LECTURE NOTES

MATH 100 — SUMMER 2022

INTRODUCTION TO PROOF AND PROBLEM SOLVING

University of California, Santa Cruz

DEEWANG BHAMIDIPATI

adapted from

Lectures by HIROTAKA TAMANOI

WINTER 2021

(all errors introduced are my own)

Last Updated: Thursday 8th December, 2022

Contents

1 Sets 2

2 Logic 10

3 Methods of Proof I. Direct Proof & Proof by Contrapositive 21

4 More on Methods of Proof I. 27

5 Methods of Proof II. Counterexamples, Proof by Contradiction and Existence Proofs 35

6 Principle of Mathematical Induction 43

7 Prove or Disprove 49

8 Relations 55

9 Equivalence Relations 60

10 Functions 68

11 Cardinality of Sets 78

1. Sets

Discussion 1.1 (Notation)**.** Throughout this lecture, we will observe the following notation. Upper case letters $A, B, C, \ldots, X, Y, Z$ will denote sets, while lower case letters $a, b, c, \ldots, x, y, z$ will denote elements.

We use $\in$ to denote membership of, or belongingness to, a set

$$a \in A : \text{“}a\text{" } \textit{is an element of a set } A$$

$$a \notin A : \text{“}a\text{" } \textit{is } \text{not } \textit{an element of a set } A$$

Discussion 1.2 (Description of Sets)**.** There are two ways to describe sets:

(1) One can list all the elements in a set, enclosing it within `{ }`.

$$A = \{-4, -2, 0, 2, 4\} = \{0, \pm 2, \pm 4\}$$

(2) Use *set-builder notation*, where we first introduce a general element and the describe the relevant property that defines the set. The recipe is

$$\{\text{typical element} \mid \text{properties of that element}\}$$

The vertical bar is read *such that*; the notation as a whole is to be read as “those elements such that they have this property”. For example, we can write the set A above as follows; here $\mathbb{Z}$ denotes the set of integers

$$\begin{aligned} A &= \{n \in \mathbb{Z} \mid n \text{ is even and } |n| \leqslant 4\} \\ &= \{n \in \mathbb{Z} \mid n = 2k, \text{ for some } k \in \mathbb{Z}, \text{and } |k| \leqslant 2\}\,. \end{aligned}$$

So, A is read as “those integers n *such that* n is even and $|n| \leqslant 4$”.

Definition 1.3 (The Empty Set)**.** There is a set with *no elements*, denoted $\varnothing$; we call it the empty set.

The set can be realised via various descriptions. A mathematical description is the set

$$\left\{x \in \mathbb{Z} \mid x^2 < 0\right\}.$$

A non-mathematical description is the set of words in the English language that start with the letter *z* and end with the letter *q*.

☡ While $\varnothing$ has no elements, the set $X = \{\varnothing\}$ is not the empty set. It is a set with one element – the empty set, $\varnothing \in X$.

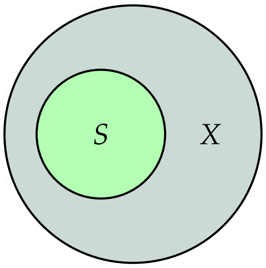
Definition 1.4 (Cardinality)**.** The cardinality of a set is the number of elements in the set. For a set X, its cardinality is denoted $\#X$ or $|X|$.

For example, let $A = \{0, \pm 2, \pm 4\}$, then $\#A = 5$.

☡ The notion of cardinality is clear for finite sets, that is, sets with finitely many elements. We will promptly ignore this notion, for now, for infinite sets.

Subsets

Definition 1.5 (Subsets)**.** Given two sets S and X, we say S is a subset of X if every element of S is also an element of X, and denote it as $S \subseteq X$. That is, S is the set of *some* elements of X.



Any set X always has two subsets: itself and the empty set.

Example 1.6. Let $B = \{\varnothing, \{\varnothing\}, 1, 2, \{1,2\}\}$, then

$$\varnothing \in B, \text{ so } \{\varnothing\} \subseteq B \qquad \{\varnothing\} \in B, \text{ so } \{\{\varnothing\}\} \subseteq B \qquad 1, 2 \in B, \text{ so } \{1,2\} \subseteq B$$

Also, $\{1,2\} \in B$ and $\varnothing$, $B \subseteq B$ as always.

☡ This example highlights a common error. We note that $\{1,2\} \subseteq B$ since 1 and 2 are *elements* of B. But also $\{1,2\} \in B$, since $\{1,2\}$ is also an element of B.

Being an element means it itself is listed, as is, in a set; while being a subset means *the elements of the subset* are listed as is. For example, take $C = \{1,2,3\}$; then $\{1,2\} \subseteq C$ but $\{1,2\} \notin C$ since the set $\{1,2\}$ is not an element of C.

We now use the notion of subsets to define what it means for two sets to be equal.

Definition 1.7 (Equality of Sets)**.** We say two sets A and B are equal if $A \subseteq B$ and $B \subseteq A$, and we denote it $A = B$.

Definition 1.8 (Proper Subsets)**.** A set S is called a proper subset of X if $S \subseteq X$ and $S \neq X$. We denote this as $S \subset X$ or $S \subsetneq X$. In other words, S is a subset that is "strictly smaller than X".

If the set is non-empty, then it has a proper subset – the empty set.

Definition 1.9 (Power Set)**.** The power set of a set X is the set of *all* subsets of X, including X and $\varnothing$. We denote it $\mathscr{P}(X)$.

For several reasons, the power set is also denoted as 2^X, one reason is revealed below.

Example 1.10. Let's compute power sets of some sets.

(1) Let $A = \{1,2,3\}$, so $|A| = 3$.

$$\varnothing \subseteq A$$

$$1 \in A, \text{ so } \{1\} \subseteq A$$

$$1,\, 2 \in A, \text{ so } \{1,2\} \subseteq A$$

$$1,\, 2,\, 3 \in A, \text{ so } A = \{1,2,3\} \subseteq A$$

We then get

$$\mathscr{P}(A) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1,2\}, \{2,3\}, \{1,3\}, \{1,2,3\}\}$$

Note that $|\mathscr{P}(A)| = 8 = 2^3 = 2^{|A|}$.

(2) Let $A = \{1, \{2\}\}$, so $|A| = 2$. We have

$$\mathscr{P}(A) = \{\varnothing, \{1\}, \{\{2\}\}, \{1, \{2\}\}\}$$

$|\mathscr{P}(A)| = 4 = 2^2 = 2^{|A|}$.

(3) Let $A = \varnothing$, so $|A| = 0$. We have

$$B = \mathscr{P}(A) = \{\varnothing\}, \quad |\mathscr{P}(A)| = 1 = 2^0 = 2^{|A|}$$

What about $\mathscr{P}(B)$? We have

$$C = \mathscr{P}(B) = \{\varnothing, \{\varnothing\}\}$$

Finally,

$$\mathscr{P}(C) = \{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}, \{\varnothing, \{\varnothing\}\}\}$$

Remark 1.11. It's true in general that $|\mathscr{P}(X)| = 2^{|X|}$, for any set X.

Set Operations

We assume all the sets in the section are subsets of some set U, labelled the "universal set".

Definition 1.12 (Set Operations)**.** Let A, $B \subseteq U$.

- The union of A and B is the set

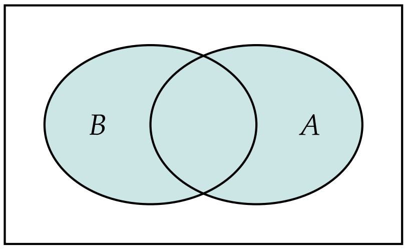
$$A \cup B = \{x \in U \mid x \in A \text{ or } x \in B\}$$

Here our use of "or" allows the possibility of x being in both A and B.

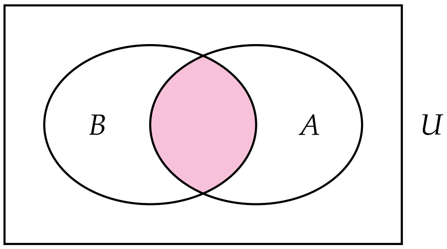
- The intersection of A and B is the set

$$A \cap B = \{x \in U \mid x \in A \text{ and } x \in B\}$$

It is clear definitionally that we always have $A \cap B \subseteq A \cup B$.



$A \cup B$



$A \cap B$

- The difference of A and B is the set

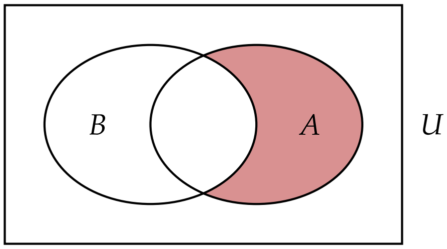
$$A \setminus B = A - B = \{x \in U \mid x \in A \textit{ and } x \notin B\}$$

That is, it is the set that's left when we remove the part of B that belonged to A. Similarly, we can also consider the set that's left when we remove the part of A that belonged to B

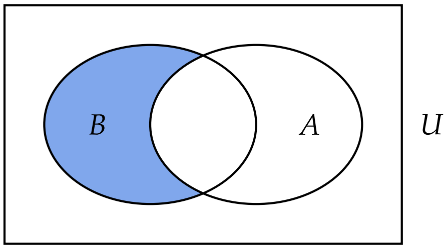
$$B \setminus A = B - A = \{x \in U \mid x \in B \textit{ and } x \notin A\}$$

A related operation is the symmetric difference defined as

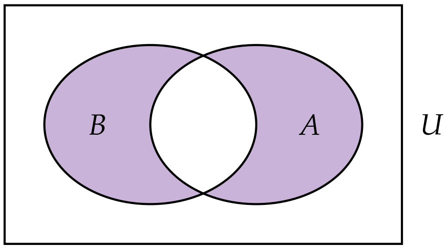
$$A \triangle B = (A \setminus B) \cup (B \setminus A)$$



$A \setminus B$



$B \setminus A$

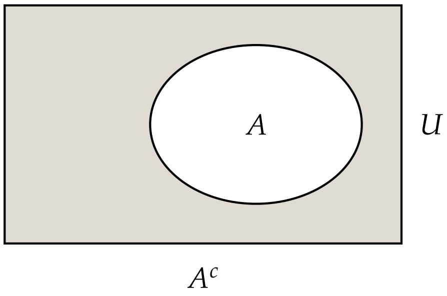


$A \triangle B$

- The complement of A in U is the set

$$A^c = \overline{A} = \{x \in U \mid x \notin A\}$$

That is, it is the set of exactly those elements in U that don't belong to A.



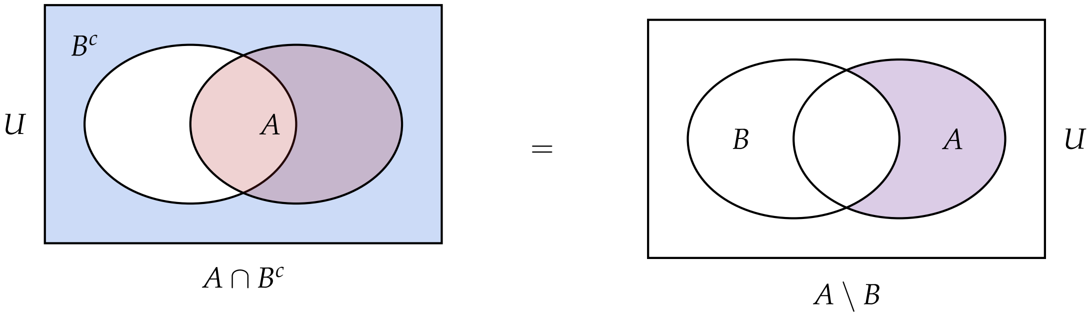
Proposition 1.13. *We have the following identities*

(1) $A \setminus B = A \cap B^c$

(2) $(A \cap B)^c = A^c \cup B^c$

(3) $(A \cup B)^c = A^c \cap B^c$

Proof. We give a "proof by diagram" for (1)



Try proving (2) and (3) similarly. Such diagrams are called *Venn diagrams*. We will revisit (2) and (3) when we discuss *de Morgan Laws*. □

Indexed Collection of Sets

Discussion 1.14. For a finite collection of sets

$$\{A_1, A_2, \dots, A_n\} = \{A_i\}_{i=1}^{n} = \{A_i\}_{i \in I}, \; I = \{1, 2, \dots, n\}$$

we have

$$A_1 \cap A_2 \cap \cdots \cap A_n = \bigcap_{i=1}^{n} A_i = \bigcap_{i \in I} A_i$$

$$A_1 \cup A_2 \cup \cdots \cup A_n = \bigcup_{i=1}^{n} A_i = \bigcup_{i \in I} A_i$$

That motivates us to consider an arbitrary collection of sets, indexed by an index set I.

$$\{X_\alpha, A_\beta, A_\gamma, \ldots\} = \{X_\alpha\}_{\alpha\in I}, \; I = \{\alpha, \beta, \gamma, \ldots\}$$

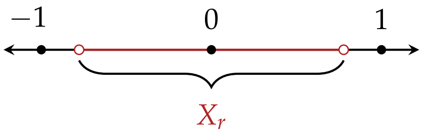
$$X_\alpha \cap X_\beta \cap X_\gamma \cap \cdots = \bigcap_{\alpha\in I} X_\alpha$$

$$X_\alpha \cup X_\beta \cup X_\gamma \cup \cdots = \bigcup_{\alpha\in I} X_\alpha$$

Our set I has no restrictions; in particular, it is allowed to infinite.

Example 1.15. Let our index set be $I = [1, \infty)$. For each $r \in I$, we consider the set

$$X_r = \left(-\frac{1}{r}, \frac{1}{r}\right)$$



Then one can show that

$$\bigcap_{r\in I} X_r = \{0\}, \text{ one point set}$$

$$\bigcup_{r\in I} X_r = X_1 = (-1, 1)$$

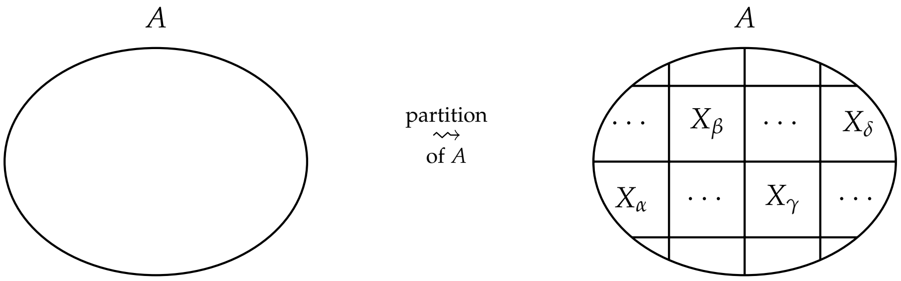
Partition of Sets

Let A be a set, and $\mathcal{S} = \{X_\alpha\}_{\alpha\in I}$ a collection (or family) of non-empty subsets of A, where I is some index set. That is, $\varnothing \neq X_\alpha \subseteq A$.

Definition 1.16 (Partitions). A collection $\mathcal{S}$ of subsets of A is said to be a partition of A if

(1) $X_\alpha \cap X_\beta = \varnothing$ if $\alpha \neq \beta$ (we say X_α and X_β are (mutually) disjoint); and

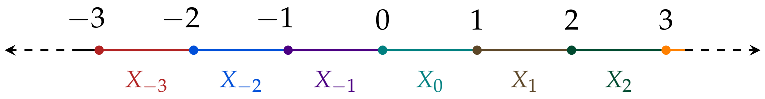
(2) $\bigcup_{\alpha\in I} X_\alpha = A$.



Remark 1.17. Later we will discuss the notion of "equivalence relations" and "equivalence classes". Partition of sets play an important role in this context.

Example 1.18.

- Let $A = \mathbb{R}$ be the set of real numbers, we will produce a partition of $\mathbb{R}$. For any integer m, consider the subset $X_m = [m, m+1)$ of $\mathbb{R}$.

  Observe that

  $$\begin{cases} X_m \cap X_k = \varnothing, \text{ for any pair of integers } m \neq k; & \text{and} \\ \mathbb{R} = \bigcup_{m \in \mathbb{Z}} X_m \end{cases}$$

  Thus, $\{X_m \mid m \in \mathbb{Z}\}$ is a partition of $\mathbb{R}$

- Let $A = \mathbb{Z}$ be the set of integers, and let us also choose a positive integer n. We will produce a partition of $\mathbb{Z}$ with respect to n.

  For an integer r such that $0 \leqslant r < n$, consider the following subset of $\mathbb{Z}$

  $$\begin{aligned} [r]_n &= \{k \in \mathbb{Z} \mid k \text{ has remainder } r \text{ when divided by } n\} \\ &= \{\ldots, -n+r, r, n+r, 2n+r, 3n+r, \ldots\} \\ &= \{k \in \mathbb{Z} \mid k \equiv r \bmod n\} \end{aligned}$$

  $[r]_n$ is an example of a *congruence class modulo n*. Here for two integers $a, b \in \mathbb{Z}$ we say $a \equiv b \bmod n$, "a is congruent to b modulo n", if n divides $b - a$, written $n \mid (b-a)$.

  For $n = 3,\ r = 0, 1, 2$

  $$\begin{aligned} [0]_3 &= \{\ldots, -6, -3, 0, 3, 6, 9, \ldots\} \\ [1]_3 &= \{\ldots, -5, -2, 1, 4, 7, 10, \ldots\} \\ [2]_3 &= \{\ldots, -4, -1, 2, 5, 8, 11, \ldots\} \end{aligned}$$

  Note that the remainder is always positive, for example $-4 = 3(-2) + 2$, which is why $-4 \in [2]_3$. Observe that

  $$\begin{cases} [0]_3 \cap [1]_3 = \varnothing,\ [0]_3 \cap [2]_3 = \varnothing,\ [1]_3 \cap [2]_3 = \varnothing; & \text{and} \\ [0]_3 \cup [1]_3 \cup [2]_3 = \mathbb{Z} \end{cases}$$

  Thus, $\{[0]_3, [1]_3, [2]_3\}$ is a partition of $\mathbb{Z}$.

We will revisit these example in greater detail later in the course.

Cartesian Product

Definition 1.19 (Cartesian Product)**.** For sets A and B, we define the cartesian product $A \times B$ as the set of ordered pairs

$$A \times B = \{(a, b) \mid a \in A,\ b \in B\}$$

Example 1.20.

(1) Let $A = B = \mathbb{R}$, the set of all real numbers.

$$\mathbb{R} \times \mathbb{R} = \{(x, y) \mid x,\, y \in \mathbb{R}\}$$

Standard notation for this set is $\mathbb{R}^2$, the Euclidean (or Cartesian) plane.

(2) $\mathbb{R} \times \mathbb{R} \times \mathbb{R} = \{(x, y, z) \mid x,\, y,\, z \in \mathbb{R}\}$. Standard notation for this set is $\mathbb{R}^3$, the three-dimensional Euclidean space.

(3) Suppose $A = \{1, 2, 3\}$ and $B = \{\text{red}, \text{blue}\}$, then

$$A \times B = \{(1, \text{red}), (1, \text{blue}), (2, \text{red}), (2, \text{blue}), (3, \text{red}), (3, \text{blue})\}$$

Lemma 1.21. $|A \times B| = |A| \cdot |B|$ *if both A and B are finite sets.*

Things quickly get more subtle if A and B were infinite.

Remark 1.22. If A and B are disjoint finite sets, that is, $A \cap B = \varnothing$, then

$$|A \cup B| = |A| + |B|$$

But if A or B have infinitely many elements, strange phenomena can occur. For example, consider $A = \mathbb{N} = \{1, 2, 3, \ldots\}$, the set of all positive integers, and $B = \{0\}$. Now A is an infinite set, so let's say $|A| = \infty$, and we of course have $|B| = 1$.

Note that $A \cap B = \varnothing$, so we expect $|A \cup B| = |A| + |B| = \infty + 1$. What is "$\infty + 1$"? Does this make sense? We will develop the mathematical theory of infinity later in the course if we have time.

2. Logic

Definition 2.1 (Statement)**.** A statement is a declarative sentence which can be objectively determined to be either *true* or *false*.

Example 2.2.

(a) *The integer* 11 *is divisible by* 4. **False** statement.

(b) *The integer* 11 *is a prime number*. **True** statement.

(c) *Is* 10^{10} *an integer?* This is a question, not a declarative sentence.

(d) *The integer* 10^{10} *is big*. Not a statement, since the word "big" is subjective; the truth value (T, F) may depend on individuals.

Logical Connectives

Definition 2.3 (Negation)**.** Given a statement P, the negation of P is the statement

$$\textbf{not } \boldsymbol{P}, \quad \text{denoted } \neg P$$

It's characterised by the following *truth table*

P	$\neg P$
T	**F**
F	**T**

Example 2.4.

$$P : \text{The integer 11 is odd.}$$

$$\neg P : \text{The integer 11 is } \textit{not} \text{ odd.} = \text{The integer 11 is even.}$$

Definition 2.5 (Disjunction)**.** Given statements P and Q, the disjunction of P and Q is the statement

$$\boldsymbol{P} \textbf{ or } \boldsymbol{Q}, \quad \text{denoted } P \vee Q$$

By definition, $P \vee Q$ is true if at least one of P or Q is true. Its truth table is

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

Example 2.6.

$$\begin{aligned} P &: \text{5 is odd.} & \mathbf{T} \\ Q &: \text{10 is prime.} & \mathbf{F} \\ P \vee Q &: \text{5 is odd or 10 is prime.} & \mathbf{T} \end{aligned}$$

Example 2.7. Let P be any statement, then ***P* or not *P*** is always true. We see this by looking at the truth table.

P	$\neg P$	$P \vee (\neg P)$
T	**F**	**T**
F	**T**	**T**

We call statements that are always true a *tautology*.

Definition 2.8 (Conjunction)**.** Given statements P and Q, the conjunction of P and Q is the statement

$$\boldsymbol{P} \textbf{ and } \boldsymbol{Q}, \quad \text{denoted } P \wedge Q$$

By definition, $P \wedge Q$ is true only when both P and Q are true. Its truth table is

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

Definition 2.9 (Implication)**.** Given statements P and Q, the implication is the statement

$$\textbf{if } \boldsymbol{P} \textbf{ then } \boldsymbol{Q}, \quad \text{denoted } P \Rightarrow Q$$

In this statement, P is called the *hypothesis*, while Q is called the *conclusion*. Its truth table is

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

When hypothesis P is not satisfied $(\mathbf{F})$, then whatever the conclusion Q may be $(\mathbf{T}, \mathbf{F})$, the implication $P \Rightarrow Q$ is true.

Example 2.10.

$$P : \text{It is raining.}$$

$$Q : \text{I will stay at home.}$$

$$P \Rightarrow Q : \text{If it is raining, then I will stay at home.}$$

Definition 2.11 (Different Terminology for Implication)**.** The statement $P \Rightarrow Q$ is read in several different ways.

$$\left.\begin{aligned} &\textit{if } P\textit{, then } Q \\ &P \textit{ implies } Q \\ &Q \textit{ if } P \\ &P \textit{ only if } Q \\ &P \text{ is } \textit{sufficient} \text{ for } Q \\ &Q \text{ is } \textit{necessary} \text{ for } P \end{aligned}\right\} \text{all mean } P \Rightarrow Q$$

We have just seen four ways to create new statements from one or two given statements. In mathematics, however, we are often interested in declarative sentences containing variables and whose truth or falseness is only known once we have assigned values to the variables.

Definition 2.12 (Open Sentences)**.** An open sentence is a declarative sentence which contains variables, where each variable can assume any value in a given set, called the domain of variables, which becomes a statement if variables are replaced by specific values.

Example 2.13. For $x \in \mathbb{R}$, consider the statement $P(x) : |x| = 3$,

$x = 1$	$P(1) : \|1\| = 3$	**F**
$x = -3$	$P(-3) : \|-3\| = 3$	**T**
$x = 2$	$P(2) : \|2\| = 3$	**F**

We can combine open sentences using $\neg$, $\vee$, $\wedge$, $\Rightarrow$ to make new open sentences.

Example 2.14.

$$P(x) : |x| = 3,\ x \in \mathbb{R} \qquad\qquad Q(x) : |x| = -3,\ x \in \mathbb{R}$$

Consider then,

$$\neg P(x) : |x| \neq 3 \qquad\qquad \neg P(1) : |1| \neq 3 \quad (\textbf{T})$$

$$P(x) \vee Q(x) : |x| = 3 \text{ or } x = -3 \qquad\qquad P(3) \vee Q(3) : |3| = 3 \text{ or } 3 = -3 \quad (\textbf{F})$$

Now consider,

$$Q(x) \Rightarrow P(x) : \text{if } x = -3\text{, then } |x| = 3;$$

this is an open sentence.

$x = -3$, $Q(-3) \Rightarrow P(-3)$: if $-3 = -3$, then $|-3| = 3$.

Since both hypothesis and conclusion are true, this statement is **T**. This is the *everyday thought*.

$x = 2$, $Q(2) \Rightarrow P(2)$: if $2 = -3$, then $|2| = 3$.

Since the hypothesis is false, this implication statement is **T**.

$x \neq -3$, since the hypothesis is false, the implication statement $Q(x) \Rightarrow P(x)$ is **T**.

Thus, *for all choices of* $x \in \mathbb{R}$, the open sentence

$$Q(x) \Rightarrow P(x)$$

is true. In other words, the open sentence

$$\text{if } x = -3, \text{ then } |x| = 3$$

is true for $x = -3$ case, as well as for all other choices of values of x. In everyday logic, we only consider the case $x = -3$. The above open sentence is a true statement whether the value of x is -3 or not.

Definition 2.15 (Converse)**.** The implication $Q \Rightarrow P$ is called the converse of $P \Rightarrow Q$.

Definition 2.16 (Biconditional)**.** Given statements P and Q, the biconditional of P and Q is the statement

$$(P \Rightarrow Q) \wedge (Q \Rightarrow P), \quad \text{denoted } P \Leftrightarrow Q$$

That is, P only if Q, and, P if Q.

We say,

$$\begin{cases} P \text{ if and only if } Q \text{ (abbreviated as } P \text{ iff } Q) \\ P \text{ is equivalent to } Q \\ P \text{ is necessary } (Q \Rightarrow P) \text{ and sufficient } (P \Rightarrow Q) \text{ for } Q \end{cases}$$

The truth table is

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

Note that $P \Leftrightarrow Q$ is true only when both P and Q are true or false.

Remark 2.17. Biconditional statements arise in mathematical definitions; the way to formally talk about that is to introduce the notion of *characterization*. Suppose some concept or object is expressed via an open sentence $P(x)$ over a domain S, and suppose $Q(x)$ is another open sentence concerning the same concept over the same domain S. Then $P(x)$ is said to be characterized by $Q(x)$ if for every $x \in S$, the statement $P(x) \Leftrightarrow Q(x)$ is true. For example a characterization for odd numbers is *a number n is odd if and only if $n-1$ is even.*

Compound Statements

Definition 2.18 (Compound Statements)**.** A compound statement is a statement consisting of at least one statement involving at least one logical connectives ($\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$). Each statement in a compound statement is called a component statement. The biconditional $P \Leftrightarrow Q$ is an example with component statements $P \Rightarrow Q$ and $Q \Rightarrow P$

Definition 2.19 (Tautology and Contradiction)**.** A compound statement is called a tautology if it is *true* for all possible combinations of truth values for its component statements. We will denote any tautology as $\top$.

A compound statement is called a contradiction if it is *false* for all possible combinations of truth values for its component statements. We will denote any tautology as $\bot$.

Example 2.20.

(1) We have seen in Example 2.7 that $P \vee (\neg P)$ is a tautology.

(2) $P \wedge (\neg P)$ is a contradiction.

P	$\neg P$	$P \wedge (\neg P)$
T	**F**	**F**
F	**T**	**F**

(3) $(P \wedge (P \Rightarrow Q)) \Rightarrow Q$, “assume P and also assume P implies Q, then Q” , is a tautology. We check by building the truth table.

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

(3) $S : ((P \Rightarrow Q) \wedge (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R)$ is a tautology.

P	Q	R	$P \Rightarrow Q$	$Q \Rightarrow R$	$(P \Rightarrow Q) \wedge (Q \Rightarrow R)$	$P \Rightarrow R$	$((P \Rightarrow Q) \wedge (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R)$
T	**T**	**T**	**T**	**T**	**T**	**T**	**T**
T	**T**	**F**	**T**	**F**	**F**	**F**	**T**
T	**F**	**T**	**F**	**T**	**F**	**T**	**T**
T	**F**	**F**	**F**	**T**	**F**	**F**	**T**
F	**T**	**T**	**T**	**T**	**T**	**T**	**T**
F	**T**	**F**	**T**	**F**	**F**	**T**	**T**
F	**F**	**T**	**T**	**T**	**T**	**T**	**T**
F	**F**	**F**	**T**	**T**	**T**	**T**	**T**

Logical Equivalence

Definition 2.21 (Logical Equivalence)**.** Two compound statements R and S are logically equivalent if they have the same truth value for all possible combinations of truth values for its component statements. We denote this as

$$R \equiv S$$

R and S are logically equivalent if and only if the biconditional statement $R \Leftrightarrow S$ is a tautology.

Theorem 2.22. *Let P and Q be statements, then*

$$(P \Rightarrow Q) \equiv ((\neg P) \vee Q)$$

Proof. We build the truth table and compare the truth values.

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

So comparing the truth values of $P \Rightarrow Q$ and $(\neg P) \vee Q$ we see $(P \Rightarrow Q) \equiv ((\neg P) \vee Q)$, and the final column also tells us that $(P \Rightarrow Q) \Leftrightarrow ((\neg P) \vee Q)$ is a tautology. □

Theorem 2.23 (Laws of Logical Equivalence)**.** *Let P, Q and R be statements, and let $\top$ and $\bot$ be a tautology and contradiction respectively, then*

(L1) *Identity laws*

$$P \vee \bot \equiv P$$

$$P \wedge \top \equiv P$$

(L2) *Domination laws*

$$P \vee \top \equiv \top$$

$$P \wedge \bot \equiv \bot$$

(L3) *Double Negation law*

$$\neg(\neg P) \equiv P$$

(L4) *Commutative laws*

$$P \vee Q \equiv Q \vee P$$

$$P \wedge Q \equiv Q \wedge P$$

(L5) *Associative laws*

$$P \vee (Q \vee R) \equiv (P \vee Q) \vee R$$

$$P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R$$

(L6) *Distributive laws*

$$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$$

$$P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$$

(L7) *De Morgan's laws*

$$\text{(L7a)} \quad \neg(P \vee Q) \equiv (\neg P) \wedge (\neg Q)$$

$$\text{(L7b)} \quad \neg(P \wedge Q) \equiv (\neg P) \vee (\neg Q)$$

Proof. We simply have to build the appropriate truth tables. For example, for (L7a) we have

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

Comparing the truth values, we see $\neg(P \vee Q) \equiv (\neg P) \wedge (\neg Q)$. □

Example 2.24. Show $\neg(P \Rightarrow Q) \equiv (P \wedge (\neg Q))$

Method 1. Build truth table

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

Comparing the truth values, we see $\neg(P \Rightarrow Q) \equiv (P \wedge (\neg Q))$.

Method 2. Use the logical equivalence laws

$$\begin{aligned} \neg(P \Rightarrow Q) &\equiv \neg((\neg P) \vee Q) && \text{by Theorem 2.22} \\ &\equiv \neg(\neg P) \wedge (\neg Q) && \text{by De Morgan's laws} \\ &\equiv P \wedge (\neg Q) && \text{by Double Negation law} \end{aligned}$$

Example 2.25. Show $((\neg Q) \Rightarrow (P \wedge \neg P)) \equiv Q$

Method 1. Build truth table (sure, but a tedious way)

Method 2. Use the logical equivalence laws

$$\begin{aligned} ((\neg Q) \Rightarrow (P \wedge \neg P)) &\equiv (\neg(\neg Q) \vee (P \wedge \neg P)) && \text{by Theorem 2.22} \\ &\equiv (\neg(\neg Q) \vee \bot) && \text{by Example 2.20 (2)} \\ &\equiv \neg(\neg Q) && \text{by Identity laws} \\ &\equiv Q && \text{by Double Negation law} \end{aligned}$$

The above statement says "if negation of Q implies a contradiction, then Q is true".

Example 2.26. Show $((P \wedge \neg Q) \Rightarrow (R \wedge \neg R)) \equiv (P \Rightarrow Q)$

Method 1. Build truth table (sure, but a tedious way)

Method 2. Use the logical equivalence laws

$$\begin{aligned} ((P \wedge \neg Q) \Rightarrow (R \wedge \neg R)) &\equiv (\neg(P \wedge \neg Q) \vee (R \wedge \neg R)) && \text{by Theorem 2.22} \\ &\equiv (\neg(P \wedge \neg Q) \vee \bot) && \text{by Example 2.20 (2)} \\ &\equiv \neg(P \wedge \neg Q) && \text{by Identity laws} \\ &\equiv \neg P \vee \neg(\neg Q) && \text{by De Morgan's laws} \\ &\equiv \neg P \vee Q && \text{by Double Negation law} \\ &\equiv P \Rightarrow Q && \text{by Theorem 2.22} \end{aligned}$$

The above equivalence is the "*proof by contradiction*". To show $P \Rightarrow Q$, do the following. Assume the hypothesis P is true but the conclusion Q is false. If you can deduce a contradiction $(R \wedge \neg R)$, then $P \Rightarrow Q$ is true.

Quantified Statements

Discussion 2.27 (Quantifiers)**.** Let $P(x)$ be an open sentence over a domain S. Recall that $P(x)$ becomes a statement once we specify an $x \in S$. We can produce specific kinds of statements from this open sentence called quantified statements.

- *for all $x \in S,\ P(x)$ is true.*

  The phrase "for all" is referred to as the universal quantifier and is denoted by the symbol $\forall$. Other ways to express the universal quantifier are "for every", "for any" and "for each". Symbolically, we express the universally quantified statement as

  $$\forall x \in S,\ P(x)$$

  The statement is true if $P(x)$ is true for every $x \in S$.

- *there exists $x \in S$ such that $P(x)$ is true.*

  The phrase "there exists" is referred to as the existential quantifier and is denoted by the symbol $\exists$. Symbolically, we express the existentially quantified statement as

  $$\exists x \in S,\ P(x)$$

  The statement is true if $P(x)$ is true for at least one $x \in S$.

Example 2.28. Consider the open sentence

$$P(n) : n^2 + n \text{ is even}$$

with domain $\mathbb{Z}$, the set of integers. Then, we have statements

$$\begin{aligned} \text{for all } n \in \mathbb{Z}, n^2 + n \text{ is even.} \qquad & \forall n \in \mathbb{Z},\ P(n) \qquad (\mathbf{T}) \\ \text{there exists an } n \in \mathbb{Z} \text{ such that } n^2 + n \text{ is even.} \qquad & \exists n \in \mathbb{Z},\ P(n) \qquad (\mathbf{T}) \end{aligned}$$

Discussion 2.29 (Negation of Quantified Statements)**.**

$$\begin{aligned} \neg(\forall x \in S,\ P(x)) &= \text{it is not the case that for all } x \in S, P(x) \text{ is true.} \\ &= \text{there exists } x \in S \text{ such that } P(x) \text{ is false.} \\ &= \exists x \in S,\ \neg P(x) \end{aligned}$$

$$\begin{aligned} \neg(\exists x \in S,\ P(x)) &= \text{it is not the case that there exists } x \in S \text{ such that } P(x) \text{ is true.} \\ &= \text{for all } x \in S, P(x) \text{ is false.} \\ &= \forall x \in S,\ \neg P(x) \end{aligned}$$

Discussion 2.30 (Summarising Negation Rules).

$$\text{under negation} \begin{cases} \wedge \leftrightarrow \vee \\ \forall \leftrightarrow \exists \\ P(x) \leftrightarrow \neg P(x) \end{cases}$$

Discussion 2.31 (Double Quantifiers and their Negation). Let $x \in S$ and $y \in T$ be variables. Consider,

$$\forall x \in S,\ \forall y \in T,\ P(x,y)$$

for all $x \in S$ and $y \in T$, $P(x,y)$ is true.

The negation is

$$\begin{aligned} \neg(\forall x \in S,\ \forall y \in T,\ P(x,y)) &\equiv \exists x \in S, \neg(\forall y \in T,\ P(x,y)) \\ &\equiv \exists x \in S,\ \exists y \in T,\ \neg P(x,y) \end{aligned}$$

For example, consider the statement *for all $x \in \mathbb{R}$ and $y \in \mathbb{R}$, $x^2 + y^2 > 0$.*

Negation: *there exists $x \in \mathbb{R}$ and $y \in \mathbb{R}$ such that $x^2 + y^2 \leqslant 0$.*

This is **T**, since for $x = y = 0$ we have $x^2 + y^2 = 0$.

Similarly,

$$\begin{aligned} \neg(\forall x \in S,\ \exists y \in T,\ P(x,y)) &\equiv \exists x \in S, \neg(\exists y \in T,\ P(x,y)) \\ &\equiv \exists x \in S,\ \forall y \in T,\ \neg P(x,y) \end{aligned}$$

In other words,

$$\begin{aligned} &\neg(\text{for all } x \in S, \text{there exists } y \in T \text{ such that } P(x,y) \text{ is true}) \\ &\qquad \equiv \text{there exists } x \in S \text{ such that for all } y \in T, P(x,y) \text{ is true} \end{aligned}$$

Finally,

$$\neg(\exists x \in S,\ \forall y \in T,\ P(x,y)) \equiv \forall x \in S,\ \exists y \in T,\ \neg P(x,y)$$
$$\neg(\exists x \in S,\ \exists y \in T,\ P(x,y)) \equiv \forall x \in S,\ \forall y \in T,\ \neg P(x,y)$$

Example 2.32 (Finding Negation). We'll negate the following statement

for all integers a, b, if their product is even, then a is even or b is even

To find the negation, we identify the component statements and re-write symbolically. Consider the following open sentences over $\mathbb{Z}$ as the domain

$P(x,y)$: the product xy is even.

$Q(x)$: x is even.

Using these open sentences, our statement is

$$\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z},\ P(a,b) \Rightarrow (Q(a) \vee Q(b))$$

To negate this statement, we need to recall how to negate the implication. We can do this using the logical equivalence laws.

> For statements U, V, what could be the $\neg(U \Rightarrow V)$? Recall from Theorem 2.22 that
>
> $$(U \Rightarrow V) \equiv (\neg U \vee V)$$
>
> Therefore,
>
> $$\begin{aligned} \neg(U \Rightarrow V) &\equiv \neg(\neg U \vee V) \\ &= \neg(\neg U) \wedge \neg V && \text{by De Morgan's Laws} \\ &= U \wedge \neg V && \text{by Double Negation Law} \end{aligned}$$
>
> Therefore, (negation of $U \Rightarrow V$) is (U and not V).

Let's go back to our problem,

$$\begin{aligned} &\neg(\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}, P(a,b) \Rightarrow (Q(a) \vee Q(b))) \\ &\qquad \equiv \exists a \in \mathbb{Z},\ \exists \in \mathbb{Z}, \neg(P(a,b) \Rightarrow (Q(a) \vee Q(b)) \\ &\qquad \equiv \exists a \in \mathbb{Z},\ \exists \in \mathbb{Z}, P(a,b) \wedge \neg(Q(a) \vee Q(b)) \\ &\qquad \equiv \exists a \in \mathbb{Z},\ \exists \in \mathbb{Z}, P(a,b) \wedge (\neg Q(a) \wedge \neg Q(b)) && \text{by De Morgan's Laws} \end{aligned}$$

Thus, the negation of our statement is

there exist integers a, b such that their product is even and *a is odd* and *b is odd*

3. Methods of Proof I. Direct Proof & Proof by Contrapositive

Trivial and Vacuous Proofs

Example 3.1. Let $x \in \mathbb{R}$, show that if $0 < x < 1$, then $x^2 - 2x + 2 > 0$.

Answer. We first re-phrase the given statement symbolically by identifying the open sentences and the quantifier. Consider the following open sentences over the domain $\mathbb{R}$

$$P(x) : 0 < x < 1$$

$$Q(x) : x^2 - 2x + 2 > 0$$

So our statement is

$$R : \forall x \in \mathbb{R},\ P(x) \Rightarrow Q(x)$$

Note that by completing the square we have $x^2 - 2x + 2 = (x-1)^2 + 1 > 0$. That is, $Q(x)$ is true for every $x \in \mathbb{R}$. Recall that an implication $U \Rightarrow V$ is true if V is true, regardless of the truth value of U. Hence, in our case, the statement R is true since $Q(x)$ is, for every $x \in \mathbb{R}$.

This type of proof is called a trivial proof, one where the conclusion is always true. □

Example 3.2. Let $x \in \mathbb{R}$, show that if $x^2 - 2x + 2 \leqslant 0$, then $x^3 \geqslant 0$.

Proof. Our statement is

$$R : \forall x \in \mathbb{R},\ P(x) \Rightarrow Q(x)$$

where

$$P(x) : x^2 - 2x + 2 \leqslant 0$$

$$Q(x) : x^3 \geqslant 0$$

Our observations in the previous example tell us that $P(x)$ is false for every $x \in \mathbb{R}$. Recall that an implication $U \Rightarrow V$ is true if U is false, regardless of the truth value of V. Hence, in our case, the statement R is true since $P(x)$ is false, for every $x \in \mathbb{R}$.

This type of proof is called a vacuous proof, one where the hypothesis is always false. □

Direct Proofs

Discussion 3.3. Let $P(x)$ and $Q(x)$ be open sentences over a domain S. Suppose our goal is to show that $P(x) \Rightarrow Q(x)$ is true for every $x \in S$, that is, we wish to show the quantified statement

$$\forall x \in S,\ P(x) \Rightarrow Q(x) \tag{$*$}$$

is true. Now, recall that if some $x \in S$, $P(x)$ is false, then the implication statement is true (vacuously). Hence, we need only be concerned with showing that $(*)$ is true for those $x \in S$ for which P(x) is true.

In a direct proof for $(*)$, we consider an arbitrary element $x \in S$ for which $P(x)$ is true and show that $Q(x)$ is true as well for this element x.

Example 3.4. For every odd integer n, show that $3n + 7$ is even.

Answer. We first re-write the statement

$$\forall n \in \mathbb{Z}, \text{ if } \underbrace{n \text{ is odd}}_{P(n)}, \text{ then } \underbrace{3n+7 \text{ is even}}_{Q(n)}$$

> For questions concerning the parity of integers, proceed as follows.
>
> (i) an integer n is even *if and only if* $n = 2k$ for some integer k.
>
> (ii) an integer n is odd *if and only if* $n = 2k + 1$ for some integer k.

Suppose n is odd (as $P(n)$ is only true for such integers), we need to show $3n + 7$ is even. Since n is odd, we can write $n = 2k + 1$ for some integer k. Therefore

$$3n + 7 = 3(2k + 1) + 7 = 6k + 10 = 2(3k + 5)$$

Since $3k + 5$ is an integer, $3n + 7 = 2(3k + 5)$ is even. □

Remark 3.5. For a positive integer m, recall from Example 1.18 that we say k is congruent to ℓ modulo m, denoted $k \equiv \ell \bmod m$,

if and only if the difference $k - \ell$ is divisibile by m

if and only if k and ℓ leave the same remainder when divided by m

Example 3.6. For an integer n, show that $n^2 \equiv 0, 1 \bmod 4$. In other words,

for a square n^2, the remainder when divided by 4 cannot be 2 or 3.

Experiment. Before we attempt to give a proof, let us first gain insight by experimenting

n	1	2	3	4	5	6	7	8	9	10	11	12
n^2	1	4	9	16	25	36	49	64	81	100	121	144
n^2 mod 4	1	0	1	0	1	0	1	0	1	0	1	0

It appears that

$$\begin{cases} \text{if } n \text{ is odd, then } n^2 \equiv 1 \bmod 4 \\ \text{if } n \text{ is even, then } n^2 \equiv 0 \bmod 4 \end{cases}$$

Proof. Suppose n is an integer, then n is either even or odd. Suppose first that n is even, we show that $n^2 \equiv 0 \bmod 4$. We can write $n = 2k$ for some integer $k \in \mathbb{Z}$. Then,

$$n^2 = (2k)^2 = 4k^2 \equiv 0 \bmod 4$$

Suppose now that n is odd, we show that $n^2 \equiv 1 \bmod 4$. We can write $n = 2\ell + 1$ for some integer $\ell \in \mathbb{Z}$. Then,

$$n^2 = (2\ell + 1)^2 = 4\ell^2 + 4\ell + 1 = 4(\ell^2 + \ell) + 1 \equiv 1 \bmod 4$$

Therefore, for every integer n, we have $n^2 \equiv 0, 1 \bmod 4$. □

Lemma 3.7. *For an integer n, $n^2 + n$ is even.*

Proof. We first make the crucial observation that $n^2 + n = n(n+1)$. We now show that $n(n+1)$ is even, by first considering the case when n is even, and then considering the case when n is odd.

Suppose first that n is even, in which case $n = 2k$ for some integer k. Then,

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

since $k(2k+1)$ is an integer, $n^2 + n$ is even.

Now suppose that n is odd, in which case we write $n = 2\ell + 1$ for some integer ℓ. Then,

$$n^2 + n = n(n+1) = (2\ell+1)(2\ell+2) = 2(2\ell+1)(\ell+1),$$

since $(2\ell+1)(\ell+1)$ is an integer, $n^2 + n$ is even.

Therefore $n^2 + n$ is even for any integer n. □

Discussion 3.8. Let's revisit our experiment in Example 3.6, this time with the last column computing the remainder when divided by 8.

n	1	2	3	4	5	6	7	8	9	10	11	12
n^2	1	4	9	16	25	36	49	64	81	100	121	144
n^2 mod 8	1		1		1		1		1		1	

It appears that when n is odd, $n^2 \equiv 1 \bmod 8$. Is this true for every odd integer n?

Proposition 3.9. *For an odd integer n, $n^2 \equiv 1$ mod 8.*

Proof. Since n is odd, we can write $n = 2k + 1$ for some integer k. Then,

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

By Lemma 3.7, $k(k+1)$ is even, so say $k(k+1) = 2\ell$ for an integer ℓ. Therefore,

$$n^2 = 4k(k+1) + 1 = 8\ell + 1 \equiv 1 \bmod 8$$

This completes the proof. □

Proof by Contrapositive

Discussion 3.10 (Contrapositive of an Implication)**.** To prove an implication $P \Rightarrow Q$ is the same as proving its contrapositive $\neg Q \Rightarrow \neg P$.

Theorem 3.11. *Let P and Q be statements, then $(P \Rightarrow Q) \equiv (\neg Q \Rightarrow \neg P)$.*

Proof. We know now that the most optimal way to prove this is not via truth tables but by using logical equivalence laws.

$$\begin{aligned}
\neg Q \Rightarrow \neg P &\equiv \neg(\neg Q) \vee \neg P && \text{by Theorem 2.22} \\
&\equiv Q \vee \neg P && \text{by Double Negation law} \\
&\equiv \neg P \vee Q && \text{by Commutative Laws} \\
&\equiv P \Rightarrow Q && \text{by Theorem 2.22}
\end{aligned}$$

□

Example 3.12. Let $x \in \mathbb{Z}$. Show that if $\underbrace{5x - 7 \text{ is even,}}_{P(x)}$ then $\underbrace{x \text{ is odd}}_{Q(x)}$.

Symbolically, we have $(\forall x \in \mathbb{Z},\ P(x) \Rightarrow Q(x))$. The contrapositive of this statement is then

$$\forall x \in \mathbb{Z},\ \neg Q(x) \Rightarrow \neg P(x)$$

which in words is *for all $x \in \mathbb{Z}$, if x is not odd (even), then $5x - 7$ is not even (odd).*

Proof. We prove the contrapositive. Suppose x is even, we can write $x = 2n$ for some integer n. Then,

$$5x - 7 = 5(2n) - 7 = 10n - 7 = 2(5n - 4) + 1$$

Since $5n - 4$ is an integer, therefore $5x - 7$ is odd. This completes the proof. □

Remark 3.13. While a direct proof of Example 3.12, it will be more complicated. The hypothesis is $5x - 7$ is even, so we can write $5x - 7 = 2k$ for some integer k. Solving for x, we get

$$x = \frac{2k + 7}{5},$$

a fraction! It is not immediately obvious why this fraction is an odd integer. Since x is an integer, $2k + 7$ must be divisible by 5 (notation: $5 \mid (2k + 7)$). So k must have some special property. If we can understand k, then we may be able to give direct proof.

Direct Proof of Example 3.12. Since $5x - 7$ is even, so we can write $5x - 7 = 2k$ for some integer k. Solving for x, we get

$$x = \frac{2k + 7}{5}.$$

Since x is an integer, $2k + 7$ must be divisible by 5. Now, $2k + 7 = 2(k + 1) + 5$, and therefore $5 \mid (2k + 7)$ is equivalent to $5 \mid 2(k + 1)$. Since 2 and 5 are coprime, 5 must divide $k + 1$. Thus, we may write $k + 1 = 5\ell$ for an integer ℓ. So, $k = 5\ell - 1$ and we have

$$x = \frac{2(5\ell - 1) + 7}{5} = \frac{10\ell + 5}{5} = 2\ell + 1$$

Since ℓ is an integer, x is odd. This completes the proof. □

As you see, proof by contrapositive was more straightforward than a direct proof.

Biconditional Statements

Recall that, by definition $(P \Leftrightarrow Q) \equiv (P \Rightarrow Q) \wedge (Q \Rightarrow P)$. So, to prove P if and only if Q, we must prove $P \Rightarrow Q$ *and* $Q \Rightarrow P$.

Example 3.14. An integer n is even if and only if n^2 is even.

We first determine the logical structure, for which we start by identifying the open sentences

$$P(n) : n \text{ is even.}$$
$$Q(n) : n^2 \text{ is even.}$$

So, what we're being asked to prove is

$$\forall n \in \mathbb{Z},\ P(n) \Leftrightarrow Q(n)$$

Proof. We need to prove

$$P(n) \Rightarrow Q(n) : \text{if } n \text{ is even, then } n^2 \text{ is even; and} \tag{1}$$

$$Q(n) \Rightarrow P(n) : \text{if } n^2 \text{ is even, then } n \text{ is even.} \tag{2}$$

Let's first show (1). When n is even, we can write $n = 2k$ for some $k \in \mathbb{Z}$. Then,

$$n^2 = (2k)^2 = 2(2k^2).$$

Since $2k^2$ is an integer, n^2 is even.

Let's now prove (2). Our initial strategy would be a direct proof which would look like

Since n^2 is even, we may write $n^2 = 2k$ for some integer k. Then,
solving n gets us $n = \sqrt{2k}$...?! We need to change our strategy.

So, we'll prove the contrapositive $\neg P(n) \Rightarrow \neg Q(n)$.

Assume n is odd, we will show then that n^2 is also odd. Since n is odd, we may write $n = 2k+1$ for some integer k. Then,

$$\begin{aligned} n^2 &= (2k+1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1. \end{aligned}$$

Since $2k^2 + 2k$ is an integer, n^2 is odd. □

Remark 3.15. (Proving) $P \Rightarrow Q$ is equivalent to (proving) its contrapositive $\neg Q \Rightarrow \neg P$. However, it is *not* the same thing as $\neg P \Rightarrow \neg Q$.

What we are saying is: to show *if P is true, then Q is true*, we instead can show

if Q is false, then P is false.

Proof by Cases

Recall that, by definition $(P \Leftrightarrow Q) \equiv (P \Rightarrow Q) \wedge (Q \Rightarrow P)$. So, to prove P if and only if Q, we must prove $P \Rightarrow Q$ *and* $Q \Rightarrow P$.

Example 3.16. Let x, $y \in \mathbb{Z}$. Show that x and y have the same parity (are both odd or both even) *if and only* if $x + y$ is even.

Scratch Notes. As we have a biconditional statement, we need to prove two implications

$$\text{if } x \text{ and } y \text{ have the same parity, then } x + y \text{ is even.} \tag{1}$$

$$\text{if } x + y \text{ is even, then } x \text{ and } y \text{ have the same parity.} \tag{2}$$

To prove (1) where we assume x and y have the same parity, we are presented with, and therefore consider, two *cases*.

Case 1. x and y are both even. So, $x = 2k$ and $y = 2\ell$ for some $k, \ell \in \mathbb{Z}$.

Case 2. x and y are both odd. So, $x = 2k + 1$ and $y = 2\ell + 1$ for some $k, \ell \in \mathbb{Z}$.

⚠ For two independent variables, x and y in our case, we must use different k, $\ell \in \mathbb{Z}$.

To prove (2), giving a direct proof may turn out to be a bit challenging. So, we instead prove the contrapositive. That is, we show that *if x and y have opposite parity, then $x + y$ is odd.* Once again, we are presented with, and therefore consider, two *cases*.

Case 1. x is even and y is odd. So, $x = 2k$ and $y = 2\ell + 1$ for some $k, \ell \in \mathbb{Z}$.

Case 2. x is odd and y is even. So, $x = 2k + 1$ and $y = 2\ell + 1$ for some $k, \ell \in \mathbb{Z}$.

Note that these two cases are *symmetric in x and y.* That is, if the first case considered as an open sentence $R(x, y)$, then the second case is $R(y, x)$. Hence, by symmetry, we only have to do one case. That is, whatever proof you give for Case 1., the proof for Case 2. will look exactly the same, except you will have switched the roles of x and y.

In such a situation, we say without loss of generality and prove one of the cases, say Case 1. and assume x is even and y is odd.

Proof. We leave it to the reader to produce a proof for this example. □

4. More on Methods of Proof I.

Divisibility of Integers

Definition 4.1. For $a, b \in \mathbb{Z}$, we say a divides b if (and only if) there exists an integer c such that $b = ac$. We have the following notation,

$$a \text{ divides } b : a \mid b$$

$$a \textit{ does not } \text{divide } b : a \nmid b$$

Lemma 4.2. *If $a \mid b$ and $b \mid c$, then $a \mid c$.*

Proof. Since $a \mid b$ and $b \mid c$, there exist integers d and e such that

$$b = ad \quad \text{and} \quad c = be$$

Then, $c = be = (ad)e = a(de)$. Since de is an integer, $a \mid c$. □

Proposition 4.3. *If a and b are integers that have the same parity, then $4 \mid (a^2 - b^2)$.*

Experiment.

$$a = 5,\ b = 3 \text{ (both odd) } a^2 - b^2 = 25 - 9 = 16 \text{ and } 4 \mid 16$$

$$a = 6,\ b = 2 \text{ (both even) } a^2 - b^2 = 36 - 4 = 32 \text{ and } 4 \mid 32$$

$$\vdots$$

do more experiments.

Proof. We encounter two cases.

Case 1. Suppose a and b are even. So we may write $a = 2k$ and $b = 2\ell$ for integers k, ℓ. Then,

$$\begin{aligned} a^2 - b^2 &= (2k)^2 - (2\ell)^2 \\ &= 4(k^2 - \ell^2) \end{aligned}$$

Since $k^2 - \ell^2$ is an integer, $4 \mid (a^2 - b^2)$.

Case 2. Suppose a and b are odd. So we may write $a = 2k + 1$ and $b = 2\ell + 1$ for integers k, ℓ. Then,

$$\begin{aligned} a^2 - b^2 &= (2k+1)^2 - (2\ell+1)^2 \\ &= (4k^2 + 4k + 1) - (4\ell^2 + 4\ell + 1) \\ &= 4(k^2 - \ell^2 + k - \ell) \end{aligned}$$

Since $k^2 - \ell^2 + k - \ell$ is an integer, $4 \mid (a^2 - b^2)$.

□

Remark 4.4. To *understand* why this statement in Proposition 4.3 is true, we present a more illuminating argument. Note that,

$$a^2 - b^2 = (a+b)(a-b)$$

We have seen earlier that if a and b have the same parity, then $a+b$ is even. Since $a - b = (a+b) - 2b$, and since $a+b$ and $2b$ are both even, we note that $a-b$ is also even. So, $a+b$ and $a-b$ are divisible by 4. We do this more formally.

Lemma 4.5. *For two integers a and b with the same parity, both $a+b$ and $a-b$ are even.*

Proof. We leave the proof to the reader. □

Another Proof of Proposition 4.3. Since $a+b$ and $a-b$ are even, by the lemma above, we write $a+b = 2k$ and $a-b = 2\ell$ for integers k, ℓ. So we have $a^2 - b^2 = (a+b)(a-b) = (2k)(2\ell) = 4k\ell$. Since $k\ell$ is an integer, $4 \mid (a^2 - b^2)$. □

Congruence

Let n be a positive integer such that $n \geqslant 2$

Definition 4.6. For two integers a and b, a is congruent to b modulo n, denoted

$$\begin{aligned} a \equiv b \bmod n \text{ if and only if } & n \mid (a-b) \\ \text{if and only if } & a - b = nk, \text{ for some } k \in \mathbb{Z} \\ \text{if and only if } & a = b + nk, \text{ for some } k \in \mathbb{Z} \\ \text{if and only if } & a \text{ and } b \text{ have the same remainder when divided by } n \end{aligned}$$

Proposition 4.7 (Arithmetic Properties of Congruence)**.** *Suppose $a \equiv b$ mod n and $c \equiv d$ mod n, then*

(1) add side-by-side

$$a + c \equiv b + d \text{ mod } n$$

(2) multiply side-by-side

$$ac \equiv bd \text{ mod } n$$

Proof. By hypothesis, $a = b + nk$ and $c = d + n\ell$ for integer k, ℓ. Then, adding and multiplying side-by-side we get

$$\begin{aligned} a + c &= (b + nk) + (d + n\ell) \\ &= (b + d) + n(k + \ell) \\ ac &= (b + nk)(d + n\ell) \\ &= bd + nb\ell + ndk + n^2 k\ell \\ &= bd + n(b\ell + dk + nk\ell) \end{aligned}$$

Therefore $a + c \equiv b + d$ mod n and $ac \equiv bd$ mod n. □

Proposition 4.8. *For an integer n, show that if $n^2 \not\equiv n$ mod 3, then $n \equiv 2$ mod 3.*

Strategy.

(1) Experiment

$$n = 6,\ 6 \equiv 0 \bmod 3, 6^2 = 36 \equiv 6 \bmod 3$$

$$n = 5,\ 5 \equiv 2 \bmod 3, 5^2 = 25 \not\equiv 5 \bmod 3$$

$$\vdots$$

(2) Try direct proof.

(3) Try contrapositive: if $n \not\equiv 2$ mod 3, then $n^2 \equiv n$ mod 3. Note that $n \not\equiv 2$ mod 3 is equivalent to $n \equiv 0, 1$ mod 3. So, we prove

$$\text{if } n \equiv 0, 1 \bmod 3, \text{ then } n^2 \equiv n \bmod 3.$$

Proof. We prove the contrapositive, and so we encounter two cases.

Case 1. Suppose $n \equiv 0$ mod 3, then by Proposition 4.7

$$n^2 \equiv 0^2 \bmod 3$$

Therefore $n^2 \equiv 0 \equiv n$ mod 3. Since $k^2 - \ell^2$ is an integer, $4 \mid (a^2 - b^2)$.

Case 2. Suppose $n \equiv 1$ mod 3, then by Proposition 4.7

$$n^2 \equiv 1^2 \bmod 3$$

Therefore $n^2 \equiv 1 \equiv n$ mod 3.

Hence in both cases $n^2 \equiv n$ mod 3. □

Example 4.9. Let $n \in \mathbb{Z}$. If $11n - 7$ is even, then n is odd.

Earlier we proved statements of this type by proving the contrapositive: if n is even, $11n - 7$ is odd. But now using congruence relations, we can give a direct proof.

Proof. Since $11n - 7$ is even, we have $11n - 7 \equiv 0$ mod 2, and naturally $7 \equiv 7$ mod 2. Adding the two we get, using Proposition 4.7

$$11n \equiv 7 \bmod 2$$

Let's focus on the right hand side of the congruence relation; naturally we have $7 \equiv 1$ mod 2. For the left hand side, note that we have $11 \equiv 1$ mod 2 and naturally $n \equiv n$ mod 2; multiplying, using Proposition 4.7, we have $11n \equiv n$ mod 2.

Combining $7 \equiv 1$ mod 2 and $11n \equiv n$ mod 2, we get $n \equiv 1$ mod 2. Thus, n is odd. □

Example 4.10. For all integers n, we have $n^3 \equiv n \bmod 3$.

Meaning

- n^3 and n leave the same remainder when divided by 3; or
- $n^3 - n$ is divisible by 3.

Experiment.

n	1	2	3	4	5	6	7	$\cdots$
$n \bmod 3$	1	2	0	1	2	0	1	$\cdots$
n^3	1	8	27	64	125	216	$\cdots$	$\cdots$
$n^3 \bmod 3$	1	2	0	1	2	0	$\cdots$	$\cdots$

Proof. We prove the congruence relation by treating three cases: $n \equiv 0, 1, 2 \bmod 3$. *(checking congruence relations case by case is a standard approach.)*

Case 1. Suppose $n \equiv 0 \bmod 3$, using Proposition 4.7, multiplying it with itself thrice get us $n^3 \equiv 0^3 \bmod 3$. Therefore $n^3 \equiv 0 \bmod 3$, and hence $n^3 \equiv n \bmod 3$, in this case.

Case 2. Suppose $n \equiv 1 \bmod 3$, using Proposition 4.7, multiplying it with itself thrice get us $n^3 \equiv 1^3 \bmod 3$. Therefore $n^3 \equiv 1 \bmod 3$, and hence $n^3 \equiv n \bmod 3$, in this case.

Case 3. Suppose $n \equiv 2 \bmod 3$, using Proposition 4.7, multiplying it with itself thrice get us $n^3 \equiv 2^3 \bmod 3$. Therefore

$$n^3 \equiv 8 \equiv 2 \bmod 3,$$

and hence $n^3 \equiv n \bmod 3$, in this case.

This completes the proof. □

Inequalities of Real Numbers

Example 4.11. For $x, y \in \mathbb{R}$, show that

$$\frac{1}{3}x^2 + \frac{3}{4}y^2 \geqslant xy$$

Some Basics.

(1) For every real number x, we have $x^2 \geqslant 0$.

(2) The show L.H.S. $\geqslant$ R.H.S., prove that

$$\text{L.H.S.} - \text{R.H.S.} \geqslant 0$$

In some cases, one can show this by expressing L.H.S. $-$ R.H.S. $=$ (some real number)^2.

Proof. We take the difference of the R.H.S. from the L.H.S. and get

$$\begin{aligned}\frac{1}{3}x^2+\frac{3}{4}y^2-xy &= \frac{1}{12}\left(4x^2-12xy+9y^2\right)\\ &= \frac{1}{12}\left((2x)^2-2(2x)(3y)+(3y)^2\right)\\ &= \frac{1}{12}(2x-3y)^2 \geqslant 0\end{aligned}$$

Hence,

$$\frac{1}{3}x^2+\frac{3}{4}y^2 \geqslant xy$$

for all $x, y \in \mathbb{R}$. □

Example 4.12. For $x, y, z \in \mathbb{R}$, show that

$$x^2+y^2+z^2 \geqslant xy+yz+zw$$

Experiment.

$$\begin{aligned} x=y=z=1;&\quad 1^2+1^2+1^2 = 1\cdot 1+1\cdot 1+1\cdot 1\\ x=2,\ y=-1,\ z=1;&\quad \underbrace{2^2+(-1)^2+1^2}_{=6} \geqslant \underbrace{2\cdot(-1)+(-1)\cdot 1+1\cdot 2}_{=-1}\end{aligned}$$

Proof. We take the difference of the R.H.S. from the L.H.S. and get

$$x^2+y^2+z^2-xy-yz-zw$$

> *Scratch Notes.* Our first instinct would be to somehow involve
>
> $$(x+y+z)^2 = x^2+y^2+z^2+2xy+2yz+2zw \geqslant 0$$
>
> Which the would give us,
>
> $$\begin{aligned} x^2+y^2+z^2-xy-yz-zw &= (x+y+z)^2-(2xy+2yz+2zw)-xy-yz-zw\\ &= (x+y+z)^2-(3xy+3yz+3zw)\end{aligned}$$
>
> We reach an impasse, because while $(x+y+z)^2 \geqslant 0$ but what about $3xy+3yz+3zw$, and what about the difference? We may need a different approach. We do know that $x^2-2xy+y^2=(x-y)^2 \geqslant 0$. What can we do about the remaining terms z^2, $-yz$, $-zx$?

Multiply 2 to our given expression, and we have

$$\begin{aligned} 2x^2+2y^2+2z^2-2xy-2yz-2zw &= (x^2-2xy+y^2)+(y^2-2yz+z^2)+(z^2-2zx+x^2)\\ &= (x-y)^2+(y-z)^2+(z-x)^2 \geqslant 0\end{aligned}$$

Thus, $x^2+y^2+z^2-xy-yz-zw \geqslant 0$, and hence we have proven $x^2+y^2+z^2 \geqslant xy+yz+zw$. □

Proposition 4.13 (AM $\geqslant$ GM)**.** *Given $x_1, x_2, \ldots, x_n \in \mathbb{R}_{\geqslant 0}$ (non-negative real numbers), we have*

$$\underbrace{\frac{x_1 + x_2 + \cdots + x_n}{n}}_{\textit{arithmetic mean}} \geqslant \underbrace{\sqrt[n]{x_1 x_2 \cdots x_n}}_{\textit{geometric mean}}$$

Equality holds exactly when $x_1 = x_2 = \cdots = x_n$.

Proof. The case for $n = 2$ is very useful. Let $x = x_1$ and $y = x_2$, we need to prove

$$\frac{x+y}{2} \geqslant \sqrt{xy}$$

Recall that we have assumed $x, y \geqslant 0$; let $a = \sqrt{x}$ and $b = \sqrt{y}$. Taking the relevant difference we note

$$\begin{aligned} \frac{x+y}{2} - \sqrt{xy} &= \frac{a^2+b^2}{2} - ab \\ &= \frac{1}{2}\left(a^2 - 2ab + b^2\right) = \frac{1}{2}(a-b)^2 \geqslant 0 \end{aligned}$$

Let's also look at this result for $n = 3$. Let $x = x_1$, $y = x_2$ and $z = x_3$, we need to prove

$$\frac{x+y+z}{3} \geqslant \sqrt[3]{xyz}$$

Recall that we have assumed $x, y, z \geqslant 0$; let $a = \sqrt[3]{x}$, $b = \sqrt[3]{y}$ and $c = \sqrt[3]{z}$. Taking the relevant difference we note

$$\begin{aligned} \frac{x+y+z}{3} - \sqrt[3]{xyz} &= \frac{a^3+b^3+c^3}{3} - 3abc \\ &= \frac{1}{3}\left(a^3 + b^3 + c^3 - 3abc\right) \\ &= \frac{1}{3}(a+b+c)(a^2+b^2+c^2-ab-bc-ca) \geqslant 0 \end{aligned}$$

since $a, b, c \geqslant 0$ and we've already noted that $a^2 + b^2 + c^2 - ab - bc - ca \geqslant 0$.

We'll skip the general proof. We will soon introduce a method of proof that is appropriately suited for such problems. □

Example 4.14 (Revisiting Example 4.11)**.** For $x, y \in \mathbb{R}$, show that

$$\frac{1}{3}x^2 + \frac{3}{4}y^2 \geqslant xy$$

Proof. We can use Proposition 4.13

$$\frac{1}{2}\left(\frac{1}{3}x^2 + \frac{3}{4}y^2\right) \geqslant \sqrt{\frac{1}{3}x^2 \cdot \frac{3}{4}y^2} = \sqrt{\frac{x^2y^2}{4}} = \frac{|x|\,|y|}{2}$$

$$\frac{1}{3}x^2 + \frac{3}{4}y^2 \geqslant |x|\,|y| \geqslant xy$$

□

Discussion 4.15. We have the following strategies for proving statements involving sets

(1) Use Venn diagrams.

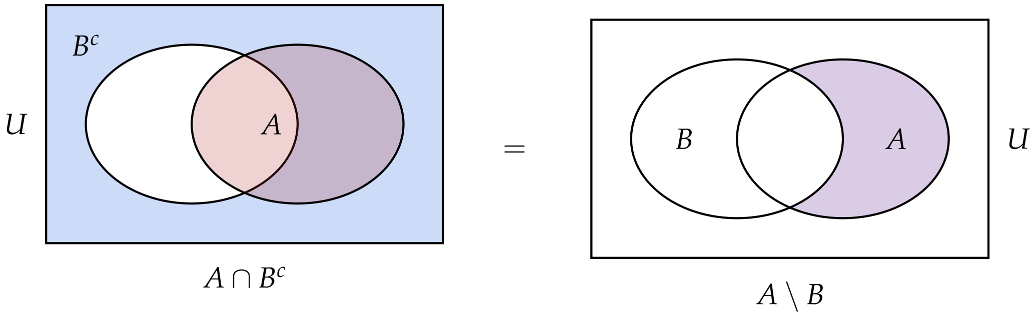
(2) Using element-wise arguments.

(3) Using basic inclusion relations among sets. For example, $A \cap B \subseteq A$, $B \subseteq A \cup B$.

Example 4.16.

(1) Show that $A \setminus B = A \cap B^c$.

Proof. We give a proof using Venn diagrams (already seen in Proposition 1.13 (1)).



Therefore $A \setminus B = A \cap B^c$, as noted by the Venn diagram above. □

(2) Show that $A \cup B = A$ if and only if $B \subseteq A$.

> *Scratch Notes.*
>
> (a) Since we are being asked to prove an "if and only if" statement, that is, a biconditional payment, we need to prove two things:
>
> $$\text{if } A \cap B = A, \text{ then } B \subseteq A \qquad \text{if } B \subseteq A, \text{ then } A \cap B = A$$
>
> (b) To show set equality $X = Y$, we need to show two inclusions: $X \subseteq Y$ and $Y \subseteq X$.
>
> (c) To show set inclusion $U \subseteq V$ is equivalent to showing that
>
> $$\text{if } x \in U, \text{ then } x \in V$$

Proof. First we show that if $A \cup B = A$, then $B \subseteq A$. Let us consider an arbitrary $x \in B$. Since $B \subseteq A \cup B$, we therefore also have $x \in A \cup B$. By hypothesis $A \cup B = A$, and hence $x \in A$. Thus, $B \subseteq A$.

Let us now show that if $B \subseteq A$, then $A \cup B = A$. For this, we need to show (i) $A \subseteq A \cup B$; and (ii) $A \cup B \subseteq A$. Note that we have (i) for free, we really need to only show (ii). Let us consider an arbitrary $x \in A \cup B$. Then $x \in A$ or $x \in B$. If $x \in A$, then we have nothing to show since $x \in A$ already. Now, if $x \in B$, then since we have our hypothesis $B \subseteq A$, we also have $x \in A$. So, in the both cases $x \in A$. Thus, we have proven that $A \cup B \subseteq A$.

This completes the proof. □

Another Proof using Set Inclusion Arguments. We first prove $A \cup B = A$ implies $B \subseteq A$, this follows immediately as

$$B \subseteq A \cup B = A.$$

Therefore $B \subseteq A$.

Let us now prove the converse: $B \subseteq A$ implies $A \cup B = A$. As noted previously, we already have $A \subseteq A \cup B$. For the other inclusion, note that since $B \subseteq A$, we have

$$A \cup B \subseteq A \cup A = A;$$

and so $A \cup B \subseteq A$. Hence $A \cup B = A$. □

Set Operations

Proposition 4.17 (Set Operation Laws)**.** *Let A, B, C be sets, then*

- *Distributive Laws*

$$\text{(a)} \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

$$\text{(b)} \quad A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

- *De Morgan's Laws*

$$\text{(a)} \quad (A \cup B)^c = A^c \cap B^c$$

$$\text{(b)} \quad (A \cap B)^c = A^c \cup B^c$$

Proof. One can prove these laws either using Venn diagrams or element-wise arguments. We leave the proof to the reader. □

Example 4.18. Show $(A \setminus B) \cap (A \setminus C) = A \setminus (B \cup C)$

Proof. Method 1. Using Venn Diagrams (gets messier as we involve more sets).

Method 2. Using set operations

$$\begin{aligned}
(A \setminus B) \cap (A \setminus C) &= (A \cap B^c) \cap (A \cap C^c) && \text{by Proposition 1.13 (1), or Example 4.16 (1)} \\
&= (A \cap A) \cap (B^c \cap C^c) \\
&= A \cap (B^c \cap C^c) \\
&= A \cap (B \cup C)^c && \text{by De Morgan's Laws} \\
&= A \setminus (B \cup C) && \text{by Proposition 1.13 (1), or Example 4.16 (1)}
\end{aligned}$$

This completes the proof. □

5. Methods of Proof II. Counterexamples, Proof by Contradiction and Existence Proofs

Counterexamples

Discussion 5.1. Our purpose is always to determine the truth value of statements. Consider a universally quantified statement

$$\forall x \in S,\ R(x)$$

Is this true or false?

If you think it is true, *prove it*.

If you think it is false, then its negation

$$\exists x \in S,\ \neg R(x)$$

is true. Therefore to show falsehood, we need to exhibit an (at least one) element $x_0 \in S$ such that $R(x_0)$ is false (that is, $\neg R(x_0)$ is true). x_0 is the called a *counterexample* to the given statement. Counterexamples prove falsehood of, disproving, universally quantified statements.

Example 5.2. The reader has shown in an assignment that if n is a sum of two squares, then

$$n \equiv 0, 1, 2 \bmod 4$$

Consider the converse: For an integer n, if $n \equiv 0, 1, 2 \bmod 4$, then n a sum of two squares.

Question. True or False? Probably false, so we seek a counterexample. We check the statement for small non-negative integers, in hopes of encountering a counterexample.

Since $n \equiv 0, 1, 2 \bmod 4$, our list is

n	0	1	2	4	5	6	8	9	10	$\cdots$
sum of squares	0^2+0^2	0^2+1^2	1^2+1^2	0^2+2^2	1^2+2^2	No.				

Answer. False. Since $6 \equiv 2 \bmod 4$, but it is not a sum of two squares. □

Example 5.3. True or False?

Let $a, b \in \mathbb{R}$ such that $a, b \neq 0$. For all $x, y \in \mathbb{R}_{>0}$, is

$$\frac{a^2}{2b^2}x^2 + \frac{b^2}{2a^2}y^2 > xy$$

Scratch Notes. We will try and prove it. If the proof goes through, the statement true and we have a proof. If the proof does not go through, then the reason why it did not could possibly give us a way to produce a counterexample.

$$\begin{aligned}
\text{L.H.S.} - \text{R.H.S.} &= \frac{a^2}{2b^2}x^2 + \frac{b^2}{2a^2}y^2 - xy \\
&= \frac{1}{2}\left(\frac{a^2}{b^2}x^2 - 2xy + \frac{b^2}{a^2}y^2\right) \\
&= \frac{1}{2}\left(\left(\frac{ax}{b}\right)^2 - 2\left(\frac{ax}{b}\right)\left(\frac{by}{a}\right) + \left(\frac{by}{a}\right)^2\right) \\
&= \frac{1}{2}\left(\frac{ax}{b} - \frac{by}{a}\right)^2 \geqslant 0
\end{aligned}$$

So, when do we get the above expression $= 0$? Exactly when

$$\frac{ax}{b} = \frac{by}{a}$$

Do such x and y exist? Well yes, consider $x = b^2$ and $y = a^2$, then

$$\frac{ax}{b} = ab = ba = \frac{by}{a}$$

Answer. False. Let $x = b^2$ and $y = a^2$. Then

$$\begin{aligned}
\text{L.H.S.} &= \frac{a^2}{2b^2}x^2 + \frac{b^2}{2a^2}y^2 \\
&= \frac{a^2}{2b^2}\cdot(b^2)^2 + \frac{b^2}{2a^2}\cdot(a^2)^2 \\
&= \frac{a^2b^2}{2} + \frac{b^2a^2}{2} \\
&= a^2b^2
\end{aligned}$$

$$\begin{aligned}
\text{R.H.S.} &= xy \\
&= a^2b^2
\end{aligned}$$

So, L.H.S. $=$ R.H.S., and therefore L.H.S. $>$ R.H.S. does not hold. □

Proof by Contradiction

Discussion 5.4. Let R be a statement. What is a proof by contradiction? The method is as follows: to show R is true, show that the negation of R leads to a contradiction $\perp$. Logical structure,

$$R \equiv (\neg R \Rightarrow \perp)$$

R	$\neg R$	$\perp$	$\neg R \Rightarrow \perp$
T	**F**	**F**	**T**
F	**T**	**F**	**F**

If the negation of R gives us a contradiction, that is, if $(\neg R \Rightarrow \perp)$ is true, since the conclusion $\perp$ is always false, the only possibility is for the hypothesis $\neg R$ to be also false. Hence R is true.

Special but useful case. If R is of the form $P \Rightarrow Q$, then to prove $P \Rightarrow Q$ we prove the following

$$\neg(P \Rightarrow Q) \Rightarrow \perp$$

Recall that

$$\neg(P \Rightarrow Q) \equiv \neg(\neg P \vee Q) \equiv P \wedge \neg Q.$$

Thus, to prove $P \Rightarrow Q$, show that

$$(P \wedge \neg Q) \Rightarrow \perp$$

The contradiction we often try to find is $S \wedge \neg S$ for some statement S. In other words, assume P is true and also assume the conclusion Q is false, then we try to find a contradiction $S \wedge \neg S$, finding an appropriate S is the heart of the proof.

Example 5.5. Suppose an integer m is such that $2 \mid m$ but $4 \nmid m$. Show that there are no integer solutions x, y to the equation

$$x^2 + 2y^2 = m$$

This is a *non-existence statement*, we use proof by contradiction to prove such statements.

Scratch Notes for Proof. Suppose we have an integer m is such that $2 \mid m$ but $4 \nmid m$, therefore $m \equiv 2 \bmod 4$. The logical structure of the statement is

Hypothesis $P(m) : m \equiv 2 \bmod 4$

Conclusion $Q(m) : x^2 + 3y^2 = m$ has no integer solution x, y

We need to show

$$\forall m \in \mathbb{Z},\ P(m) \Rightarrow Q(m)$$

To give a proof by contradiction, we assume two things: $P(m)$ and $\neg Q(m)$. That is, suppose $m \equiv 2 \bmod 4$ and that there exist integers x, y such that $x^2 + 3y^2 = m$.

How do we find a contradiction? Consider integers modulo 4, we have seen that for any integer n, we have $n^2 \equiv 0, 1 \bmod 4$. So, for the solutions x, y, we have $x^2 \equiv 0, 1 \bmod 3$ and $y^2 \equiv 0, 1 \bmod 3$. So, we have the cases

$$\begin{array}{ll}
x^2 \equiv 0 \bmod 4,\ y^2 \equiv 0 \bmod 4 & \text{So, } x^2 + 3y^2 \equiv 0 \bmod 4 \\
x^2 \equiv 1 \bmod 4,\ y^2 \equiv 0 \bmod 4 & \text{So, } x^2 + 3y^2 \equiv 1 \bmod 4 \\
x^2 \equiv 0 \bmod 4,\ y^2 \equiv 1 \bmod 4 & \text{So, } x^2 + 3y^2 \equiv 3 \bmod 4 \\
x^2 \equiv 1 \bmod 4,\ y^2 \equiv 1 \bmod 4 & \text{So, } x^2 + 3y^2 \equiv 4 \equiv 0 \bmod 4
\end{array}$$

Thus, $x^2 + 3y^2 \equiv 0, 1, 3 \bmod 4$ and therefore $x^2 + 3y^2 \not\equiv 2 \bmod 3$. But our assumption is $x^2 + 3y^2 = m \equiv 2 \bmod 4$, this our S. Hence, we have arrived at a contradiction. So, $x^2 + 3y^2 = m$ cannot have integer solutions.

Proof. Check back tomorrow for a proof. □

Discussion 5.6. We now have three methods to prove implications $P \Rightarrow Q$

$$\underset{\substack{\text{(I) Direct}\\\text{Proof}}}{P \Rightarrow Q} \quad\equiv\quad \underset{\substack{\text{(II) Proof by}\\\text{Contrapositive}}}{\neg Q \Rightarrow \neg P} \quad\equiv\quad \underset{\substack{\text{(III) Proof by}\\\text{Contradiction}}}{(P \wedge \neg Q) \Rightarrow \perp}$$

Example 5.7. Let $x \in \mathbb{R}$ and $x \neq 0$. Show that if $x + \dfrac{1}{x} < 2$, then $x > 0$.

Direct Proof. Suppose x is a non-zero real number such that $x + 1/x < 2$, we show $x < 0$. We first observe that we have

$$x + \frac{1}{x} - 2 < 0$$

Note that

$$\begin{aligned} x + \frac{1}{x} - 2 &= \frac{x^2 + 1 - 2x}{x} \\ &= \frac{(x-1)^2}{x} \end{aligned}$$

Since $(x-1)^2 \geqslant 0$ for any x, for the ration to be negative, we necessarily must have $x < 0$. This completes the proof. □

Proof by Contrapositive. We prove its contrapositive. Assume $x \geqslant 0$, since $x \neq 0$, we may assume $x > 0$. We wish to prove $x + 1/x \geqslant 2$. Using AM $\geqslant$ GM, we have

$$\frac{1}{2}\left(x + \frac{1}{x}\right) \geqslant \sqrt{x \cdot \frac{1}{x}} = 1$$

Hence $x + \dfrac{1}{x} \geqslant 2$. This completes the proof. □

Proof by Contrapositive. For the sake of contradiction, assume that $x \geqslant 0$ is a real number such that $x + 1/x < 2$ and $x > 0$. Using AM $\geqslant$ GM, we have

$$\frac{1}{2}\left(x + \frac{1}{x}\right) \geqslant \sqrt{x \cdot \frac{1}{x}} = 1$$

Hence $x + \dfrac{1}{x} \geqslant 2$. This contradicts our hypothesis, hence $x + 1/x < 2$ implies $x < 0$. □

Existence Proofs

Discussion 5.8. We now turn our attention to proving

$$\exists x \in S,\ R(x)$$

there exists an x such that $R(x)$ is true. Methods to prove existence results

(1) Exhibit $x \in S$ satisfying $R(x)$.

(2) Use other existence theorems.

(3) Use proof by contradiction. *the method of choice for proving existence results*.

Example 5.9.

for (1) Rationality of a^b, where $a, b \in \mathbb{R}$ and $a, b > 0$.

Question. Is a^b is rational or irrational?

Proof. We divide this into cases: where a and b are rational or irrational.

Case I. a is rational, b is rational

$$\begin{aligned} 2^3 &= 8 \text{ (rational)} \\ 2^{1/2} &= \sqrt{2} \text{ (irrational)} \end{aligned}$$

Case II. a is rational, b is irrational

$$\begin{aligned} 1^{\sqrt{2}} &= 1 \text{ (rational)} \\ 2^{\log_2 3} &= 3 \text{ (rational)} \\ 2^{\log_2 \sqrt{3}} &= \sqrt{3} \text{ (irrational)} \end{aligned}$$

Case III. a is irrational, b is rational

$$\begin{aligned} (\sqrt{2})^2 &= 2 \text{ (rational)} \\ (\sqrt{2})^3 &= 2\sqrt{2} \text{ (irrational)} \end{aligned}$$

Case IV. a is irrational, b is irrational

$$\begin{aligned} (\sqrt{2})^{2\log_2 3} &= 2^{\log_2 3} = 3 \text{ (rational)} \\ (\sqrt{2})^{\log_2 3} &= (2^{\log_2 3})^{1/2} = \sqrt{3} \text{ (irrational)} \end{aligned}$$

□

for (2) Show that $x^2 + 2x - 5 = 0$ has a solution in the interval $[1, 2]$.

Proof. We use the following existence result to prove this.

Theorem 5.10 (Intermediate Value Theorem)**.** *Suppose $f : [a, b] \to \mathbb{R}$ is continuous. If $f(a) < 0$ and $f(b) > 0$, then there exists a $c \in (a, b)$ such that $f(c) = 0$.*

Back to our proof. As a polynomial $f(x) = x^2 + 2x - 5$ is continuous. Since $f(1) = -2 < 0$ and $f(2) = 3 > 0$, therefore there exists a $c \in (1, 2)$ such that $f(c) = 0$. That is, $c^2 + 2c - 5 = 0$. This completes our proof. □

for (3) We look at a very fundamental counting principle.

Theorem 5.11 (Pigeonhole Principle)**.** *Suppose n objects are placed in m boxes. If $n > m$, then there exists a box containing at least two objects.*

Proof. For the sake of contradiction, suppose $n > m$ and every box contains at most one object. Since there are m boxes, it follows that there are at most m objects; that is $n \leqslant m$. This contradicts our hypothesis that $n > m$. This completes our proof. □

Example 5.12 (on the Pigeonhole Principle)**.** Let S be a set of three integers. For a non-empty subset A of S, let σ_A be the sum of elements in A. Prove that there exist two distinct nonempty subsets B and C of S such that $\sigma_B \equiv \sigma_C$ mod 6.

Experiments. Let $S = \{2, 5, 7\}$

A	$\{2\}$	$\{5\}$	$\{7\}$	$\{2,5\}$	$\{5,7\}$	$\{7,2\}$	$\{2,5,7\}$
σ_A	2	5	7	7	11	9	14

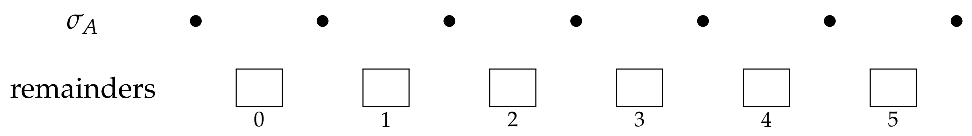
Subsets $B = \{2\}$, $\sigma_B = 2$ and $C = \{2, 5, 7\}$, $\sigma_C = 14$ are such that $\sigma_B \equiv \sigma_C$ mod 6. Also, subsets $B' = \{7\}$, $\sigma_{B'} = 7$ and $C' = \{2, 5\}$, $\sigma_{C'} = 7$ are such that $\sigma_{B'} \equiv \sigma_{C'}$ mod 6.

Let $S = \{1, 3, 8\}$

A	$\{1\}$	$\{3\}$	$\{8\}$	$\{1,3\}$	$\{3,8\}$	$\{8,1\}$	$\{1,3,8\}$
σ_A	1	3	8	4	11	9	12

Subsets $B = \{3\}$, $\sigma_B = 3$ and $C = \{1, 8\}$, $\sigma_C = 9$ are such that $\sigma_B \equiv \sigma_C$ mod 6.

Proof. Let S be a three element set. The number of non-empty subsets of S are $|\mathsf{P}(S)| - 1 = 2^3 - 1 = 7$. So, we obtain $n = 7$ integers σ_A for every non-empty subset A of S. These are our objects. While there are $m = 6$ possibly remainders when an integer is divided by 6. These are our boxes.



Therefore, by the Pigeonhole Principle, there must be one box with at least two objects; that is, there must exist two sets B and C such that σ_B and σ_C leave the same remainder when divided by 6 (are in the same box). This completes the proof. □

Discussion 5.13. Previously we discussed existence proofs, that is, proving a statement of the form

$$\exists x \in S,\ R(x)$$

We wish to now discuss a proof of a variation about the above statement. Recall that the above statement says *there exists an $x \in S$ such that $R(x)$ is true*. We focus on a statement when such an x

is unique, that is, not only is $R(x)$ true for this x, x is the only element for which $R(x)$ is true. The statement is then *there exists a unique $x \in S$ such that $R(x)$ is true*, and is denoted symbolically as

$$\exists! x \in S,\ R(x)$$

So, there are two steps to proving such a statement

Step 1. Existence proof. Prove such an x exists.

Step 2. Uniqueness proof. Prove such an x is unique.

We have already discussed Step 1. For Step 2., one typically does the following

(1) If $x, y \in S$ are such that $R(x)$ and $R(y)$ is true, prove that $y = x$.

(2) If $x, y \in S$ are such that $R(x)$ and $R(y)$ is true and $y \neq x$, then show that this leads to a contradiction.

Example 5.14. Show that $x^5 + 2x - 5 = 0$ has a unique root between $x = 1$ and $x = 2$.

Proof. We are being asked to prove both an existence statement and a uniqueness statement.

(Existence) Let $f(x) = x^5 + 2x - 5$. Since $f(1) = -2 < 0$ and $f(2) = 31 > 0$, by the Intermediate Value Theorem, there exists a real number $c \in (1, 2)$ such that $f(c) = 0$.

(Uniqueness, Method 1) Suppose there exist $c_1, c_2 \in (1, 2)$ such that $f(c_1) = f(c_2) = 0$. We aim to show $c_1 = c_2$. By assumption,

$$c_1^5 + 2c_1 - 5 = f(c_1) = 0 \quad \text{and} \quad c_2^5 + 2c_2 - 5 = f(c_2) = 0$$

Taking their difference of these two equations, we obtain

$$(c_1^5 - c_2^5) + 2(c_1 - c_2) = 0 \tag{$*$}$$

> To show $c_1 = c_2$, we want to factor out $c_1 - c_2$ from the L.H.S. in $(*)$. We use the following identity: for any real numbers x, y
>
> $$x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1})$$

Factoring out $c_1 - c_2$ from the L.H.S. in $(*)$, we get

$$(c_1 - c_2)(c_1^4 + c_1^3 c_2 + c_1^2 c_2^2 + c_1 c_2^3 + c_2^4 + 2) = 0$$

> To show $c_1 = c_2$, we want to argue that the other factor $c_1^4 + c_1^3 c_2 + c_1^2 c_2^2 + c_1 c_2^3 + c_2^4 + 2$ is non-zero.

Since $1 < c_1, c_2 < 2$, we have $c_1^4,\ c_1^3 c_2,\ c_1^2 c_2^2,\ c_1 c_2^3,\ c_2^4 > 1$. Thus, we get

$$c_1^4 + c_1^3 c_2 + c_1^2 c_2^2 + c_1 c_2^3 + c_2^4 + 2 > 7$$

In particular, this factor is non-zero. Hence, necessarily $c_1 - c_2 = 0$. This completes the uniqueness proof.

(Uniqueness, Method 2) Suppose there exist $c_1, c_2 \in (1,2)$ such that $f(c_1) = f(c_2) = 0$ and $c_1 \neq c_2$. We will provide a contradiction. Since $f(x) = x^5 + 2x - 5$, we have

$$f'(x) = 5x^4 + 2 > 0.$$

Therefore $f(x)$ is a strictly increasing function. We may assume, without loss of generality, that $c_1 < c_2$. Then, since f is increasing, we have $f(c_1) < f(c_2)$. This contradicts our assumption that $f(c_1) = f(c_2) = 0$. Hence, necessarily $c_1 = c_2$. This completes the uniqueness proof. □

Remark 5.15. Generally speaking, proof by contradiction is the method of choice for existence and uniqueness proofs. But if you can give a direct proof, by all means do so.

Disproving Existence Statements

Discussion 5.16. To disprove

$$\exists x \in S,\ R(x)$$

Prove that its negation is true

$$\neg(\exists x \in S,\ R(x)) \equiv \forall x \in S,\ \neg R(x)$$

Example 5.17. Disprove that there exist integers $a \geqslant 2$ and $n \geqslant 1$ such that

$$a^2 + 1 = 2^n$$

Proof. We prove that for all integers $a \geqslant 2$ and $n \geqslant 1$, we have $a^2 + 1 \neq 2^n$, by using proof by contradiction. Suppose there exist $a \geqslant 2$ and $n \geqslant 1$ such that $a^2 + 1 = 2^n$.

Since $n \geqslant 1$, 2^n is even. Therefore a^2 is odd, and hence so is a. We may then write $a = 2k + 1$ for an integer k. Since $a \geqslant 2$, we get that $k \geqslant 1$. Therefore,

$$\begin{aligned} a^2 + 1 &= (2k+1)^2 + 1 \\ &= (4k^2 + 4k + 1) + 1 \\ &= 4k^2 + 4k + 2 \\ &= 2(2k^2 + 2k + 1) \end{aligned}$$

Since $a^2 + 1 = 2^n$, by assumption, we have $2(2k^2 + 2k + 1) = 2^n$. Hence,

$$2^{n-1} = 2k^2 + 2k + 1 = 2k(k+1) + 1$$

Which gives us

$$2k(k+1) = 2^{n-1} - 1$$

Since $k \geqslant 1$, the L.H.S. $\geqslant 4$. Thus $2^{n-1} - 1 \geqslant 4$, and hence necessarily $n > 1$. Therefore the R.H.S., $2^{n-1} - 1$ is odd, but the L.H.S. is always even. We have thus arrived at a contradiction. This completes the proof. □

6. Principle of Mathematical Induction

Discussion 6.1. We have the set of positive integers

$$\mathbb{Z}_{>0} = \{1, 2, 3, \dots\}$$

The principle of mathematical induction is a method of proof for statements of the form

$$\forall n \in \mathbb{Z}_{>0},\ P(n)$$

$$P(1) \text{ is true, and } P(2) \text{ is true, and } P(3) \text{ is true, and } \dots$$
$$\text{and } P(n) \text{ is true, and } P(n+1) \text{ is true, and } \dots$$

To prove such a statement, do the following

Step 1. (*Base Step*, or *Initial Step*) Prove that $P(1)$ is true.

Step 2. (*Inductive Step*) Prove that for all $k \geqslant 1$, $P(k)$ implies $P(k+1)$. That is, prove

$$\forall k \in \mathbb{Z}_{>0},\ P(k) \Rightarrow P(k+1)$$

In words, assume $P(k)$ is true (*inductive hypothesis*) and conclude $P(k+1)$ is true for any $k \geqslant 1$.

This is the (first) principle of mathematical induction.

What are we doing?

$$\underset{\text{(Step 1)}}{P(1) \text{ is true}} \xrightarrow[\text{for } k=1]{\text{Step 2}} P(2) \text{ is true} \xrightarrow[\text{for } k=2]{\text{Step 2}} P(3) \text{ is true} \xrightarrow[\text{for } k=3]{\text{Step 2}} \cdots$$

$$\cdots \xrightarrow[\text{for } k=n-1]{\text{Step 2}} P(n) \text{ is true} \xrightarrow[\text{for } k=n]{\text{Step 2}} P(n+1) \text{ is true} \longrightarrow \cdots$$

The logical foundation is the fact that the statement

$$P \wedge (P \Rightarrow Q) \Rightarrow Q$$

is a tautology. So, if $P(k)$ is true and $P(k) \Rightarrow P(k+1)$ is true, then $P(k+1)$ is true.

Example 6.2. Show that for $n \geqslant 1$,

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

Proof. We have the open sentence

$$P(n) : 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

We give a proof to the statement *for all* $n \geqslant 1$, $P(n)$ *is true* using the principle of mathematical induction.

(Base Step, $n = 1$) Consider the statement $P(1)$. L.H.S. $= 1$, while

$$\text{R.H.S.} = \frac{1(1+1)}{2} = \frac{2}{2} = 1$$

Therefore $P(1)$ is true.

(Inductive Step) Assume $P(k)$ is true, that is,

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

We wish to prove $P(k+1)$ is true, that is, we wish to prove the following equality

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

is true.

Note,

$$\begin{aligned} 1 + 2 + \cdots + (k+1) &= 1 + 2 + \cdots + k + (k+1) \\ &= \frac{k(k+1)}{2} + (k+1) && \text{by the inductive hypothesis} \\ &= (k+1)\left(\frac{k}{2} + 1\right) \\ &= \frac{(k+1)(k+2)}{2} \end{aligned}$$

Therefore $P(k+1)$ is true.

Hence, by the principle of mathematical induction, $P(n)$ is true for every integer $n \geqslant 1$. □

Discussion 6.3. It happens often that our base case for a statement $P(n)$, that is the first instance for which $P(n)$ is true, does not occur at $n = 1$, but may occur for a larger integer, say some $n = m$. We may still use the principle of mathematical induction by "starting induction from $n = m$". One then proves

(Base Case) Prove $P(m)$ is true.

(Inductive Step) For any $k \geqslant m$, prove $P(k) \Rightarrow P(k+1)$ is true.

This is the (second) principle of mathematical induction.

Example 6.4. Show that for $n \geqslant 5$, we have $2^n > n^2$.

Experiment.

n	1	2	3	4	5	6	7	$\cdots$
2^n	2	4	8	16	32	64	128	$\cdots$
n^2	1	4	9	16	25	36	49	$\cdots$

Proof. We have the open sentence

$$P(n) : 2^n = n^2$$

We give a proof to the statement *for all* $n \geqslant 5$, $P(n)$ *is true* using the principle of mathematical induction.

(Base Step, $n = 5$) Consider the statement $P(5)$. Note that

$$2^5 = 32 > 25 = 5^2$$

Therefore $P(1)$ is true.

(Inductive Step) Assume $P(k)$ is true for some $k \geqslant 5$, that is, $2^k > k^2$. We wish to prove $P(k+1)$ is true, that is, we wish to prove $2^{k+1} > (k+1)^2$ is true.

Note,

$$\begin{aligned}
2^{k+1} - (k+1)^2 &= 2 \cdot 2^k - (k+1)^2 \\
&> 2 \cdot k^2 - (k+1)^2 && \text{by the inductive hypothesis} \\
&= 2k^2 - (k^2 + 2k + 1) \\
&= k^2 - 2k - 1 \\
&= k^2 - 2k + 1 - 2 \\
&= (k-1)^2 - 2 \\
&> 0 && \text{for any } k \geqslant 5
\end{aligned}$$

Therefore $P(k+1)$ is true.

Hence, by the principle of mathematical induction, $P(n)$ is true for every integer $n \geqslant 5$. □

Example 6.5. Show that for $n \geqslant 2$ and for any $a_1, \dots, a_n \geqslant 0$, we have

$$(n-1)\left(\sum_{i=1}^{n} a_i^2\right) \geqslant 2 \sum_{1 \leqslant i < j \leqslant n} a_i a_j$$

$(n = 2)$ For $a_1, a_2 \geqslant 0$

$$a_1^2 + a_2^2 \geqslant 2a_1a_2$$

$(n = 3)$ For $a_1, a_2, a_3 \geqslant 0$

$$2(a_1^2 + a_2^2 + a_3^2) \geqslant 2(a_1a_2 + a_2a_3 + a_1a_3)$$

$(n=4)$ For $a_1, a_2, a_3, a_4 \geqslant 0$

$$3(a_1^2+a_2^2+a_3^2+a_4^2) \geqslant 2(a_1a_2+a_1a_3+a_1a_4+a_2a_3+a_2a_4+a_3a_4)$$

Proof. We have the open sentence

$$P(n) : (n-1)\left(\sum_{i=1}^{n} a_i^2\right) \geqslant 2 \sum_{1\leqslant i<j\leqslant n} a_ia_j, \quad a_1,\dots,a_n \geqslant 0$$

We give a proof to the statement *for all* $n \geqslant 2$, $P(n)$ *is true* using the principle of mathematical induction.

(Base Step, $n=2$) Consider the statement

$$P(2) : a_1^2+a_2^2 \geqslant 2a_1a_2, \quad a_1, a_2 \geqslant 0$$

Note that

$$\begin{aligned} a_1^2+a_2^2-2a_1a_2 &= (a_1)^2 - 2(a_1)(a_2) + (a_2)^2 \\ &= (a_1-a_2)^2 \\ &\geqslant 0 \end{aligned}$$

Therefore $P(2)$ is true.

(Inductive Step) Assume $P(k)$ is true for some $k \geqslant 2$, that is,

$$(k-1)\left(\sum_{i=1}^{k} a_i^2\right) \geqslant 2 \sum_{1\leqslant i<j\leqslant k} a_ia_j, \quad a_1,\dots,a_k \geqslant 0.$$

We wish to prove $P(k+1)$ is true, that is, we wish to prove

$$k\left(\sum_{i=1}^{k+1} a_i^2\right) \geqslant 2 \sum_{1\leqslant i<j\leqslant k+1} a_ia_j, \quad a_1,\dots,a_{k+1} \geqslant 0$$

is true. Our first step is to re-write the L.H.S. $-$ R.H.S. in such a way that we can use the inductive hypothesis $P(k)$. We observe

$$\begin{aligned} &k\left(\sum_{i=1}^{k+1} a_i^2\right) - 2\sum_{1\leqslant i<j\leqslant k+1} a_ia_j \\ &\qquad = (k-1)\left(\sum_{i=1}^{k+1} a_i^2\right) + \left(\sum_{i=1}^{k+1} a_i^2\right) - 2\sum_{1\leqslant i<j<k+1} a_ia_j - 2\sum_{1\leqslant i<j=k+1} a_ia_j \\ &\qquad = (k-1)\left(\sum_{i=1}^{k} a_i^2 + a_{k+1}^2\right) + \left(\sum_{i=1}^{k+1} a_i^2\right) - 2\sum_{1\leqslant i<j\leqslant k} a_ia_j - 2\sum_{1\leqslant i\leqslant k} a_ia_{k+1} \\ &\qquad = (k-1)a_{k+1}^2 + \left(\sum_{i=1}^{k+1} a_i^2\right) - 2\sum_{i=1}^{k} a_ia_{k+1} + \underbrace{(k-1)\left(\sum_{i=1}^{k} a_i^2\right) - 2\sum_{1\leqslant i<j\leqslant k} a_ia_j}_{\geqslant 0 \text{ by } P(k)} \end{aligned}$$

Therefore by our observations above and the inductive hypothesis, we have

$$\begin{aligned}
k\left(\sum_{i=1}^{k+1} a_i^2\right) - 2\sum_{1\leqslant i<j\leqslant k+1} a_i a_j &\geqslant (k-1)a_{k+1}^2 + \left(\sum_{i=1}^{k+1} a_i^2\right) - 2\sum_{i=1}^{k} a_i a_{k+1} \\
&= ka_{k+1}^2 - a_{k+1}^2 + \left(\sum_{i=1}^{k} a_i^2 + a_{k+1}^2\right) - 2\sum_{i=1}^{k} a_i a_{k+1} - a_{k+1}^2 \\
&= \left(\sum_{i=1}^{k} a_i^2\right) + ka_{k+1}^2 - 2\sum_{i=1}^{k} a_i a_{k+1} \\
&= (a_1^2 + a_{k+1}^2 - 2a_1 a_{k+1}) + (a_2^2 + a_{k+1}^2 - 2a_2 a_{k+1}) + \\
&\qquad \cdots + (a_k^2 + a_{k+1}^2 - 2a_k a_{k+1}) \\
&= (a_1 - a_{k+1}) + (a_2 - a_{k+1})^2 + \cdots + (a_k - a_{k+1})^2 \geqslant 0
\end{aligned}$$

Therefore $P(k+1)$ is true.

Hence, by the principle of mathematical induction, $P(n)$ is true for every integer $n \geqslant 2$. □

Example 6.6 (try it yourself!). Show that for $n \geqslant 1$ and a real number $a \neq 1$, we have

$$1 + a + \cdots + a^n = \frac{1 - a^{n+1}}{1 - a}$$

Remark 6.7. Re-writing the equality in Example 6.6 as

$$1 - a^{n+1} = (1-a)(1 + a + \cdots + a^n), \tag{$\star$}$$

this is now true for $a = 1$ as well. So $(\star)$ is true for all real numbers a.

If we write $a = y/x$ for real numbers x, y, we get

$$1 - (y/x)^{n+1} = (1 - (y/x))(1 + (y/x) + \cdots + (y/x)^n)$$

Multiplying both sides by x^n, we get

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

This is the formula we used in Example 5.14.

Strong Principle of Mathematical Induction

Discussion 6.8. The strong principle of mathematical induction is a variation of the principle of mathematical induction. We are still trying to prove statements of the form

$$\forall n \geqslant 1,\ P(n)$$

or more generally $\forall n \geqslant m,\ P(n)$ for some fixed integer m. This time our steps are:

(Base Case)

Prove $P(1)$ is true; or more generally $P(m)$ is true.

(Inductive Step)

For any $k \geqslant 1$, prove

$$P(1) \text{ and } P(2) \text{ and } \ldots \text{ and } P(k) \text{ together imply } P(k+1)$$

Or more generally, for all $k \geqslant m$, prove $P(m) \wedge P(m+1) \wedge \cdots \wedge P(k) \Rightarrow P(k+1)$ is true.

Theorem 6.9 (Prime Factorisation Theorem)**.** *Every positive integer $n \geqslant 2$ is a product of primes*

Proof. We have the open sentence

$$P(n) : n \text{ is a product of primes}$$

We give a proof to the statement *for all $n \geqslant 2$, $P(n)$ is true* using the strong principle of mathematical induction.

(Base Step, $n = 2$) Consider the statement $P(2)$. Since 2 is already a prime, therefore $P(2)$ is true.

(Inductive Step) Let $k \geqslant 2$. ~~Assume $P(k)$ is true for k~~ Assume $P(2), \ldots, P(k)$ are true, equivalently, assume $P(\ell)$ is true for all $2 \geqslant \ell \leqslant k$. That is, assume every integer $2 \leqslant \ell \leqslant k$ is a product of primes. We wish to prove $P(k+1)$ is true, that is, we wish to prove $k+1$ is a product of primes.

We have two cases: $k+1$ is a prime, or $k+1$ is not a prime.

Case 1. If $k+1$ is a prime, then $k+1$ is already a product of primes.

Case 2. If $k+1$ is not a prime, then it has a divisor $a \neq 1, k+1$. Necessarily, $a \mid (k+1)$ and $1 < a < k+1$. Hence, there exists an integer b such that

$$k+1 = ab,$$

and necessarily $1 < b < k+1$. By the inductive hypothesis $P(a)$ and $P(b)$ are true, that is, a and b are a product of primes. Thus, $k+1 = ab$ is necessarily also a product of primes.

Therefore $P(k+1)$ is true.

Hence, by the strong principle of mathematical induction, for any $n \geqslant 2$, $P(n)$ is true. That is, every integer $n \geqslant 2$ is a product of primes. □

7. Prove or Disprove

Conjectures in Mathematics

Discussion 7.1. In mathematics, we sometimes encounter statements for which we have ample evidence (several examples) that they may be true. We call these statements conjectures. In many ways, a conjecture is nothing more than an intelligent guess.

When one encounters a pattern, one first tries to synthesise the pattern into a conjecture. The next step is then to attempt a proof.

Example 7.2. Consider the following pattern

$$\begin{aligned} 1 = 0 + 1 &= 0^3 + 1^3 \\ 2 + 3 + 4 = 1 + 8 &= 1^3 + 2^3 \\ 5 + 6 + 7 + 8 + 9 = 8 + 27 &= 2^3 + 3^3 \\ 10 + 11 + 12 + 13 + 14 + 15 + 16 = 27 + 64 &= 3^3 + 4^3 \\ &\vdots \end{aligned}$$

We formulate the following conjecture.

Conjecture 7.3. *For every integer $n \geqslant 0$, we have*

$$(n^2 + 1) + (n^2 + 2) + \cdots + (n + 1)^2 = n^3 + (n + 1)^3$$

Is this true or false? If one thinks it is true, one needs to provide a proof. If one think it is false, one needs to exhibit a counterexample.

This is true.

Proof. There are two methods of proof that we can do here.

A proof using the Principle of Mathematical Induction. (Try this!)

A direct proof using the formula for sum of positive integers

$$1 + 2 + \cdots + k = \frac{k(k + 1)}{2}, \quad k \geqslant 1$$

We give a proof using the latter method. Note,

$$\begin{aligned} \text{L.H.S.} &= (n^2 + 1) + (n^2 + 2) + \cdots + (n + 1)^2 \\ &= (n^2 + 1) + (n^2 + 2) + \cdots + (n^2 + 2n + 1) \\ &= \sum_{k=1}^{2n+1} (n^2 + k) \\ &= \sum_{k=1}^{2n+1} n^2 + \sum_{k=1}^{2n+1} k \end{aligned}$$

$$
\begin{aligned}
&= (2n+1)n^2 + \frac{(2n+1)((2n+1)+1)}{2} \\
&= (2n+1)n^2 + \frac{(2n+1)(2n+2)}{2} \\
&= (2n+1)n^2 + (2n+1)(n+1) \\
&= (2n^3+n^2) + (2n^2+2n+n+1) \\
&= n^3 + (n^3+3n^2+3n+1) \\
&= n^3 + (n+1)^3 \\
&= \text{R.H.S.}
\end{aligned}
$$

This completes the proof. □

Prove or Disprove

Discussion 7.4. Basic principle for universally quantified statements. If you think they are true, provide a proof. If you think they are false, exhibit a counterexample.

Example 7.5.

- Prove or disprove: If ab, bc, ca are even, then a, b and c are even.

  Proof. This is false. A counterexample is found when we take $a = b = 2$ and $c = 1$. □

- Prove or disprove: If $n^2 + n$ is even, then n is even.

  Proof. This is false. A counterexample is found when we take $n = 1$. □

Example 7.6.

Question. Which integer $n \geqslant 3$ can be expressed as a sum of at least two consecutive integers?

Experiment.

$$
\begin{array}{ll}
3 = 1+2 & 12 = 3+4+5 \\
4 = \text{not possible} & 13 = 6+7 \\
5 = 2+3 & 14 = 2+3+4+5 \\
6 = 1+2+3 & 15 = 7+8 = 4+5+6 = 2+3+4+5 \\
7 = 3+4 & 16 = \text{not possible}
\end{array}
$$

$$\begin{aligned} 8 &= \text{not possible} \\ 9 &= 4+5 = 2+3+4 \\ 10 &= 1+2+3+4 \\ 11 &= 5+6 \end{aligned}$$

$$\begin{aligned} 17 &= 8+9 \\ 18 &= 5+6+7 = 3+4+5+6 \\ &\vdots \end{aligned}$$

Conjecture 7.7. *If n is a positive integer that is not a power of 2, then n is a sum of two or more consecutive positive integers.*

Observations.

- Any odd integer can be written as a sum of *two* consecutive integer, as an odd integer n can be written, for some integer k, as
$$n = 2k+1 = k+(k+1)$$
- Some integers can be written as a sum of consecutive integers in more than one way. What property of the integers control this? Possibly the number of odd factors.

More ambitiously, we make the following conjecture

Conjecture 7.8 (Improved Conjecture 7.7)**.** *A positive integer $n \geqslant 3$ is a sum of two or more consecutive positive integers if and only if it is not a power of 2.*

Experiments towards a Proof. Consider an integer n that is not a power of 2.

Case 1. $n = 2\ell+1$, an odd integer. In this case, we have seen

$$n = \ell + (\ell+1).$$

Case 2. $n = 2(2\ell+1)$.

$$\begin{aligned} 2\cdot(2\cdot 1+1) &= 2\cdot 3 = 6 = 1+2+3 \\ 2\cdot(2\cdot 2+1) &= 2\cdot 5 = 10 = 1+2+3+4 \\ 2\cdot(2\cdot 3+1) &= 2\cdot 7 = 14 = 2+3+4+5 \\ 2\cdot(2\cdot 4+1) &= 2\cdot 9 = 18 = 3+4+5+6 = 5+6+7 \end{aligned}$$

We claim

$$2(2\ell+1) = \underbrace{(\ell-1)+\ell+(\ell+1)+(\ell+2)}_{\text{4 terms}}, \quad \ell \geqslant 2$$

Case 3. $n = 2^2(2\ell+1)$.

$$\begin{aligned} 2^2\cdot(2\cdot 1+1) &= 2^2\cdot 3 = 12 = 3+4+5 \\ 2^2\cdot(2\cdot 2+1) &= 2^2\cdot 5 = 20 = 2+3+4+5+6 \end{aligned}$$

$$2^2 \cdot (2 \cdot 3 + 1) = 2^2 \cdot 7 = 28 = 1 + 2 + 3 + 4 + 5 + 6 + 7$$

$$2^2 \cdot (2 \cdot 4 + 1) = 2^2 \cdot 9 = 36 = 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8$$

$$2^2 \cdot (2 \cdot 5 + 1) = 2^2 \cdot 11 = 44 = 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9$$

$$2^2 \cdot (2 \cdot 6 + 1) = 2^2 \cdot 13 = 52 = 3 + 4 + 5 + 6 + 7 + 8 + 9 + 10$$

We claim

$$2^2(2\ell + 1) = \underbrace{(\ell - 3) + (\ell - 2) + (\ell - 1) + \ell + (\ell + 1) + (\ell + 2) + (\ell + 3) + (\ell + 4)}_{8 \text{ terms}}, \quad \ell \geqslant 4$$

Case 4. $n = 2^3(2\ell + 1)$.

$$\vdots$$

Do your own experiments.

Proof of Conjecture 7.8.

(⇒) Suppose $n \geqslant 3$ is a sum of consecutive integers, we show n is not a power of 2 by exhibiting an odd factor ($\geqslant 3$).

> Suppose that $n = k + (k + 1) + \cdots + (k + r)$ for some $k > 0$ and $r \geqslant 1$. Then,
>
> $$\begin{aligned} n = \underbrace{k + (k + 1) + \cdots + (k + r)}_{r+1 \text{ terms}} &= (r + 1)k + \sum_{\ell=0}^{r} \ell \\ &= (r + 1)k + \frac{r(r + 1)}{2} \\ &= (r + 1)\left(k + \frac{r}{2}\right) = (r + 1)\left(\frac{2k + r}{2}\right) \end{aligned}$$
>
> If r is even, then $r + 1$ is an odd factor of n.
>
> If r is odd, in $n = \left(\frac{r + 1}{2}\right)(2k + r)$, $2k + r$ is an odd factor.

While what we have above is a valid proof, a more illuminating proof is obtained by starting at the middle summand of n.

Case 1. Suppose n is a sum of odd-many, say $2\ell + 1 \geqslant 3$, consecutive positive integers. Then, we write n as

$$n = \underbrace{(t - \ell) + \cdots (t - 2) + (t - 1)}_{\ell \text{ terms}} + t + \underbrace{(t + 1) + (t + 2) \cdots (t + \ell)}_{\ell \text{ terms}}$$

Since these are positive integers, we get $t - \ell > 0$, or equivalently $\ell < t$. Re-arranging, we have

$$\begin{aligned} n &= (t-\ell) + \cdots + (t-2) + (t-1) + t + (t+1) + (t+2) + \cdots + (t+\ell) \\ &= (t-\ell) + (t+\ell) + \cdots + (t-2) + (t+2) + (t-1) + (t+1) + t \\ &= \underbrace{2t + \cdots + 2t + 2t}_{\ell \text{ terms}} + t \\ &= 2\ell t + t \\ &= (2\ell+1)t \end{aligned}$$

Thus n has an odd factor $2\ell + 1 \geqslant 3$.

Case 2. Suppose n is a sum of even-many, say $2t \geqslant 2$, consecutive positive integers. Then, we write n as

$$n = \underbrace{(\ell - t + 1) + \cdots + (\ell - 1) + \ell}_{t \text{ terms}} + \underbrace{(\ell+1) + (\ell+2) + \cdots + (\ell+t)}_{\ell \text{ terms}}$$

Since these are positive integers, we get $\ell - (t-1) > 0$, or equivalently $\ell \geqslant t$. Re-arranging, we have

$$\begin{aligned} n &= (\ell - (t-1)) + \cdots + (\ell-1) + \ell + (\ell+1) + (\ell+2) + \cdots + (\ell+t) \\ &= (\ell - t + 1) + (\ell + t) + \cdots + (\ell - 1) + (\ell + 2) + \ell + (\ell + 1) \\ &= \underbrace{(2\ell+1) + \cdots + (2\ell+1) + (2\ell+1)}_{t \text{ terms}} \\ &= (2\ell+1)t \end{aligned}$$

Thus n has an odd factor $2\ell + 1 \geqslant 3$.

($\Leftarrow$) Suppose n is not a power of 2, then we show that it can be written as a sum of at least two consecutive numbers. We can write such an n as

$$n = (2\ell+1)t$$

for some integers $\ell, t > 1$. We have two cases:

Case A. $\ell < t$, in which case can use Case 1. from above to re-write n as a sum of consecutive numbers.

Case B. $\ell \geqslant t$, in which case can use Case 2. from above to re-write n as a sum of consecutive numbers.

This completes the proof. □

Thus, Conjecture 7.8 is now a theorem.

Theorem 7.9. *A positive integer $n \geqslant 3$ is a sum of two or more consecutive positive integers if and only if it is not a power of 2.*

Example 7.10. Consider $n = 15 = 3 \cdot 5 = 5 \cdot 3 = 15 \cdot 1$. It has three odd factors $\geqslant 3$, we should be able to obtain three ways of writing it as a sum of consecutive integers. In terms of the notation introduced in the proof above, we have

Case 1. Consider $15 = 3 \cdot 5$, here $2\ell + 1 = 3$ and $t = 5$, so $\ell = 1$ and $\ell < t$. Hence

$$15 = 4 + 5 + 6$$

Case 2. Consider $15 = 5 \cdot 3$, here $2\ell + 1 = 5$ and $t = 3$, so $\ell = 2$ and $\ell < t$. Hence

$$15 = 1 + 2 + 3 + 4 + 5$$

Case 3. Consider $15 = 15 \cdot 1$, here $2\ell + 1 = 15$ and $t = 1$, so $\ell = 7$ and $\ell \geqslant t$. Hence

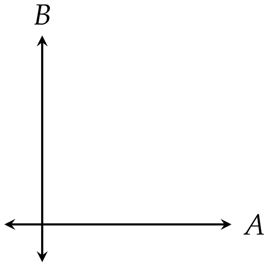
$$15 = 7 + 8$$

Corollary 7.11 (to Theorem 7.9)**.** *An odd prime p can only be written as a sum of two consecutive integers.*

$$p = \left(\frac{p-1}{2}\right) + \left(\frac{p+1}{2}\right).$$

8. Relations

Fix sets A, B. For a visual motivation, we view the cartesian product $A \times B$ as a plane with the horizontal axis represented by A and the vertical axis represented by B.



This in no way rigorously reflects the set $A \times B$ but is useful in getting a sense of definitions and notions we will see.

Definition 8.1. A relation from A to B is a subset of $A \times B$.

For a relation $R \subseteq A \times B$, given any element $(a,b) \in R$, we write aRb and say

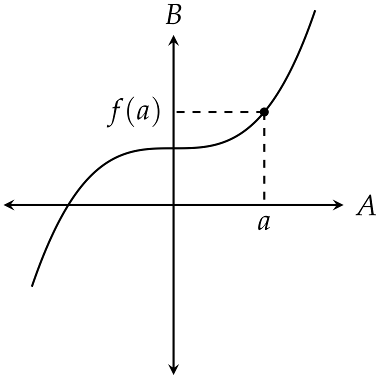
a is R-related to b

If $(a,b) \notin R$, then we write $a \not R b$ and say *a is not R-related to b*.

Example 8.2.

(1) Let $f : A \times B$ be a function, let $\Gamma(f)$ be its graph

$$\Gamma(f) = \{(a, f(a)) \mid a \in A\} \subseteq A \times B$$

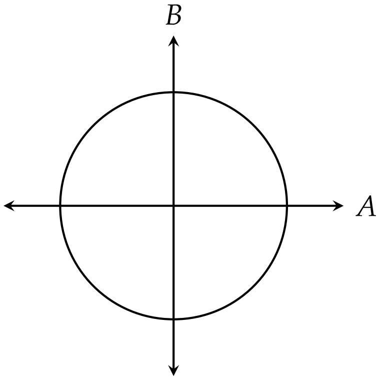


This is a relation from A to B. In this way, a function is a special case of a relation.

(2) Let

$$S = \left\{(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\right\} \subseteq \mathbb{R} \times \mathbb{R},$$

this is a relation from $\mathbb{R}$ to $\mathbb{R}$.



Solving for y gives

$$y = \pm\sqrt{1-x^2}$$

This is a *multi-valued function* (fails the vertical line test) defined on $[-1,1]$. We usually do not call such things functions, but it is a legitimate relation on $\mathbb{R}$.

Definition 8.3. Let $R \subseteq A \times B$ be a relation from A to B. The domain of R is

$$\mathrm{dom}(R) = \{a \in A \mid (a,b) \in R \text{ for some } b \in B\}$$

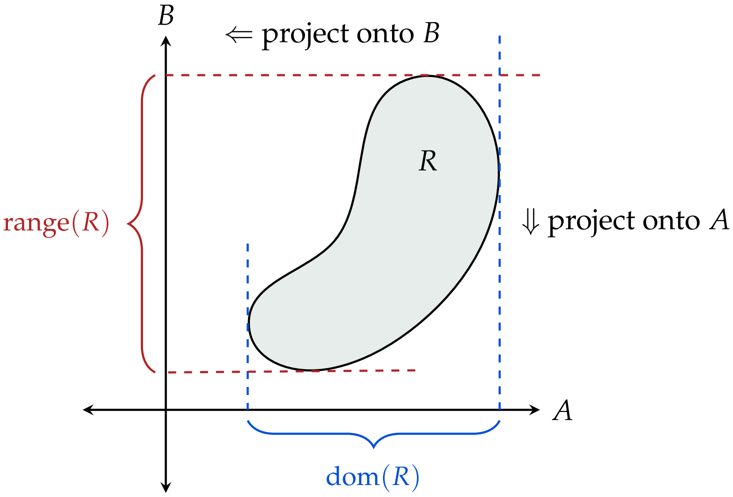
This is the set of all first coordinates that occur in elements of R.

The range of R (also called image of R) is

$$\mathrm{range}(R) = \{b \in B \mid (a,b) \in R \text{ for some } a \in A\}$$

This is the set of all second coordinates that occur in elements of R.

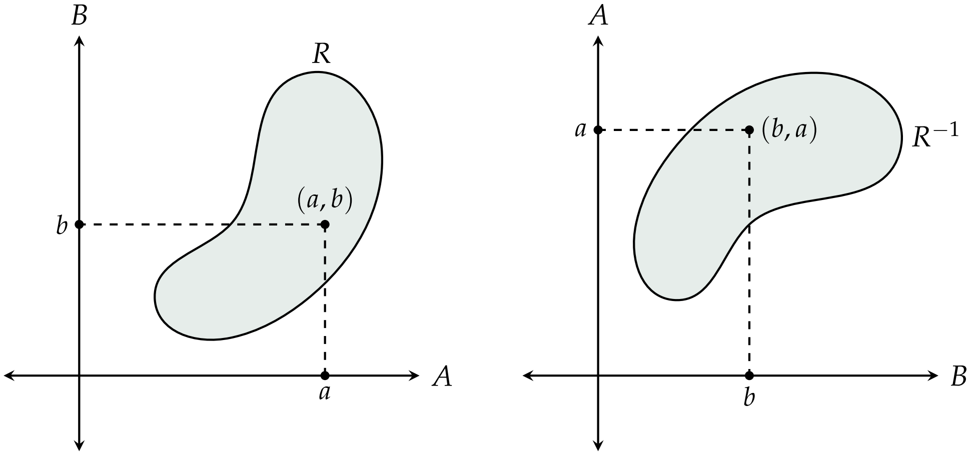
Visually, for example,



Definition 8.4. Let $R \subseteq A \times B$ be a relation from A to B. The inverse relation R^{-1} is

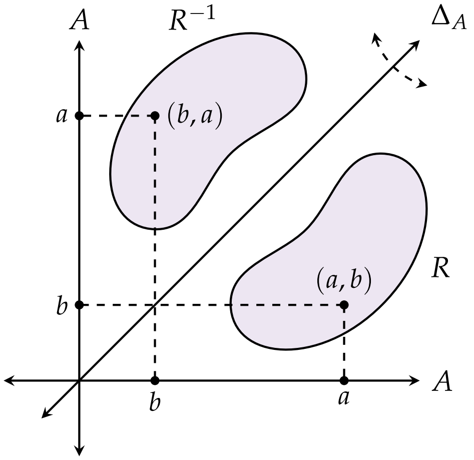
$$R^{-1} = \{(b,a) \in B \times A \mid (a,b) \in R\},$$

a relation from B to A. Visually, for example,



If $A = B$, then we obtain R^{-1} by reflecting along the *diagonal*, this is the subset defined as

$$\Delta_A = \{(a,a) \mid a \in A\} \subseteq A \times A.$$



Example 8.5. In the special case of a bijection $f : A \to B$, its graph is a relation

$$\Gamma(f) = \{(a,b) \in A \times B \mid b = f(a)\} \leftrightarrow f$$

Its inverse relation is

$$\begin{aligned}
\Gamma(f)^{-1} &= \{(b,a) \in B \times A \mid (a,b) \in \Gamma(f)\} \\
&= \{(b,a) \in B \times A \mid b = f(a)\} \\
&= \left\{(b,a) \in B \times A \mid a = f^{-1}(b)\right\} \\
&= \Gamma(f^{-1})
\end{aligned}$$

Example 8.6. Consider sets $A = \{1,2,3,4,5\}$ and $B = \{u,v,w,x,y,z\}$. Then consider the following relation from A to B.

$$R = \{(1,z),(2,v),(4,x),(2,v),(4,u),(5,w),(2,x)\}$$

The domain of R is the list of those elements of A that appear as first coordinates of elements of R, that is,

$$\mathrm{dom}(R) = \{1,2,4,5\}\,.$$

While the range of R is the list of those elements of B that appear as second coordinates of elements of R, that is,

$$\mathrm{range}(R) = \{u,v,w,x,z\}\,.$$

The inverse relation from B to A is obtained by swapping the first and second coordinates

$$R^{-1} = \{(z,1),(v,2),(x,4),(v,2),(u,4),(w,5),(x,2)\} \subseteq B \times A$$

Properties of Relations

From now on we assume $B = A$; a relation from A to A is called a *relation on* A.

Example 8.7 (Equality)**.** Consider the following relation on A, the diagonal

$$R = \Delta_A = \{(a,a) \mid a \in A\}$$

For this relation, we have

$$aRb \quad \text{if and only if} \quad (a,b) \in R \quad \text{if and only if} \quad a = b$$

So, this R corresponds to the usual equality relation. We generalise the concept of equality to "equivalence". For this, we first record the most fundamental properties of equality.

(i) $a = a$ for every $a \in A$.

(ii) If $a = b$, then $b = a$, for every $a, b \in A$.

(iii) If $a = b$ and $b = c$, then $a = c$, for every $a, b, c \in A$.

Definition 8.8. Let R be a relation on A, that is, $R \subseteq A \times A$.

- R is said to be reflexive if xRx for every $x \in A$, that is, if $(x,x) \in R$ for every $x \in A$.

  Set theoretically, this is saying that we require $\Delta_A \subseteq R$.

- R is said to be symmetric if xRy implies yRx for every $x, y \in A$, that is, if $(x,y) \in R$ implies $(y,x) \in R$ for every $x, y \in A$.

  Set theoretically, this is saying that we require $R = R^{-1}$.

- R is said to be transitive if xRy and yRz implies xRz for every $x, y, z \in A$, that is, if $(x, y), (y, z) \in R$ implies $(x, z) \in R$ for every $x, y, z \in A$.

Example 8.9. Consider the set $A = \{a, b, c\}$, and the following relation on A

$$R = \{(a, a), (b, b), (c, c), (a, b), (b, c), (a, c)\}$$

Note that

R is reflexive, since $(a, a), (b, b), (c, c) \in R$.

R is *not* symmetric, since $(a, b) \in R$ but $(b, a) \notin R$.

R is transitive, $(a, b), (b, c), (a, c) \in R$ etc.

Example 8.10. Let $A = \mathbb{R}$, and consider the following relation R on $\mathbb{R}$

$$R = \left\{(x, y) \in \mathbb{R}^2 \mid |x - y| \leqslant 1\right\}$$

For any $(x, y) \in R$ we have $|x - y| \leqslant 1$ and therefore $-1 \leqslant x - y \leqslant 1$. Hence R is bounded by the lines given as $x - y = -1$ and $x - y = 1$, or equivalently, the lines $y = x + 1$ and $y = x - 1$

insert image

Is R reflexive, symmetric or transitive?

Note that R contains the diagonal line, hence R is reflexive. This is the fact that

$$|x - x| = 0 \leqslant 1, \text{ so } (x, x) \in R$$

Furthermore, R is symmetric along the diagonal. This is the fact that

$$|y - x| = |x - y| \leqslant 1, \text{ so if } (x, y) \in R, \text{ then } (y, x) \in R$$

Is R transitive? This is then asking that if $|x - y| \leqslant 1$ and $|y - z| \leqslant 1$, then is $|x - z| \leqslant 1$.

We exhibit a counterexample to conclude that R is not transitive. Consider $x = 1.5$, $y = 1$ and $z = 0$. Then since

$$|x - y| = |1.5 - 1| = 0.5 \leqslant 1 \quad \text{and} \quad |y - z| = |1 - 0| = 1 \leqslant 1,$$

therefore $(x, y), (y, z) \in R$. But

$$|x - z| = |1.5 - 0| = 1.5 > 1$$

and thus $(x, z) \notin R$. Therefore R is not transitive.

9. Equivalence Relations

Definition 9.1. Let R be a relation on A. We call R an equivalence relation if

- R is reflexive
- R is symmetric
- R is transitive

In this case, if aRb, then we say a is equivalent to b and we alternatively denote it as $a \sim b$ (by symmetry, $b \sim a$ as well).

An equivalence relation is a generalisation of equality.

Example 9.2. $R = \Delta_A = \{(a,a) \mid a \in A\}$ is an equivalence relation.

$$aRb \text{ if and only if } a = b \quad \text{and} \quad R = \text{“} = \text{''}$$

Since,

(i) $a = a$ for every $a \in A$.

(ii) If $a = b$, then $b = a$, for every $a, b \in A$.

(iii) If $a = b$ and $b = c$, then $a = c$, for every $a, b, c \in A$.

Example 9.3. For $A = \{1,2,3,4,5\}$, consider the following relation on A

$$R = \{(1,1),(2,2),(3,3),(4,4),(5,5),(1,3),(1,5),(5,1),(5,3),(3,1),(3,5),(2,4),(4,2)\} \subseteq A \times A$$

R is an equivalence relation. Note,

(i) for every $a \in A$, we have $(a,a) \in A$.

(ii) Whenever $(a,b) \in R$, we have $(b,a) \in R$. (e.g. $(1,3) \in R$ and $(3,1) \in R$, $(3,6),(6,3) \in R$ etc.)

(iii) We have $(1,6),(6,3) \in R$, is $(1,3) \in R$? Yes! Check remaining cases.

Example 9.4. Consider the following relation on $\mathbb{R}^2 \setminus \{(0,0)\}$

$$(x,y)R(a,b) \quad \text{if and only if (i.e. the definition)} \quad \text{there exists } \lambda \in \mathbb{R}_{\neq 0} \text{ such that } (a,b) = (\lambda x, \lambda y)$$

We show R is an equivalence relation.

(i) Note that for $\lambda = 1$, we have

$$(x,y) = (\lambda x, \lambda y)$$

Therefore $(x,y)R(x,y)$, for all $(x,y) \in \mathbb{R}^2$, and hence R is reflexive.

(ii) Suppose $(x,y),(a,b) \in \mathbb{R}^2$ is such that $(x,y)R(a,b)$. Therefore $(a,b) = (\lambda x, \lambda y)$, for some $\lambda \in \mathbb{R}_{\neq 0}$, and hence $a = \lambda x$, $b = \lambda y$. Thus,

$$(x,y) = ((1/\lambda)a, (1/\lambda)b).$$

Therefore $(a,b)R(x,y)$, and hence R is symmetric.

(iii) Suppose $(x,y),(a,b),(u,v) \in \mathbb{R}^2$ is such that $(x,y)R(a,b)$ and $(a,b)R(u,v)$. Therefore $(a,b) = (\lambda x, \lambda y)$ and $(u,v) = (\mu a, \mu b)$, for some $\lambda, \mu \in \mathbb{R}_{\neq 0}$. Hence

$$a = \lambda x,\ b = \lambda y \ \text{ and } \ u = \mu a,\ v = \mu b.$$

Thus,

$$(u,v) = (\mu\lambda x, \mu\lambda y).$$

Therefore $(x,y)R(u,v)$, and hence R is transitive.

Example 9.5. For $A = \{\text{all people}\}$, consider the following relation on A

$$P_1 \sim P_2 \quad \text{if and only if} \quad \text{age}(P_1) = \text{age}(P_2)$$

This is an equivalence relation. Try and verify the definition!

Definition 9.6. Let R be an equivalence relation on A.

For $a \in A$, define the R-equivalence class represented by a to be the subset

$$\begin{aligned}[a] &= \{x \in A \mid xRa \text{ (or } aRx\text{, by symmetry)}\} = \{\text{all elements of } A \text{ that are equivalent to } a\} \subseteq A \\ &= \{x \in A \mid (x,a) \in R\ ((a,x) \in R)\}\end{aligned}$$

Since R is reflexive, that is, aRa, we have $a \in [a]$ for any $a \in A$.

Example 9.7. Let us find the equivalence classes for

$$R = \{(1,1),(2,2),(3,3),(4,4),(5,5),(1,3),(1,5),(5,1),(5,3),(3,1),(3,5),(2,4),(4,2)\}$$

described in Example 9.3 on $A = \{1,2,3,4,5\}$.

$$\begin{aligned}[1] &= \text{the equivalence class of } 1 \\ &= \text{all elements "equivalent" (that is, } R\text{-related) to } 1 \\ &= \{x \in A \mid (x,1) \in R\} \\ &= \{1,3,5\}, \quad \text{since } (1,1),(3,1) \in R\end{aligned}$$

Similarly,

$$\begin{aligned}[2] &= \{x \in A \mid (x,2) \in R\} & [4] &= \{x \in A \mid (x,4) \in R\} \\ &= \{2,4\} & &= \{2,4\} = [2] \\ [3] &= \{x \in A \mid (x,3) \in R\} & [5] &= \{x \in A \mid (x,5) \in R\} \\ &= \{1,3,5\} & &= \{1,3,5\} = [1] = [3]\end{aligned}$$

So,

$$\begin{aligned}[1] = [3] = [5] &= \{1,3,5\} \\ [2] = [4] &= \{2,4\}\end{aligned}$$

We make the following observations: for $a, b \in A$,

$$\text{if } a \not R b, \text{ then } [a] \cap [b] = \varnothing; \text{ and}$$
$$\text{if } aRb, \text{ then } [a] = [b]$$

Example 9.8. Consider the equivalence relation as described in Example 9.4. Let's compute the equivalence class of $(3,5) \in \mathbb{R}^2$

$$\begin{aligned}
[(3,5)] &= \left\{(x,y) \in \mathbb{R}^2 \mid (3,5)R(x,y)\right\} \\
&= \left\{(x,y) \in \mathbb{R}^2 \mid (x,y) = (3\lambda, 5\lambda), \text{ for some } \lambda \in \mathbb{R}_{\neq 0}\right\} \\
&= \left\{(x,y) \in \mathbb{R}^2 \mid x = 3\lambda \text{ and } y = 5\lambda, \text{ for some } \lambda \in \mathbb{R}_{\neq 0}\right\} \\
&= \left\{(3\lambda, 5\lambda) \in \mathbb{R}^2 \mid \lambda \in \mathbb{R}_{\neq 0}\right\}
\end{aligned}$$

This is nothing but the line defined by the equation $3y = 5x$, minus the origin.

Example 9.9. Consider the equivalence relation as described in Example 9.5. Let's compute the equivalence class of me!

$$\begin{aligned}
[\text{Deewang}] &= \{P \in A \mid P \sim \text{Deewang}\} \\
&= \{P \in A \mid \text{age}(P) = \text{age}(\text{Deewang}) = 28\} \\
&= \{\text{all people that are 28 years of age}\}
\end{aligned}$$

Example 9.10 (Congruence is an Equivalence Relation)**.** Let $A = \mathbb{Z}$ and fix a positive integer n. Define a relation R on $\mathbb{Z}$ as

$$aRb \text{ if and only if } a \equiv b \bmod n$$

Recall that we say $a \equiv b \bmod n$ if $n \mid (a - b)$. This is an equivalence relation.

(i) $a \equiv a \bmod n$, for every $a \in \mathbb{Z}$.

This is because $n \mid (a - a)$ for every integer a, as $a - a = 0 = n \cdot 0$.

(ii) If $a \equiv b \bmod n$, then $b \equiv a \bmod n$, for every $a, b \in \mathbb{Z}$.

This is because if $a \equiv b \bmod n$, then $n \mid (a - b)$. That is, $a - b = nk$ for an integer k. Therefore $b - a = n(-k)$; since $-k \in \mathbb{Z}$, hence $n \mid (b - a)$. Thus $b \equiv a \bmod n$.

(iii) If $a \equiv b \bmod n$ and $b \equiv c \bmod n$, then $a \equiv c \bmod n$, for every $a, b, c \in \mathbb{Z}$.

This is because if $a \equiv b \bmod n$ and $b \equiv c \bmod n$, then $n \mid (a - b)$ and $n \mid (b - c)$. That is, $a - b = nk$ and $b - c = n\ell$ for integers k, ℓ. Therefore $a - c = (a - b) + (b - c) = n(k + \ell)$; since $k + \ell \in \mathbb{Z}$, hence $n \mid (a - c)$. Thus $a \equiv c \bmod n$.

Thus the congruence relation "$\equiv$" is an equivalence relation.

Let $n = 5$, we find the equivalence class of 3 with respect to the congruence modulo 5 relation.

$$\begin{aligned}
[3]_5 &= \{n \in \mathbb{Z} \mid n \equiv 3 \bmod 5\} \\
&= \{n \in \mathbb{Z} \mid 5 \mid (n-3)\} \\
&= \{n \in \mathbb{Z} \mid n - 3 = 5k, \text{ for some integer } k\} \\
&= \{n \in \mathbb{Z} \mid n = 5k + 3, \text{ for some integer } k\} \\
&= \{5k + 3 \mid k \in \mathbb{Z}\} \\
&= \{\dots, -7, -2, 3, 8, 13, \dots\} \\
&= \{\text{all integers that leave remainder 3 when divided by 5}\}
\end{aligned}$$

Example 9.11. Let $A = \mathbb{Z}$, we define a relation R on $\mathbb{Z}$ as

$$aRb \text{ if and only if } a + 3b \text{ is even}$$

We show this is an equivalence relation.

(i) Is aRa, for every $a \in \mathbb{Z}$?

Since for any $a \in \mathbb{Z}$, we have that $a + 3a = 4a$ is even. Thus aRa, and so R is reflexive.

(ii) Does aRb imply bRa?

Suppose aRb, that is, $a + 3b$ is even. We show bRa, or $b + 3a$ is even. Note that $(a + 3b) + (b + 3a) = 4a + 4b$ is even, therefore $b + 3a = 4(a + b) - (a + 3b)$ is even, as a sum of even integers. Hence bRa, and thus R is symmetric.

(iii) Do aRb and bRc imply aRc?

Suppose aRb and bRc, that is, $a + 3b$ and $b + 3c$ is even. We show aRc, or $a + 3c$ is even. Note that $(a + 3b) + (b + 3c) = a + 3c + 4b$, therefore $a + 3c = (a + 3b) + (b + 3c) - 4b$ is even, as a sum of even integers. Hence aRc, and thus R is transitive.

Thus, R is an equivalence relation.

Properties of Equivalence Classes

Theorem 9.12. *Let R be an equivalence relation on a set A. Then, for $a, b \in A$,*

$$[a] = [b] \text{ if and only if } aRb$$

Proof. Let $a, b \in A$.

($\Rightarrow$) Suppose $[a] = [b]$, we show aRb. Note that, since R is reflexive, we have aRa. Therefore, $a \in [a] = [b]$, and hence $a \in [b]$. Thus, aRb.

($\Leftarrow$) Suppose aRb, we show $[a] = [b]$, that is, we show $[a] \subseteq [b]$ and $[b] \subseteq [a]$. Note that since R is symmetric, we also have bRa.

Consider any $x \in [a]$, by definition, xRa. Since xRa and aRb, by assumption, we obtain xRb, by transitivity. Therefore, $x \in [b]$, and hence $[a] \subseteq [b]$.

Consider any $y \in [b]$, by definition, yRb. Since yRb and bRa, by assumption, we obtain yRa, by transitivity. Therefore, $y \in [a]$, and hence $[b] \subseteq [a]$.

Thus, $[a] = [b]$.

□

We have shown that a and b are equivalent, if and only if $[a] = [b]$. As a consequence, we obtain the following.

Theorem 9.13. *Let R be an equivalence relation on a set A. Then, for $a, b \in A$, if $[a] \cap [b] \neq \varnothing$, then $[a] = [b]$.*

Thus, given any two equivalence classes $[a]$ and $[b]$, they are either disjoint or identical.

Proof. Let $a, b \in A$, and suppose $[a] \cap [b] = \varnothing$. We show $[a] = [b]$. Consider any $x \in [a] \cap [b]$. Then $x \in [a]$ and $x \in [b]$, and therefore xRa and xRb. Since R is symmetric and xRa, we obtain aRx. Hence we have aRx and xRb, and thus aRb by transitivity of R. Therefore $[a] = [b]$, by Theorem 9.12. □

Remark 9.14. Recall that a partition of A is a collection of subsets $X_\alpha \subseteq A$, where $\alpha \in I$ for some index set (that is, for each element $\alpha \in I$, we have a subset X_α) such that

$$X_\alpha \cap X_\beta = \varnothing \text{ if } \alpha \neq \beta$$

$$\bigcup_{\alpha \in I} X_\alpha = A$$

In this case, write $A = \coprod_{\alpha \in I} X_\alpha$ ("disjoint union").

Theorem 9.15. *Let R be an equivalence relation on a set A. Then, the collection of all R-equivalence classes defines a partition of A.*

This partition is denoted A/R (read as: "A mod R"), and is called *the quotient set of A by R.*

Proof. The proof follows from the theorems above. We leave it to the reader to work out the details and write out a formal proof. □

Conversely,

Theorem 9.16. *Let $\mathcal{S} = \{X_\alpha\}_{\alpha \in I}$ be a partition of a set A. Then, there exists a unique relation R on A such that the resulting partition by equivalence classes is the partition given*

This is saying that *giving an equivalence relation on A is equivalent to defining a partition of A.*

Sketch of Proof. We first prove the existence of such a relation R on A. Define R as follows: say,

$$aRb \text{ if and only if } a, b \in X_\alpha \text{ for some } \alpha$$

for any $a, b \in A$. One checks that this R is equivalent, verifying that R is reflexive and symmetric is straightforward. Following is the argument for showing transitivity of R.

Suppose aRb and bRc. By definition $a, b \in X_\alpha$ and $b, c \in X_\beta$. Therefore $b \in X_\alpha$ and $b \in X_\beta$, that is, $b \in X_\alpha \cap X_\beta$. Unless $X_\alpha = X_\beta$, we have shown that $X_\alpha \cap X_\beta \neq \varnothing$ contradicting the fact $\mathscr{S}$ is a partition. Hence, $X_\alpha = X_\beta$ and thus $a, c \in X_\alpha$. Therefore aRc.

We still need to check following: (1) that X_α is an equivalence class for any $\alpha \in I$, we do this by exhibiting that for any $a \in X_\alpha$ we have $X_\alpha = [a]$; (2) This R is the unique relation with this property.

Example 9.17. Let $A = \{1, 2, 3, 4, 5, 6\}$, and consider a partition

$$\mathscr{S} = \{\{1, 2\}, \{3, 4\}, \{5, 6\}\}$$

What is the equivalence relation R reproducing this partition?

Let $X_\alpha = \{1, 2\}, X_\beta = \{3, 4\}$ and $X_\gamma = \{5, 6\}$.

$$\begin{aligned}
&\text{Since } 1, 2 \in \{1, 2\}, \text{ we have } 1R2 \text{ or } (1, 2) \in R \subseteq A \times A \\
&\text{Since } 3, 4 \in \{3, 4\}, \text{ we have } 3R4 \text{ or } (3, 4) \in R \subseteq A \times A \\
&\text{Since } 5, 6 \in \{5, 6\}, \text{ we have } 5R6 \text{ or } (5, 6) \in R \subseteq A \times A
\end{aligned}$$

Congruence modulo n

Discussion 9.18. Fix a positive integer $n \geqslant 2$. Recall that we say $a \equiv b \bmod n$ if

$$n \mid (a - b) \text{ if and only if } a \text{ and } b \text{ have the same remainder when divided by } n$$

We have seen in Example 9.10 that *congruence modulo n* is an equivalence relation. What are the equivalence classes?

$$\begin{aligned}
[0] &= \{x \in \mathbb{Z} \mid x \equiv 0 \bmod n\} = \{nk \mid k \in \mathbb{Z}\} \\
[1] &= \{x \in \mathbb{Z} \mid x \equiv 1 \bmod n\} = \{nk + 1 \mid k \in \mathbb{Z}\} \\
&= \quad \vdots \\
[n-1] &= \{x \in \mathbb{Z} \mid x \equiv n - 1 \bmod n\} = \{nk + (n-1) \mid k \in \mathbb{Z}\}
\end{aligned}$$

Since $n \in [0]$, therefore $[n] = [0]$.

Similarly, since $n + 1 \in [1]$, therefore $[n + 1] = [1]$; so on and so forth.

Note that the above list is of the form $[r]$ for $0 \leqslant r \leqslant n$, all possible remainders when a number is divided by r. In particular, for any integer $x \in \mathbb{Z}$, when divided by n, we have a quotient q and remainder r such that $x = nq + r$, and thus $x \in [r]$. Hence, $[0], [1], \ldots, [n-1]$ is the complete list of equivalence classes under the congruence relation modulo n.

We denote the collection of distinct equivalence classes under congruence modulo n as

$$\mathbb{Z}/n\mathbb{Z} = \underbrace{\{[0], [1], \ldots, [n-1]\}}_{n\text{-many elements}},$$

the set of *integers modulo n*, read as "$\mathbb{Z}$ mod $n\mathbb{Z}$".

Surprisingly, $\mathbb{Z}/n\mathbb{Z}$ has properties similar to that of $\mathbb{Z}$. We can define addition, subtraction and multiplication for elements in $\mathbb{Z}/n\mathbb{Z}$.

Addition. Given two elements $[a], [b] \in \mathbb{Z}/n\mathbb{Z}$, define

$$[a] + [b] \overset{\text{def}}{=} [a+b]$$

Here $[0]$ acts as a "zero" element under addition. That is,

$$[a] + [0] = [a] = [0] + [a]$$

Multiplication. Given two elements $[a], [b] \in \mathbb{Z}/n\mathbb{Z}$, define

$$[a] \cdot [b] \overset{\text{def}}{=} [ab]$$

Here $[0]$ acts as a "unit" element under multiplication. That is,

$$[a] \cdot [1] = [a] = [1] \cdot [a]$$

Also note that $[a] \cdot [0] = [0] = [0] \cdot [a]$.

Example 9.19. For $n = 5$, consider $\mathbb{Z}/5\mathbb{Z} = \{[0], [1], [2], [3], [4]\}$.

+	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

addition table

×	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

multiplication table

Observation. In the multiplication table, we have

$$[2] \cdot [3] = [1] = [3] \cdot [2] \quad \text{and} \quad [4] \cdot [4] = [1];$$

note that $[1]$ is "unit" element under multiplication.

In this way, we say

$$[2] \text{ is the "inverse" of } [3]$$

$$[3] \text{ is the "inverse" of } [2]$$

$$[4] \text{ is the "inverse" of } [4]$$

In this way, "division" in $\mathbb{Z}/5\mathbb{Z}$ is possible. "Dividing" by [2] means multiplying by [3], for example.

Division is not always possible for all $\mathbb{Z}/n\mathbb{Z}$.

Example 9.20. For $n = 4$, consider $\mathbb{Z}/4\mathbb{Z} = \{[0], [1], [2], [3]\}$.

×	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

multiplication table

For no $[a] \in \mathbb{Z}/4\mathbb{Z}$ do we get $[2] \cdot [a] = [1]$. So, "dividing" by [2] has no meaning in $\mathbb{Z}/4\mathbb{Z}$. Thus, division is not possible in $\mathbb{Z}/4\mathbb{Z}$.

Discussion 9.21 (Fact)**.** For a prime number p, $\mathbb{Z}/p\mathbb{Z}$ admits division.

If n is not prime, you cannot do division in $\mathbb{Z}/n\mathbb{Z}$. If $n = ab$, $1 < a, b < n$, then

$$[a] \cdot [b] = [n] = [0]$$

So, $[a], [b]$ are "zero divisors".

In $\mathbb{Z}/p\mathbb{Z}$, where p is a prime number, we can do all arithmetic operations: addition, subtraction, multiplication and division; this is an example of a *field*.

$$\underbrace{\underbrace{\underbrace{\text{addition, subtraction}}_{\text{group}}\text{, multiplication}}_{\text{ring}}\text{, division}}_{\text{field}}$$

10. Functions

Discussion 10.1. Let A, B be sets, recall that a function

$$f : A \to B$$

is a "rule" that assigns an element of B to every element of A. We note the following.

(i) $\operatorname{dom}(f) = A$. ($f$ is defined for every element of A)

(ii) For each $a \in A$, f assigns a *unique* element $f(a) \in B$.

We now give a formal definition of a function $f : A \to B$ in terms of relations.

Definition 10.2. Let A, B be non-empty sets. A function $f : A \to B$ is a relation $f \subseteq A \times B$ from A to B such that for every $a \in A$

$$\text{if } afb \text{ and } afc, \text{ then } b = c;$$

or equivalently we have

$$|f \cap (\{a\} \times B)| = 1$$

i.e. for every $a \in A$, there is a single element in f with a as the first coordinate.

That is, for every $a \in A$, there is a unique $b \in B$ that is f-related to a; that is, for every a, there is a unique b such that $(a, b) \in f$. In this case, we write $b = f(a)$. Notationally, we have

$$\begin{aligned} f : A &\to B \\ a &\mapsto b \end{aligned}$$

With the $a \mapsto b$ notation meaning $b = f(a)$.

With this notation, a relation f is a function if for any $a, c \in A$,

$$a = c \text{ implies } f(a) = f(c)$$

Verifying this property to show that a given relation is a function is called *showing f is well-defined*.

As a relation, f has a domain and range. We have $\operatorname{dom}(f) = A$ and $\operatorname{range}(f) = \{f(a) \mid a \in A\}$. To note, the range can be a proper subset of B; we call B the codomain of f, we denote $\operatorname{codom}(f) = B$.

Remark 10.3. In terms of our notation, the function f as a relation, that is, as a subset of $A \times B$, is

$$f = \{(a, f(a)) \mid a \in A\} \subseteq A \times B,$$

which is what we usually call the *graph of f*.

Example 10.4 (some abstract examples).

- *Identity function.*

  For any set X, the *identity function on* X is the function

  $$\begin{aligned} \mathrm{id}_X : X &\to X \\ x &\mapsto x \end{aligned}$$

  That is, this is the function $\mathrm{id}_X(x) = x$. As a relation, this is just the diagonal subset

  $$\mathrm{id}_X = \{(x,x) \mid x \in X\} \subseteq X \times X$$

- *Inclusion function.*

  For any non-empty set A, and a subset $C \subseteq A$. The inclusion function is the function

  $$\begin{aligned} \iota : C &\to A \\ c &\mapsto c \end{aligned}$$

  As a relation, this is the subset

  $$\iota = \{(c,c) \mid c \in C\} \subseteq C \times A$$

- *Restriction function.*

  Let $f : A \to B$ be a function, and consider a subset $C \subseteq A$. Then, the relation

  $$f|_C \overset{\text{def}}{=} f \cap (C \times B)$$

  is a function. This is now a function

  $$\begin{aligned} f|_C : C &\to B \\ c &\mapsto f(c) \end{aligned}$$

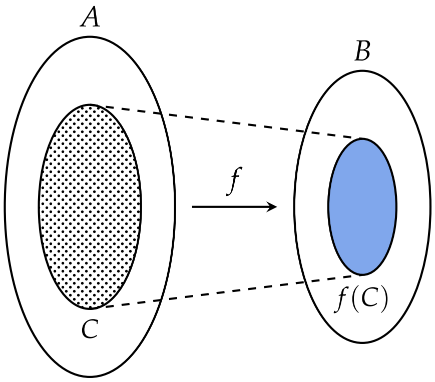
  where $\mathrm{dom}(f|_C) = C$. That is, given the rule f on A, we are restricting this rule to a subset.

Definition 10.5. Let $f : A \to B$ be a function, and let $C \subseteq A$ and $D \subseteq B$.

- The image of C under f is the set

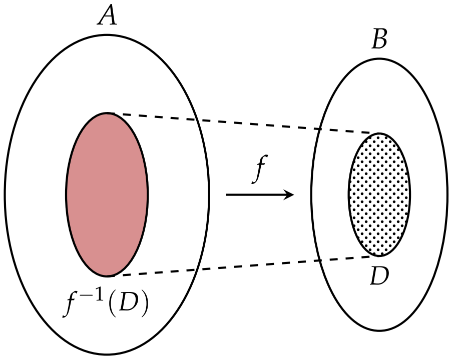
  $$f(C) \overset{\text{def}}{=} \{f(x) \mid x \in C\} \subseteq B$$

  Note that $\mathrm{range}(f) = f(A)$.



- The preimage of D under f is the set

$$f^{-1}(D) \overset{\text{def}}{=} \{y \in A \mid f(y) \in D\} \subseteq A$$



Definition 10.6. Let A, B be non-empty sets. Define,

$$B^A = \{f : A \to B \mid f \text{ is a function}\}$$

Lemma 10.7. *For non-empty finite sets A, B, we have $|B^A| = |B|^{|A|}$.*

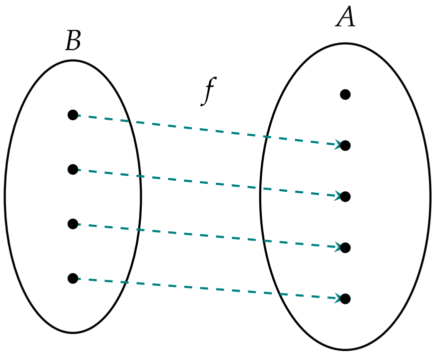
Proof. Each element in A has $|B|$-many choices to be mapped to. Each such choice gives us a unique function. Since each element has $|B|$-many choices, the total number of functions from A to B is

$$\underbrace{|B| \cdot |B| \cdots |B|}_{|A|\text{-times}} = |B|^{|A|}$$

This completes the proof. □

Definition 10.8. Let $f : A \to B$ be a function.

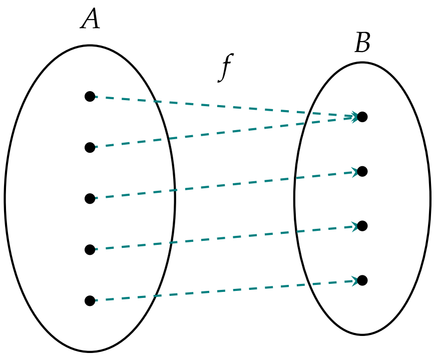
- f is said to be injective (or one-to-one) if "f maps distinct elements to distinct elements"; that is, if for every $x, y \in A$, $x \neq y$ implies $f(x) \neq f(y)$.



Equivalently, taking the contrapositive, f is injective if for every $x, y \in A$, $f(x) = f(y)$ implies $x = y$. This definition is more convenient for proofs.

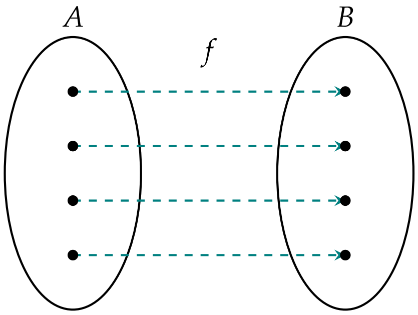
B has a "copy of A inside it".

- f is said to be surjective (or onto) if $f(A) = B$.



Equivalently, "if every element in B is mapped to by f", that is, for every $b \in B$, there exists an $a \in A$ such that $b = f(a)$ (this is just saying $B \subseteq f(A)$).

- f is bijective if it is both injective and surjective.



f gives an exact correspondence of elements between A and B. So sets A and B have the "same size".

Example 10.9. A function $f : \mathbb{R} \setminus \{2\} \to \mathbb{R} \setminus \{3\}$ is given by

$$f(x) = 3 + \frac{6}{x-2}$$

(f is not defined for $x = 2$ and its value can never be 3).

Show that f is a bijection.

Proof. We show f is injective and bijective. To show f is injective, suppose $x, y \neq 2$ are such that $f(x) = f(y)$, we want to show $x = y$. So, note

$$\begin{aligned} f(x) &= f(y) \\ 3 + \frac{6}{x-2} &= 3 + \frac{6}{y-2} \\ \frac{6}{x-2} &= \frac{6}{y-2} && \text{subtracting 3} \\ 6(y-2) &= 6(x-2) && \text{cross-multiplying} \\ 6y - 12 &= 6x - 12 \end{aligned}$$

$$
\begin{aligned}
6y &= 6x && \text{adding 12} \\
y &= x && \text{dividing by 6}
\end{aligned}
$$

Thu, f is injective.

To show f is surjective, let $b \in \mathbb{R} \setminus \{3\}$. We show that there exists an element $a \in \mathbb{R} \setminus \{2\}$ such that $f(a) = b$.

> *Scratch work.* We will work backwards to find such an a; suppose we did have $f(a) = b$, we solve for a.
>
> $$
> \begin{aligned}
> 3 + \frac{6}{a-2} &= f(a) = b \\
> \frac{6}{a-2} &= b - 3 && \text{subtracting 3} \\
> \frac{a-2}{6} &= \frac{1}{b-3} && \text{taking reciprocal, we can since } b \neq 3 \\
> a - 2 &= \frac{6}{b-3} && \text{multiplying by 6} \\
> a &= 2 + \frac{6}{b-3} && \text{adding 2}
> \end{aligned}
> $$
>
> Note that this expression is $\neq 2$.

For given b, consider

$$a = 2 + \frac{6}{b-3} \in \mathbb{R} \setminus \{2\}$$

This is such that

$$
\begin{aligned}
f(a) &= 3 + \frac{6}{a-2} \\
&= 3 + \frac{6}{\left(2 + \frac{6}{b-3}\right) - 2} \\
&= 3 + \frac{6}{\frac{6}{b-3}} \\
&= 3 + \frac{6(b-3)}{6} \\
&= 3 + (b-3) \\
&= b
\end{aligned}
$$

Thus f is surjective.

This completes the proof. □

Discussion 10.10. We can characterise injectivity and surjectivity in another way. Let $f : A \to B$ be a function. For any $b \in B$, we can consider its pre-image

$$f^{-1}(\{b\}) = \{a \in A \mid f(a) = b\}$$

f is injective if and only if $|f^{-1}(\{b\})| \leqslant 1$ for every $b \in B$.

f is surjective if and only if $|f^{-1}(\{b\})| \geqslant 1$ for every $b \in B$.

Therefore f is bijective if and only if $|f^{-1}(\{b\})| = 1$.

Definition 10.11 (Composition of Functions)**.** Let $f : A \to B$ and $g : B \to C$ be functions. Then their composition is the function

$$g \circ f : A \to C$$

defined as

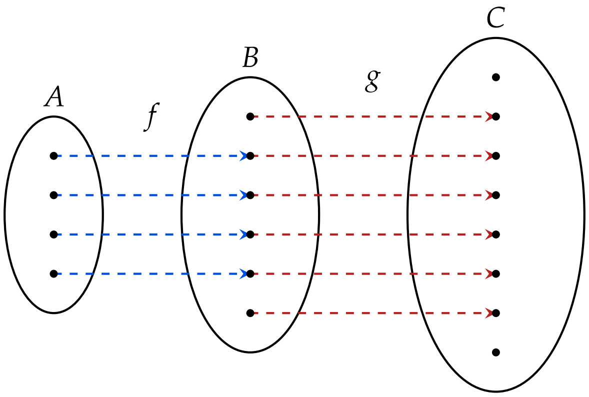
$$(g \circ f)(a) = g(f(a))$$

for any $a \in A$.

Proposition 10.12. *Let $f : A \to B$ and $g : B \to C$ be functions.*

(1) If both f and g are injective, then their composition $g \circ f$ is also injective.

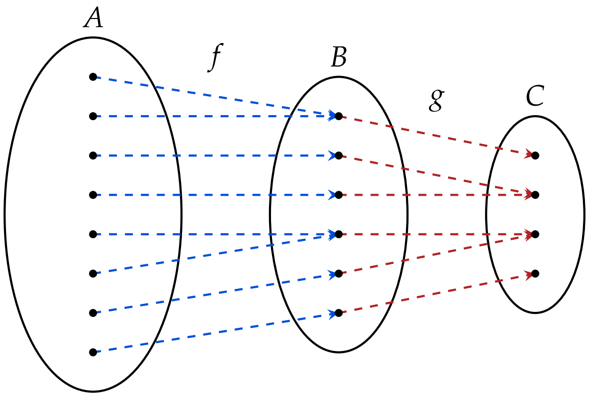
(2) If both f and g are surjective, then their composition $g \circ f$ is also surjective.



Proof of (1). Suppose f and g are injective, we need to show $g \circ f$ is injective. Consider any $x, y \in A$ such that $(g \circ f)(x) = (g \circ f)(y)$, we need to show $x = y$. We have,

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

since g is injective, we have $f(x) = f(y)$. Now, since f is injective, we obtain $x = y$. Hence $g \circ f$ is injective. □



Proof of (2). Suppose f and g are surjective, we need to show $g \circ f$ is surjective. We aim to show that for every $c \in C$, we can find an $a \in A$ such that $(g \circ f)(a) = c$.

Consider any $c \in C$, since g is surjective, there exists a $b \in B$ such that $g(b) = c$. Since f is surjective, for this b, there exists an $a \in A$ such that $f(a) = b$. Hence,

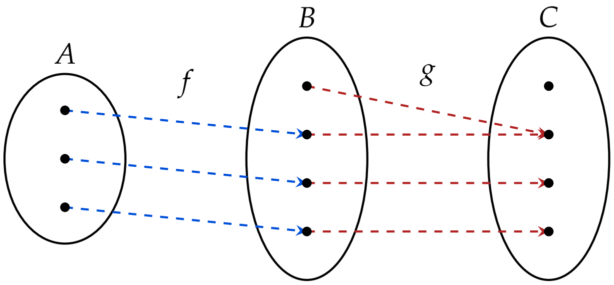
$$(g \circ f)(a) = g(f(a)) = g(b) = c.$$

Thus $g \circ f$ is surjective. □

What about the converse?

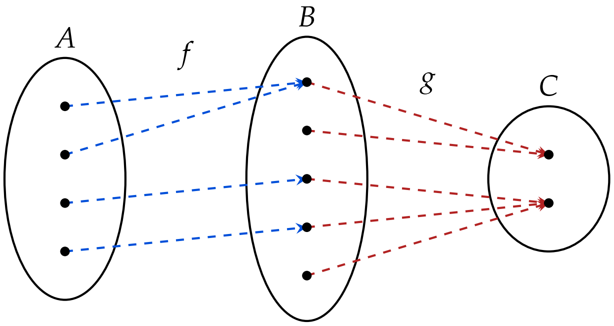
Proposition 10.13. *Let $f : A \to B$ and $g : B \to C$ be functions.*

(1) *If $g \circ f$, then f is injective.*



g need not be injective in (1)

(2) *If $g \circ f$ is surjective, then g is surjective.*



f need not be surjective in (2)

Proof of (1). Suppose $g \circ f$ is injective, we need to show f is injective. Consider any $x, y \in A$ such that $f(x) = f(y)$, we need to show $x = y$.

Since $f(x) = f(y)$, therefore $g(f(x)) = g(f(y))$. That is,

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

Since $g \circ f$ is injective, we obtain $x = y$. Hence f is injective. □

Proof of (2). Suppose $g \circ f$ is surjective, we need to show g is surjective. We aim to show that for every $c \in C$, we can find an $b \in B$ such that $g(b) = c$.

Consider any $c \in C$, since $g \circ f$ is surjective, there exists a $a \in A$ such that $(g \circ f)(a) = c$. Define $b = f(a)$, then $g(b) = g(f(a)) = (g \circ f)(a) = c$. Hence g is surjective. □

Definition 10.14. Two functions f and g are said to be equal, denoted $f = g$ if

(1) $\operatorname{dom} f = \operatorname{dom} g$; and

(2) $f(x) = g(x)$ for every $x \in \operatorname{dom} f = \operatorname{dom} g$.

Theorem 10.15. *Let $f : A \to B$ and $g : B \to A$ be functions. Suppose,*

$$g \circ f = \mathrm{id}_A \quad \textit{and} \quad f \circ g = \mathrm{id}_B$$

Then f and g are bijective, and are inverses of each other as relations.

We call g the *inverse function* of f (or vice versa).

Remark 10.16. Often the most convenient way to show a function $f : A \to B$ is bijective is to find a function $g : B \to A$ such that $f \circ g = \mathrm{id}_B$ and $g \circ f = \mathrm{id}_A$. If we can find such a function, we do not have give a separate argument on the injectivity and surjectivity of f.

Proof. Since the identity functions are bijective, we obtain that $g \circ f$ and $f \circ g$ are both bijective. In particular, $g \circ f$ and $f \circ g$ are injective, therefore by Theorem 10.13 (1), we obtain f and g are injective respectively. We also have that $g \circ f$ and $f \circ g$ are surjective, therefore by Theorem 10.13 (2), we obtain f and g are surjective. Hence, both f and g are injective and surjective, and thus bijective.

Since $g \circ f = \mathrm{id}_A$, one can show by set inclusion arguments that as relations $g = f^{-1}$, where f^{-1} is the inverse relation of f. That is, in this case the relation f^{-1} is a function (in fact, f^{-1} is a function if and only if f is bijective). □

Example 10.17. A function $f : \mathbb{R} \setminus \{2\} \to \mathbb{R} \setminus \{3\}$ is given by

$$f(x) = 3 + \frac{6}{x-2}$$

Show that f is a bijection.

Proof. We produce an inverse function to prove f is bijective.

Scratch work. We do some algebra to obtain the inverse function.

Step 1. First let $y = f(x)$, that is,

$$y = 3 + \frac{6}{x-2}$$

Step 2. Replace x by y and vice versa. That is,

$$x = 3 + \frac{6}{y-2}$$

Step 3. Solve for y.

$$\begin{aligned} 3 + \frac{6}{y-2} &= x \\ \frac{6}{y-2} &= x - 3 && \text{subtracting 3} \\ \frac{y-2}{6} &= \frac{1}{x-3} && \text{taking reciprocal, we can since } b \neq 3 \\ y - 2 &= \frac{6}{x-3} && \text{multiplying by 6} \\ y &= 2 + \frac{6}{x-3} && \text{adding 2} \end{aligned}$$

Note that this expression is $\neq 2$.

Step 4. The resulting y is your candidate for an inverse function.

Define $g : \mathbb{R} \setminus \{3\} \to \mathbb{R} \setminus \{2\}$ as

$$g(x) = 2 + \frac{6}{x-3}$$

Then,

$$\begin{aligned} (g \circ f)(x) = g(f(x)) &= 2 + \frac{6}{f(x) - 3} \\ &= 2 + \frac{6}{\left(3 + \frac{6}{x-2}\right) - 3} \\ &= 2 + \frac{6}{\left(\frac{6}{x-2}\right)} \\ &= 2 + \frac{6(x-2)}{6} \\ &= 2 + (x-2) = x \end{aligned}$$

$$\begin{aligned} (f \circ g)(x) = f(g(x)) &= 3 + \frac{6}{g(x) - 2} \\ &= 3 + \frac{6}{\left(2 + \frac{6}{x-3}\right) - 2} \\ &= 3 + \frac{6}{\left(\frac{6}{x-3}\right)} \\ &= 3 + \frac{6(x-3)}{6} \\ &= 3 + (x-3) = x \end{aligned}$$

Hence $f \circ g = \mathrm{id}$ and $g \circ f = \mathrm{id}$. Thus f is bijective. $\square$

Remark 10.18 (Common Notations)**.** We commonly also use the word *map* to mean a function, and if $b = f(a)$, we say *a maps to b under* f, the symbolic notation for which is $a \mapsto b$, as we have seen.

Given a function $f : A \to B$, if

- f is injective, then one often writes this as $f : A \hookrightarrow B$.
- f is surjective, then one often writes this as $f : A \twoheadrightarrow B$.
- f is bijective, then one often writes this as $f : A \xrightarrow{\sim} B$.

11. Cardinality of Sets

Discussion 11.1. We want to "count the number of elements in a set". For finite sets, we simply do that, count the number of elements in the set. For infinite sets, how do we "count"? There are many sets with infinitely many elements ; for example

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

are infinite sets. Here $\mathbb{N} \overset{\text{def}}{=} \mathbb{Z}_{>0} = \{1, 2, 3, \ldots\}$. How can we compare the number of elements in these sets? Since the above sets are related by proper inclusions, we may expect there are different levels of infinity.

Lemma 11.2. *Let A, B be finite sets, then $|A| = |B|$ if and only if there exists a bijection $f : A \to B$.*

Proof.

($\Rightarrow$) Suppose $|A| = |B| = n$; write $A = \{a_1, \ldots, a_n\}$ and $B = \{b_1, \ldots, b_n\}$. Define the function

$$f : A \to B,\ a_i \mapsto b_i,$$

this is evidently a bijection.

($\Leftarrow$) Suppose there exists a bijection $f : A \to B$. Let $|A| = n$; write $A = \{a_1, \ldots, a_n\}$. Since f is a bijection, it is in particular an injection, therefore $f(A) = \{f(a_1), \ldots, f(a_n)\}$ is such that $|f(A)| = n$. Since f is also surjective, $f(A) = B$, and hence $|B| = n$. □

This motivates the following general definition.

Definition 11.3. Let A, B be sets. A and B are said to be numerically equivalent (or have the same cardinality, or have the same number of elements), denoted $|A| = |B|$, if there exits a bijection

$$f : A \to B$$

If A is finite with n-many elements, we write $|A| = n$.

Theorem 11.4. *Numerical equivalence is a equivalence relation among sets.*

Definition 11.5. Let A be a set.

- A is said to be denumerable if $|A| = |\mathbb{N}|$, that is, if there exists a bijection

$$f : \mathbb{N} \to A$$

  This means we can enumerate, label with positive integers, the elements of A. So, we can write $A = \{a_1, a_2, \ldots\}$.

- A is said to be countable if $|A| < \infty$ or $|A| = |\mathbb{N}|$, that is, if A is finite or denumerable.

- A is said to be uncountable if A is not countable.

Discussion 11.6. We will soon see that there are different levels of infinity, different infinite cardinalities. We will try and see that

$$\underbrace{|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}|}_{\text{denumerable}} < |\mathbb{R}| = |\mathbb{R} \times \mathbb{R}| = |\mathbb{R} \times \mathbb{R} \times \mathbb{R}| \underbrace{< (?) < (??) < \cdots < (?!?!?!) < \cdots}_{\text{these sets do exist}}$$

- $|\mathbb{N}| < |\mathbb{R}|$ was proved by Cantor using *Cantor's diagonal argument*.
- $|\mathbb{R}| = |\mathbb{R}^n|$, that is, there exists a bijection $f : \mathbb{R} \to \mathbb{R}^n$. It is enough to show $|\mathbb{R}| = \left|\mathbb{R}^2\right|$, that is, the real line and the plane have the same number of points, this is done by considering *space-filling curves* (or *Peano curves*).

Continuum Hypothesis. Can there be an infinite set A such that $|\mathbb{N}| < |A| < |\mathbb{R}|$.

Theorem 11.7.

(1) An infinite subset of a denumerable set is denumerable.

(2) A cartesian product of denumerable sets is denumerable.

Proof of Theorem 11.7(1). Let A be a denumerable set and let $S \subseteq A$ be infinite. Then, by definition, there exists a bijection

$$f : \mathbb{N} \to A$$

Consider $f^{-1}(S) \subseteq \mathbb{N}$, necessarily infinite, we order the elements in this set as

$$k_1 < k_2 < \cdots < k_n < \cdots$$

Then, we can define a bijection

$$g : \mathbb{N} \to f^{-1}(S),\ i \mapsto k_i$$

Thus, $|\mathbb{N}| = |f^{-1}(S)|$.

Now, note that the function

$$f^{-1}(S) = \{k \in \mathbb{N} \mid f(k) \in S\} \to S : k \mapsto f(k)$$

is a bijection; and hence $|f^{-1}(S)| = |S|$.

Thus, $|S| = |\mathbb{N}|$ (as numerical equivalence is, in particular, transitive, by Theorem 11.4) and therefore S is denumerable. □

Example 11.8. $2\mathbb{N}$, the set of even numbers, is denumerable. One can explicitly also give a bijection

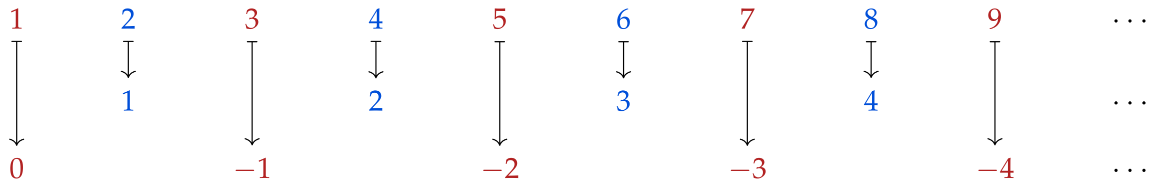
$$2\mathbb{N} \to \mathbb{N} : n \mapsto n/2$$

Remark 11.9. Theorem 11.7 (1) tells us that, for an infinite set A, it is enough to exhibit an *injective function* $f : A \to X$, where X is denumerable, to conclude A is denumerable.

Since if f is injective, then $f : A \to f(A)$ is a bijection, so $|A| = |f(A)|$. Since A is infinite, so is $f(A)$. Now, $f(A)$ is an infinite subset of X, a denumerable set, and is therefore denumerable.

Proposition 11.10. $|\mathbb{Z}| = |\mathbb{N}|$

Strategy. Our strategy is the following: we will send even numbers to positive integers, and odd numbers to non-positive integers.



Proof. We explicitly construct a bijection $\mathbb{N} \to \mathbb{Z}$. Consider the function

$$f : \mathbb{N} \to \mathbb{Z},\ n \mapsto \begin{cases} \dfrac{n}{2} & \text{if } n \text{ is even} \\[2ex] \dfrac{1-n}{2} & \text{if } n \text{ is odd} \end{cases}$$

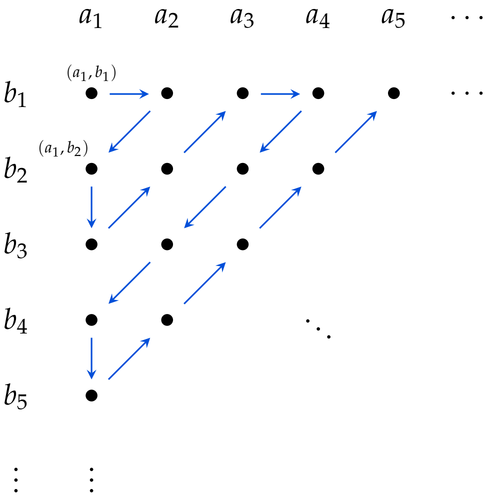
One directly verifies that this is a bijection. □

Proof of Theorem 11.7(2). Let A and B be two denumerable sets. Then we can order elements of A and B as

$$A = \{a_1, a_2, a_3, \dots, a_n, \dots\}$$

$$B = \{b_1, b_2, b_3, \dots, b_n, \dots\}$$

Then we can order $A \times B$ as follows



$\longrightarrow$ gives us one way to order all elements in $A \times B$, hence $|\mathbb{N}| = |A \times B|$. □

Discussion 11.11. We saw that $|\mathbb{Z}| = |\mathbb{N}|$. This is a common phenomenon with infinite sets, and a property not shared with finite sets: infinite sets may have the same cardinality as a proper subsets.

Our goal now is to prove $|\mathbb{Q}| = |\mathbb{N}|$ and $|\mathbb{N}| < |\mathbb{R}|$. That is, that $\mathbb{Q}$ is denumerable and $\mathbb{R}$ is uncountable.

Theorem 11.12. *The set $\mathbb{Q}$ is countable.*

Proof. We will show that there is a injective map from $\mathbb{Q}$ to a denumerable set, and we will have proven that $\mathbb{Q}$ is denumerable as per Remark 11.9.

Note that any rational number $r \in \mathbb{Q}$ can be written in its reduced form, that is, as

$$r = \frac{a}{b}, \quad a \in \mathbb{Z}, b \in \mathbb{N}, \text{and } a \text{ and } b \text{ have no common factors}$$

Then we have the following injective function

$$f : \mathbb{Q} = \left\{ \frac{a}{b} \mid \frac{a}{b} \text{ is in reduced form} \right\} \to \mathbb{Z} \times \mathbb{N},\ \frac{a}{b} \mapsto (a, b)$$

Note that this map is not surjective, since, for example, $(4, 6) \in \mathbb{Z} \times \mathbb{N}$ is not in the range of f because

$$\frac{4}{6} = \frac{2}{3}, \text{ and } f\left(\frac{2}{3}\right) = (2, 3)$$

In any case, this completes the proof. □

Uncountable Sets

Theorem 11.13. *The open interval $(0, 1)$ has the same cardinality as $\mathbb{R}$.*

Proof. The main idea is to find a function that "stretches $(0, 1)$" to $\mathbb{R}$. Consider the function

$$f : (0, 1) \to \mathbb{R},\ x \mapsto -\frac{1}{x} + \frac{1}{1 - x}$$

It's straightforward to show it is injective but for surjectivity we are forced to revert to some limit arguments that are beyond the scope of this course. To convince yourself, you can graph the function and see that the range is indeed all of $\mathbb{R}$.

Thus, $|(0, 1)| = |\mathbb{R}|$. □

Theorem 11.14. $|\mathbb{N}| < |\mathbb{R}|$

Proof. In view of the previous theorem, it suffices to show that $|\mathbb{N}| < |(0, 1)|$. For the sake of contradiction, assume $|(0, 1)| = |\mathbb{N}|$. That is, there exists a bijection

$$f : \mathbb{N} \to (0, 1)$$

We examine the range of f. Any real number $0 < r < 1$ has a decimal expansion. If r is irrational, then it has a unique decimal expansion. On the other hand, if r is rational, then it can have two possible decimal expansions; for example,

$$0.4000000\ldots = 0.399999\ldots$$

In this case, we choose the expansion with a string of 0's from some point on. Thus, for every element in the range of f (which is all of $(0,1)$ as f is surjective), we can choose a distinct decimal expansion

$$\begin{aligned}
f(1) &= a_1 = 0.a_{11}a_{12}a_{13}a_{14}\ldots\\
f(2) &= a_2 = 0.a_{21}a_{22}a_{13}a_{14}\ldots\\
f(3) &= a_3 = 0.a_{31}a_{32}a_{33}a_{34}\ldots\\
f(4) &= a_4 = 0.a_{41}a_{42}a_{43}a_{44}\ldots\\
&\vdots
\end{aligned}$$

Cantor chose to examine the diagonal entries to produce an element in $(0,1)$ that is part of this list, that is, not contained in the range of f, thereby contradicting its surjectivity.

Consider a sequence $\{b_n\}_{n\geqslant 1}$, where for each n, we have $0 \leqslant b_n \leqslant 9$, given by

$$b_k = \begin{cases} a_{kk}+1 & \text{if } 0 \leqslant a_{kk} < 9 \\ 0 & \text{if } a_{kk} = 9 \end{cases}$$

Consider the real number

$$b = 0.b_1b_2b_3b_4\ldots$$

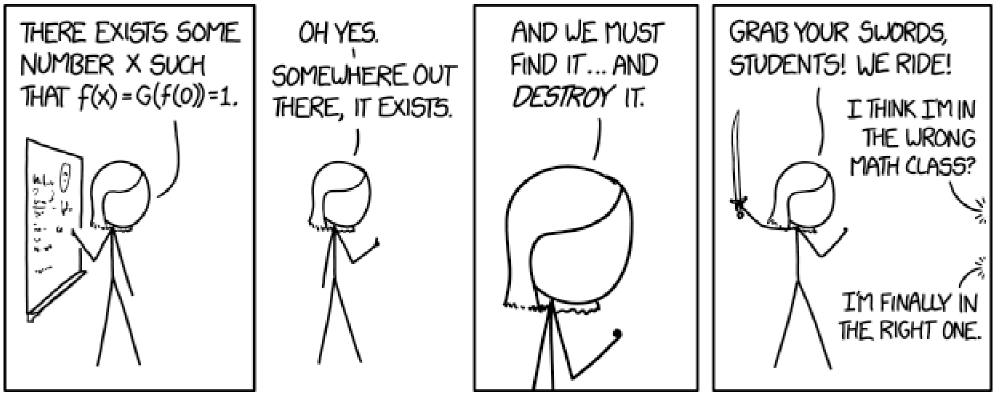
Note that for each n, $b \neq f(n) = a_n$, since they have different n^{th} digits in their decimal expansion. We have produced an $b \in (0,1)$ but $b \notin f(\mathbb{N})$ and hence $f(\mathbb{N}) \neq \mathbb{R}$, contradicting the surjectivity of f. Thus, $|\mathbb{N}| < |(0,1)| = |\mathbb{R}|$. □

References

[CPZ18] Gary Chartrand, Albert D. Polimeni, and Ping Zhang, *Mathematical Proofs: A Transition to Advanced Mathematics*, Fourth ed., Pearson, 2018.

Solving a problem for which you know there's an answer is like climbing a mountain with a guide, along a trail someone else has laid. In mathematics, the truth is somewhere out there in a place no one knows, beyond all the beaten paths. And it's not always at the top of the mountain. It might be in a crack on the smoothest cliff or somewhere deep in the valley.

– Yoko Ogawa, *The Housekeeper and the Professor*


THERE EXISTS SOME NUMBER X SUCH THAT f(X) = G(f(0)) = 1.
OH YES. SOMEWHERE OUT THERE, IT EXISTS.
AND WE MUST FIND IT... AND DESTROY IT.
GRAB YOUR SWORDS, STUDENTS! WE RIDE!
I THINK I'M IN THE WRONG MATH CLASS?
I'M FINALLY IN THE RIGHT ONE.

Existence Proof by xkcd