisible by both 2 and 3, and these having no common factor, the product is divisible by 6. Hence $6 \mid n^3 - n$.

■

**Exercise 0.E.36** [biconditional]

Prove that an integer $n$ is even if and only if $n^2$ is even.

Solution.

A biconditional needs both directions (0.5.9). ($\Rightarrow$) If $n$ is even, $n = 2k$, then $n^2 = 4k^2 = 2(2k^2)$ is even—a direct argument. ($\Leftarrow$) If $n^2$ is even then $n$ is even; this is the contrapositive proof already given in 0.5.4 (an odd $n$ has an odd square). Both directions

holding, $n$ is even exactly when $n^2$ is.

■

**Exercise 0.E.37** [prove or disprove]

Prove or disprove: the sum of two irrational numbers is always irrational.

SOLUTION.

False. Take $a = \sqrt{2}$ and $b = -\sqrt{2}$; both are irrational (0.5.5), yet $a + b = 0$ is rational. The claim is a universal statement, so this single counterexample disproves it. (What *is* true is narrower: an irrational plus a *rational* is irrational—a good direct exercise on its own.)

■

## Mathematical induction

**Exercise 0.E.38** [summation identity]

Prove that for every integer $n \geq 1$,

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

SOLUTION.

The identity holds for all $n \geq 1$, by induction on $n$. For the base case $n = 1$ the left side is $1^2 = 1$ and the right side is $\frac{1\cdot 2\cdot 3}{6} = 1$, so the two agree.

Fix $k \geq 1$ and assume $1^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}$. Adding the next term $(k+1)^2$ and putting everything over 6,

$$\begin{aligned}\sum_{i=1}^{k+1} i^2 &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \\ &= \frac{(k+1)\big[k(2k+1) + 6(k+1)\big]}{6} = \frac{(k+1)\big(2k^2+7k+6\big)}{6}.\end{aligned}$$

The quadratic factors as $2k^2 + 7k + 6 = (k+2)(2k+3)$, so the right side becomes $\frac{(k+1)(k+2)(2k+3)}{6}$, which is the formula with $k+1$ in place of $n$. The inductive step holds, and by 0.6.2 the identity is valid for all $n \geq 1$.

■

**Exercise 0.E.39** [telescoping sum]

Prove that for every integer $n \geq 1$,

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

Solution.

The identity holds for all $n \geq 1$. For the base case $n = 1$ the left side is $\frac{1}{1 \cdot 2} = \frac{1}{2}$ and the right side is $\frac{1}{2}$, which agree.

Assume the identity for a fixed $k \geq 1$. Adding the term $\frac{1}{(k+1)(k+2)}$ to both sides,

$$\begin{aligned} \sum_{i=1}^{k+1} \frac{1}{i(i+1)} &= \frac{k}{k+1} + \frac{1}{(k+1)(k+2)} = \frac{k(k+2)+1}{(k+1)(k+2)} \\ &= \frac{(k+1)^2}{(k+1)(k+2)} = \frac{k+1}{k+2}, \end{aligned}$$

which is the formula at $k+1$. By 0.6.2 it holds for every $n \geq 1$. (The name "telescoping" fits: since $\frac{1}{i(i+1)} = \frac{1}{i} - \frac{1}{i+1}$, the sum collapses to $1 - \frac{1}{n+1} = \frac{n}{n+1}$, which is the quicker route once you see it.)

■

**Exercise 0.E.40** [geometric sum]

Let $r$ be a real number with $r \neq 1$. Prove that for every integer $n \geq 0$,

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

Solution.

The formula holds for all $n \geq 0$, by induction on $n$. For the base case $n = 0$ the left side is the single term 1 and the right side is $\frac{r^1 - 1}{r - 1} = \frac{r-1}{r-1} = 1$ (well defined since $r \neq 1$), so they agree.

Fix $k \geq 0$ and assume $1 + r + \cdots + r^k = \frac{r^{k+1} - 1}{r - 1}$. Adding $r^{k+1}$,

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

after cancelling $r^{k+1} - r^{k+1} = 0$ in the numerator. This is the formula at $k+1$, so by 0.6.2 it holds for all $n \geq 0$. Taking $r = 2$ recovers 0.6.6(b).

■

**Exercise 0.E.41** [Bernoulli's inequality]

Let $x$ be a real number with $x \geq -1$. Prove *Bernoulli's inequality*: for every $n \in \mathbb{N}$,

$$(1+x)^n \geq 1 + nx.$$

SOLUTION.

The inequality holds for all $n \in \mathbb{N}$ and every fixed $x \geq -1$. For the base case $n = 0$ both sides equal 1 (since $(1+x)^0 = 1$ and $1 + 0 \cdot x = 1$), so $\geq$ holds.

Fix $k \geq 0$ and assume $(1+x)^k \geq 1 + kx$. The hypothesis $x \geq -1$ makes $1 + x \geq 0$, so multiplying the inductive hypothesis by the nonnegative factor $1 + x$ preserves the inequality:

$$(1+x)^{k+1} = (1+x)^k(1+x) \;\geq\; (1+kx)(1+x) = 1 + (k+1)x + kx^2.$$

Since $kx^2 \geq 0$, the right side is at least $1 + (k+1)x$, hence $(1+x)^{k+1} \geq 1 + (k+1)x$, which is the claim at $k+1$. By 0.6.2 the inequality holds for all $n \in \mathbb{N}$. The step used $1 + x \geq 0$ in an essential way; without $x \geq -1$ the factor could be negative and reverse the inequality.

■

**Exercise 0.E.42** [divisibility]

Prove that for every $n \in \mathbb{N}$, $6 \mid (n^3 - n)$. (This sharpens 0.6.8.)

SOLUTION.

The claim holds for all $n \in \mathbb{N}$. For the base case $n = 0$, $0^3 - 0 = 0 = 6 \cdot 0$, divisible by 6.

Fix $k \geq 0$ and assume $6 \mid (k^3 - k)$, say $k^3 - k = 6q$ for some integer $q$. As in 0.6.8,

$$(k+1)^3 - (k+1) = (k^3 - k) + 3(k^2 + k) = 6q + 3k(k+1).$$

Among the two consecutive integers $k$ and $k+1$ one is even, so their product $k(k+1)$ is even, say $k(k+1) = 2m$; then $3k(k+1) = 6m$. Hence

$$(k+1)^3 - (k+1) = 6q + 6m = 6(q+m),$$

a multiple of 6, which is the claim at $k+1$. By 0.6.2 it holds for every $n \in \mathbb{N}$. The extra factor of 2 over 0.6.8 comes exactly from the even member of the consecutive pair $k, k+1$.

■

**Exercise 0.E.43** [strong induction (Fibonacci)]

Define the Fibonacci numbers by $F_1 = 1$, $F_2 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 3$. Prove that $F_n < 2^n$ for every $n \geq 1$.

Solution.

The bound $F_n < 2^n$ holds for all $n \geq 1$, by strong induction (0.6.9); the recursion reaches *two* steps back, so the strong form is the natural tool. Because the recursion only kicks in at $n \geq 3$, we verify the two starting values directly: $F_1 = 1 < 2 = 2^1$ and $F_2 = 1 < 4 = 2^2$.

Fix $k \geq 2$ and assume $F_j < 2^j$ for every $j$ with $1 \leq j \leq k$. Then $k+1 \geq 3$, so the recursion gives $F_{k+1} = F_k + F_{k-1}$, and both $k$ and $k-1$ lie in the range covered by the hypothesis. Hence

$$F_{k+1} = F_k + F_{k-1} < 2^k + 2^{k-1} = 2^{k-1}(2+1) = 3 \cdot 2^{k-1} < 4 \cdot 2^{k-1} = 2^{k+1}.$$

Thus $F_{k+1} < 2^{k+1}$, and by 0.6.9 the bound holds for all $n \geq 1$. Ordinary induction would stall: $F_{k+1}$ depends on $F_{k-1}$ as well as $F_k$, and only the strong hypothesis supplies both at once.

■

**Exercise 0.E.44** [strong induction (coins)]

Prove that every integer amount of $n \geq 8$ cents can be paid exactly using only 3-cent and 5-cent coins.

Solution.

Every $n \geq 8$ is so payable, by strong induction (0.6.9). Three base cases are needed because the step will reach three back: $8 = 3 + 5$, $9 = 3 + 3 + 3$, and $10 = 5 + 5$ are each payable.

Fix $k \geq 10$ and assume every amount $j$ with $8 \leq j \leq k$ is payable. Consider $k + 1$. Since $k + 1 \geq 11$, the smaller amount $(k + 1) - 3 = k - 2$ satisfies $k - 2 \geq 8$, so by the inductive hypothesis $k - 2$ is payable with 3- and 5-cent coins. Adding one more 3-cent coin pays $k + 1$. Hence every $n \geq 8$ is payable; the three base cases plus this step cover all of them by 0.6.9.

The reduction is to the case three smaller, not the immediate predecessor, which is exactly why the strong form and three base cases are the honest setup. (The amount 7 is *not* payable, so 8 is the true threshold.)

■

**Exercise 0.E.45** [find the flaw]

The following purports to prove that every natural number is equal to 0. Find the exact step that fails. *"Claim: for all $n \in \mathbb{N}$, $n = 0$. Strong induction. Base case $n = 0$: $0 = 0$. Step: fix*

*$k$ and assume $j = 0$ for all $j$ with $0 \le j \le k$. Write $k+1 = a+b$ with $a, b \in \mathbb{N}$ and $a, b \le k$. By the hypothesis $a = 0$ and $b = 0$, so $k+1 = a+b = 0$. Hence $n = 0$ for all $n$."*

SOLUTION.

The fatal line is the claim "write $k+1 = a+b$ with $a, b \le k$," which is impossible at the very first transition $k = 0$. When $k = 0$ we are proving $P(1)$, i.e. $1 = 0$, and we would need $1 = a+b$ with both $a, b \le 0$; the only option is $a = b = 0$, giving $a+b = 0 \neq 1$. No valid decomposition exists, so the inductive step is never established for $k = 0$, and the chain breaks immediately after the base case exactly as in the horse fallacy (0.6.14).

For $k \ge 1$ a decomposition $k+1 = a+b$ with $a, b \le k$ does exist (e.g. $a = 1$, $b = k$), so the argument *looks* uniform—but a step that holds for all $k \ge 1$ together with a base case at $k = 0$ proves nothing past $P(0)$, since the link $P(0) \Rightarrow P(1)$ is precisely the one missing. The moral of 0.6.15 applies: test the step at its first instance, where the hidden requirement (here, a decomposition into smaller summands) can fail.

■

**Exercise 0.E.46** [equivalence of the principles]

Assume the principle of mathematical induction (0.6.2) and use it to *prove* well-ordering (0.6.1): every nonempty $S \subseteq \mathbb{N}$ has a least element. (Together with the converse proved in 0.6.2, this shows the two are equivalent.)

SOLUTION.

We prove the contrapositive: a subset $S \subseteq \mathbb{N}$ with *no* least element must be empty. Suppose $S$ has no least element. Let $P(n)$ be the statement "no natural number $m \le n$ belongs to $S$," and prove $P(n)$ for all $n \in \mathbb{N}$ by ordinary induction.

For the base case $n = 0$: if $0 \in S$ then 0 would be a least element of $S$ (nothing in $\mathbb{N}$ is below it), contradicting our supposition; so $0 \notin S$, and $P(0)$ holds. For the step, fix $k$ and assume $P(k)$, so no $m \le k$ lies in $S$. If $k+1$ belonged to $S$, then since all of $0, 1, \ldots, k$ are absent from $S$, $k+1$ would be the least element of $S$—again a contradiction. Hence $k+1 \notin S$, and combined with $P(k)$ this gives $P(k+1)$.

By 0.6.2, $P(n)$ holds for every $n$, meaning no natural number lies in $S$; that is, $S = \emptyset$. Contrapositively, every nonempty $S \subseteq \mathbb{N}$ has a least element. Since 0.6.2 derived induction from well-ordering, the two principles—and, by 0.6.10, strong induction—are logically equivalent, as recorded in 0.6.13.

■

# Index of Objects