

MATH 109 lecture notes

Lucas Buzaglo

Based on lecture notes by Rayan Saab

Fall 2026

Math 109: Mathematical Reasoning

- **Book:** *An Introduction to Mathematical Reasoning*, Peter J. Eccles.
- **Webpage:** <https://mathweb.ucsd.edu/~lbuzaglo/teaching/109F26/index.html>

Grading

Higher of two formulas:

- (1) 20/20/20/40 (HW / MT1 / MT2 / Final)
- (2) 20/20/60 (HW / $\max(\text{MT1}, \text{MT2})$ / Final)

Course Objectives

- Introduction to rigorous mathematics, in other words, methods of reasoning where all assumptions are clear and conclusions follow logically.
- Emphasis on clear proof writing.

Some Topics we will cover

- Propositions, truth tables, logical implications
- Proof techniques:
 - direct proof
 - proof by cases
 - proof by contradiction
 - proof by contrapositive
 - proof by induction
- Set theory

- Functions, injections, surjections, bijections
- Binomial coefficients / theorem
- Countability of sets

1 The language of mathematics

1.1 Propositions, predicates, and statements

Definition 1.1. A *proposition* is a sentence that is either true or false (but not both).

Example 1.2. Propositions:

- $2 \times 5 = 10$ (true)
- $\pi = 3$ (false)
- Every even integer greater than two is the sum of two prime numbers (Goldbach conjecture from 1742; it is unknown whether this is true or false)

Not propositions:

- $n^2 + 3n > 7$
- $m < n$

These two are *predicates*. They become propositions when values are assigned to n (and to m for the second one). Finally, $12 - 5$ is neither a proposition nor a predicate: it is an expression, not a sentence.

Definition 1.3. A *statement* is a proposition or predicate.

In particular, $12 - 5$ is **not** a statement.

1.2 Logical connectives (or/and/not)

Logical connectives are “tools” to put together simple statements and form complicated ones.

1.2.1 The connective “or”

Consider two statements P and Q , each of which may be either true (T) or false (F). The statement “ P or Q ” is also either true or false, depending on the truth values of P and Q . The mathematical notation for this statement is $P \vee Q$.

In fact, we define the logical connective $\vee$ (“or”) by means of a truth table:

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

Example 1.4. • $(a = 0) \vee (b = 0)$

- $a \geq 0$ ($a > 0$ or $a = 0$)
- $a = \pm b$ ($a = b$ or $a = -b$)

Caution. The connective $\vee$ is an “inclusive or”, i.e. for the statement “ $P \vee Q$ ” to be true, it is enough for one of the two statements P, Q to be true (if both are true, “ $P \vee Q$ ” is still true — see the truth table).

Example 1.5. $1 = \pm 1$ is true because $1 = 1$ is true.

1.2.2 The connective “and”

The notation is $\wedge$.

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

Example 1.6. $3 < \pi < 4$ ($3 < \pi$ and $\pi < 4$).

1.2.3 The connective “not” (negation of a statement)

The negation of a statement P is denoted $\neg P$ (some texts use $\overline{P}$ instead).

P	$\neg P$
T	F
F	T

Example 1.7. Let P be the statement ‘For real numbers a , if $f(a) = 0$, then $a > 0$ ’. Write down the statement $\neg P$.

Solution. There exists a real number a such that $f(a) = 0$ and $a \leq 0$.

We will deal with such statements formally next.

2 Implications

Definition 2.1. A *proof* is a sequence of statements starting with true statements and finishing with the statement to be proved.

Informally, the way we move from statement to statement is via ‘implications’.

Example 2.2. Suppose $P(n)$ is the statement ' $n > 2$ ' and $Q(n)$ is the statement ' $n > 0$ '. Now, we can define a new statement ' $P(n) \implies Q(n)$ '.

$$\underbrace{n > 2}_{\text{hypothesis}} \implies \underbrace{n > 0}_{\text{conclusion}}$$

This is clearly a true statement for each integer n (even though $P(n)$ and $Q(n)$ are not true for every value of n).

	$P(n)$	$Q(n)$
$n \leq 0$	F	F
$n = 1$	F	T
$n = 2$	F	T
$n > 2$	T	T

Notice above:

- When P was true, so was Q .
- When P was false, Q could be anything.
- Q was never false if P was true.

Intuitively, the statement $P(n) \implies Q(n)$ should be true for all values of n . If we want to define implication to match our intuition, we are therefore forced to make the following definition.

Definition 2.3. *Implication* (denoted $\implies$) is defined by the following table.

P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T
F	F	T

Example 2.4. Here are some 'funny' examples:

- The statement $(\pi < 4) \implies (1 + 1 = 2)$ is true.
- The statement $(\pi < 4) \implies (1 + 1 = 3)$ is false (why?).

Note: There is no cause/effect relationship in our mathematical use of ' $P \implies Q$ '.

Definition 2.5. A *universal implication* is an implication involving one or more free variables that is true no matter what values are assigned to the free variable(s).

Example 2.6. $n > 3 \implies n > 0$ is a universal implication.

Example 2.7 (Not a universal implication). The statement $n \geq 4 \implies n \geq 6$ is **not** universally true.

	$n \geq 4$	$n \geq 6$	$n \geq 4 \implies n \geq 6$
$n < 4$	F	F	T
$4 \leq n < 6$	T	F	F
$n \geq 6$	T	T	T

The issue is in the row $4 \leq n < 6$: there *exist* values of n for which the hypothesis is true and the conclusion is false. In other words, there is a value of n for which the statement becomes $T \implies F$, whose truth value is F .

Here are some ways to read the statement $P \implies Q$:

- (i) If P then Q .
- (ii) P implies Q .
- (iii) Q if P .
- (iv) P only if Q .
- (v) Q whenever P .
- (vi) P is sufficient for Q .
- (vii) Q is necessary for P .

Definition 2.8. The notation $(P \iff Q)$ means $(P \implies Q)$ and $(Q \implies P)$. Here are some ways to read it:

- (i) P is equivalent to Q .
- (ii) P is necessary and sufficient for Q .
- (iii) P if and only if Q (P iff Q).
- (iv) P precisely when Q (don't like).

2.1 Arithmetic

Definition 2.9. Given two integers a and b , we say that b *divides* a or that a *is a multiple of* b to mean that there is an integer q with

$$a = bq.$$

The notation for this is $b \mid a$.

Example 2.10.

- 3 divides 6.
- -4 divides 8.
- n divides 0 whatever integer n is (why?).

We now define even and odd integers rigorously, using the notion of divisibility defined above. When answering homework or exam questions involving even/odd numbers, you should generally use the definition below in your proof.

Definition 2.11. 1. Given an integer n , we say n is even to mean 2 divides n .

2. Given an integer n , we say n is odd to mean n is not even.

Remark 2.12. We used the definition of ‘even’ to define ‘odd’, and the definition of ‘divides’ to define even. Such chains of definitions are common.

Example 2.13. Prove the proposition “1023 is odd”.

Proof. We need to show that 1023 is odd, i.e., that it is not even, i.e., that there is no integer q such that $1023 = 2q$.

We cannot check all integers q one by one. Instead, note that every integer q satisfies either $q \leq 511$ or $q \geq 512$. If $q \leq 511$, then $2q \leq 1022$, and if $q \geq 512$, then $2q \geq 1024$. In either case $2q \neq 1023$, so 1023 is odd. $\square$

Remark 2.14. The symbol $\square$ marks the end of a proof.

In the remainder of the course we will assume the following algebraic properties of real numbers, and of the $+$ and $\times$ operations.

Axioms 2.15. For real numbers a , b and c :

(i) **Commutativity:**

$$a + b = b + a \quad ab = ba$$

(ii) **Associativity:**

$$a + (b + c) = (a + b) + c \quad (ab)c = a(bc)$$

(iii) **Distributivity:**

$$a(b + c) = ab + ac \quad (a + b)c = ac + bc$$

(iv) **Additive identity 0:** $a + 0 = a = 0 + a$

(v) **Multiplicative identity 1:** $a \times 1 = a = 1 \times a$

(vi) **Subtraction:** $a + x = 0$ has the unique solution $x = -a$ so

$$a + x = b \iff x = b + (-a) = b - a$$

(vii) **Division:** If $a \neq 0$, $ax = 1$ has the unique solution $x = 1/a$ so

$$ax = b \iff x = b \left(\frac{1}{a} \right) = ba^{-1}.$$

All the usual algebraic properties of real numbers can be deduced from the above axioms.

3 Proofs

Many theorems are of the form $(P \implies Q)$.

Recall the truth table for implication:

P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T
F	F	T

Note: Rows three and four mean that $P \implies Q$ is always true when P is false (regardless of Q 's truth value).

Therefore, to prove " $P \implies Q$ ", it is enough to assume that P is true and deduce Q (we only need to show that row two of the above table cannot occur). This is called *direct proof*.

Example 3.1. For **positive** real numbers a and b , we have $a < b \implies a^2 < b^2$.

Proof. Following the reasoning above, we assume that $a < b$. Now,

$$(a < b) \implies (a^2 < ab) \quad \textcircled{1}$$

and

$$(a < b) \implies (ab < b^2) \quad \textcircled{2}$$

So $a < b$ implies both $a^2 < ab$ and $ab < b^2$, and $[(a^2 < ab) \wedge (ab < b^2)] \implies (a^2 < b^2)$. Hence

$$(a < b) \implies (a^2 < b^2). \quad \textcircled{3}$$

□

We need to justify why steps ①, ②, ③ are correct. These are justified by the *inequality axioms* (also known as *order axioms*) of real numbers.

Axioms 3.2 (Inequality axioms). For real numbers a, b, c :

- (i) **Trichotomy:** One and only one of the three possibilities $a < b$, $a = b$, $a > b$ is true.
- (ii) **Addition:** $a < b \iff a + c < b + c$.
- (iii) **Multiplication:**

$$\begin{aligned} a < b &\iff ac < bc && \text{if } c > 0, \\ a < b &\iff ac > bc && \text{if } c < 0. \end{aligned}$$

- (iv) **Transitivity:** $a < b$ and $b < c \implies a < c$.

Question 3.3. Which of the axioms was used to justify each of ①, ②, ③?

Remark 3.4. We could have (or perhaps should have) written the proof with more words and fewer symbols. See the book for more details.

3.1 Proof by cases

Example 3.5. If $x = 2$ or $x = 7$ then $x^2 - 9x + 14 = 0$.

Proof. If $x = 2$ then $x^2 - 9x + 14 = 4 - 18 + 14 = 0$.

If $x = 7$ then $x^2 - 9x + 14 = 49 - 63 + 14 = 0$.

Hence if $x = 2$ or $x = 7$ then $x^2 - 9x + 14 = 0$. □

Note: We used the observation that $(P \vee Q) \implies R$ is equivalent to $(P \implies R) \wedge (Q \implies R)$.

Exercise 3.6. Using truth tables, check that the statement $(P \vee Q) \implies R$ is equivalent to $(P \implies R) \wedge (Q \implies R)$.

Example 3.7. For real numbers x , $x^2 \geq 0$.

Idea (scratch). Since this statement involves inequalities, we should attempt to use the inequality axioms. Note that

$$x^2 = x \cdot x$$

There are three cases: $x = 0$, $x > 0$, or $x < 0$ (trichotomy).

Proof. For a real number x , either $x = 0$, $x > 0$, or $x < 0$ (three cases). By the multiplication laws:

1. If $x = 0$ then $x^2 = 0$.

2. If $x > 0$ then $x^2 > 0$.

3. If $x < 0$ then $x^2 > 0$.

Hence, $x^2 \geq 0$ as required. □

3.2 Proof technique: backward proof

Useful tip. Often, to construct a proof, a good approach is to work *backward*.

Proposition 3.8. For real numbers a and b

$$(a < b) \implies 4ab < (a + b)^2.$$

Idea. Working backward, we have

$$\begin{aligned} 4ab < (a + b)^2 &\Leftarrow 4ab < a^2 + 2ab + b^2 \\ &\Leftarrow 0 < a^2 - 2ab + b^2 \\ &\Leftarrow 0 < (a - b)^2 \\ &\Leftarrow a \neq b \quad (\text{why?}) \\ &\Leftarrow a < b \end{aligned}$$

(actually these are $\iff$, but $\Leftarrow$ is enough for us to work backward).

So $a < b \implies 4ab < (a + b)^2$.

The above is **not** a finished proof! Instead, we should write a direct proof by reversing the steps of the backward argument above.

Proof. We have

$$\begin{aligned} a < b &\implies a \neq b \implies (a - b) \neq 0 \\ &\implies 0 < (a - b)^2 \implies 0 < a^2 - 2ab + b^2 \\ &\implies 4ab < a^2 + 2ab + b^2 \\ &\implies 4ab < (a + b)^2 \end{aligned}$$

Thus, $a < b \implies 4ab < (a + b)^2$. □

4 Proof by contradiction

Definition 4.1. A *contradiction* is a statement of the form $P \wedge (\neg P)$.

Example 4.2. For integers a , the statement

“ a is even and a is odd”

is a contradiction (why?).

4.1 Example of a proof by contradiction

Proposition 4.3. *There are no integers m, n such that $6m + 8n = 75$.*

Remark 4.4. A direct approach here is a bad idea, because we would have to check all pairs of integers m, n , of which there are infinitely many.

Idea. Note that

$$\begin{aligned} 6m &\text{ is even} \\ 8n &\text{ is even} \\ \text{so } 6m + 8n &\text{ is even} \end{aligned}$$

If $6m + 8n = 75$, then 75 would be even. But 75 is odd (why?). So if $6m + 8n = 75$, 75 would be both even and odd, which is a contradiction.

Let's now write the proof.

Proof. We will prove the proposition by contradiction. Assume, for a contradiction, that m and n are integers that satisfy

$$6m + 8n = 75.$$

Since 6 and 8 are even,

$$75 = 6m + 8n = 2(3m + 4n)$$

is also even. But 75 is odd, so 75 is both even and odd, which is a contradiction. Thus such integers m and n do not exist. □

Generally, a proof by contradiction will follow a similar method to the one above.

Method. To prove a statement P by contradiction, we follow these steps.

1. Assume the opposite of what you want to prove, in other words, assume $\neg P$.
2. Using the assumption $\neg P$, prove something that is clearly false.

4.2 Justification for proof by contradiction

Suppose we want to prove that P is true. Instead, we show that

$$(\neg P) \implies Q \text{ where } Q \text{ is false.}$$

Why is this enough to prove P ? Let's make a truth table to see why.

P	$\neg P$	Q	$(\neg P) \implies Q$	
T	F	T	T	Case I
T	F	F	T	Case II
F	T	T	T	Case III
F	T	F	F	Case IV

Note:

- We can exclude Case IV because we showed that the implication $\neg P \implies Q$ is true.
- We can exclude Case III and Case I because we know Q is false.

Only case II remains possible so P is true!

4.3 Proving implications by contradiction

Example 4.5. Prove by contradiction the proposition: "For integers a and b

$$(a + b \geq 11) \implies [(a \geq 6) \text{ or } (b \geq 6)]."$$

In the example above, we are asked to prove a statement of the form $P \implies Q$ by contradiction. Our general method of proof by contradiction tells us that the first step should be to assume $\neg(P \implies Q)$.

Question 4.6. How do we negate an implication $P \implies Q$?

Solution. Observe that

$$\neg(P \implies Q) \iff (P \wedge \neg Q),$$

as shown by the following truth table.

P	Q	$P \implies Q$	$\neg(P \implies Q)$	$P \wedge \neg Q$
T	T	T	F	F
T	F	F	T	T
F	T	T	F	F
F	F	T	F	F

(the last two columns are the same).

Therefore, to prove $P \implies Q$ by contradiction, we should start by assuming $P \wedge \neg Q$. Then we should use this assumption to prove something clearly false. In other words, we want to show

$$(P \wedge (\neg Q)) \implies R$$

where R is false.

Back to our example:

Proof. Assume, for a contradiction, that

$$\underbrace{(a + b \geq 11)}_P \text{ and } \underbrace{(a \leq 5) \wedge (b \leq 5)}_{\neg Q}.$$

But

$$(a \leq 5) \wedge (b \leq 5) \implies \overbrace{(a + b \leq 10)}^R$$

by the inequality axioms, which contradicts our assumption that $a + b \geq 11$. So

$$(a + b \geq 11) \implies (a \geq 6) \text{ or } (b \geq 6). \quad \square$$

We summarize the method of proof by contradiction for implications.

Method. To prove that $P \implies Q$ by contradiction, we follow these steps.

1. Assume P and $\neg Q$.
2. Using the assumptions P and $\neg Q$, prove something that is clearly false.

4.4 Proof by contrapositive

Definition 4.7. The *contrapositive* of $(P \implies Q)$ is $(\neg Q \implies \neg P)$.

Notice that $P \implies Q$ and its contrapositive $\neg Q \implies \neg P$ are equivalent:

P	Q	$\neg P$	$\neg Q$	$P \implies Q$	$(\neg Q \implies \neg P)$
T	T	F	F	T	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

So to prove $(P \implies Q)$, we can instead prove $(\neg Q \implies \neg P)$.

Example 4.8. If a, b, c are integers with $a > b$, then

$$ac \leq bc \implies c \leq 0.$$

Proof. We will prove the contrapositive of $ac \leq bc \implies c \leq 0$. That is, we will prove that for integers a, b, c with $a > b$, we have $(c > 0 \implies ac > bc)$. This holds by the multiplicative law of inequalities (one of the axioms of inequalities), so we are done. $\square$

5 The induction principle

Goal. We may want to prove that some property holds for all positive integers (or for all integers greater than or equal to some n_0).

Observation 5.1. The positive integers come in a sequence. The integer $n+1$ is the *successor* of the integer n .

Axiom 5.2 (The induction principle). Let $P(n)$ be a statement involving a general positive integer n . Then $P(n)$ is true for all $n \geq 1$ if

- (i) $P(1)$ is true, and
- (ii) $P(k) \implies P(k+1)$ for all positive integers k .

So, to prove $P(n)$ by induction, we have to do *two* things.

- (1) Prove that $P(1)$ is true (base case)
- (2) Prove that $\underbrace{P(k)}_{\text{Inductive hypothesis}} \implies P(k+1)$ for all positive integers k (inductive step)

You should **always** do these two things when using induction. Here is an example.

Proposition 5.3. *For all positive integers n , we have $n \leq n^3$.*

Proof. We will prove this by induction.

- (i) We start by checking the base case ($n = 1$), which is clearly true as $1 \leq 1^3$.
- (ii) We now proceed to the inductive step, so we assume that $k \leq k^3$ for some positive integer k and prove that $(k+1) \leq (k+1)^3$.

To that end, note that

$$k \leq k^3 \implies k+1 \leq k^3+1$$

and

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

Hence, $k \leq k^3 \implies (k+1) \leq (k+1)^3$. So, by induction, we have $n \leq n^3$ for all positive integers n . $\square$

We now summarize the method of proof by induction.

Method. To prove a statement $P(n)$ is true for all positive integers n , we do the following.

1. **Base case:** Prove that $P(1)$ is true.
2. **Inductive hypothesis:** Assume $P(k)$, where k is some positive integer.
3. **Inductive step:** Using the assumption that $P(k)$ is true, prove that $P(k+1)$ is true.

Exercise 5.4. By observing that $n \leq n^3 \iff n^3 - n \geq 0$, can you prove Proposition 5.3 *without* induction?

Exercise 5.5. Prove that for all positive integers n ,

$$n \leq 2^n.$$

5.1 Changing the base case

Suppose we want to prove that the statement $P(n)$ is true for all integers $n \geq n_0$ (where n_0 is some given integer).

To prove $P(n)$ by induction, the method is essentially the same as the one given above, with the only major change being the base case:

- (1) Prove that $P(n_0)$ is true (base case)
- (2) Prove that $P(k) \implies P(k+1)$ for all integers $k \geq n_0$ (inductive step)

However, there is also a less noticeable (but important) change with the inductive step: we should assume that $k \geq n_0$. Sometimes this does not make too much of a difference, but a lot of the time this assumption is crucial!

Remark 5.6. The value of n_0 should be clear by the way the question is phrased. If the question says “for all positive integers”, then $n_0 = 1$; if it says “for all natural numbers” or “for all nonnegative integers”, then $n_0 = 0$; if it says “for all integers $n \geq 7$ ”, then $n_0 = 7$. You should always be careful to use the correct base case in your proof!

Proposition 5.7. For all integers $n \geq 4$

$$n^2 \leq 2^n.$$

Proof. We will proceed by induction.

(i) **Base case** ($n = 4$): This is true because $16 = 4^2 \leq 2^4 = 16$.

(ii) **Inductive hypothesis:** Suppose that $k^2 \leq 2^k$ for some $k \geq 4$.

We want to show that $(k+1)^2 \leq 2^{k+1}$. By the inductive hypothesis, we have $2k^2 \leq 2^{k+1}$. So, we will be done if we can show that $(k+1)^2 \leq 2k^2$ (why?). Notice that $(k+1)^2 \leq 2k^2 \iff 2k+1 \leq k^2$. Since $k \geq 4$, we have $k^2 \geq 4k = 2k+2k \geq 2k+1$. Hence $2k^2 \geq (k+1)^2$ and consequently $(k+1)^2 \leq 2^{k+1}$. Thus, by induction $n^2 \leq 2^n$, for all $n \geq 4$. $\square$

Exercise 5.8. Prove that $n^2 + n \leq 2^n$ for all integers $n \geq 5$.

Example 5.9. Prove that 3 divides $n^3 + 2n$ whenever n is a positive integer.

Proof. We will proceed by induction.

(i) **Base case** ($n = 1$): Clearly 3 divides $1^3 + 2(1)$.

(ii) **Inductive hypothesis:** Suppose that 3 divides $k^3 + 2k$ for some positive integer k . We would like to show that 3 divides $(k+1)^3 + 2(k+1)$.

Note that

$$\begin{aligned} (k+1)^3 + 2(k+1) &= k^3 + 3k^2 + 3k + 1 + 2k + 2 \\ &= (k^3 + 2k) + 3(k^2 + k + 1), \end{aligned}$$

where $3 \mid (k^3 + 2k)$ by the inductive hypothesis and $3 \mid 3(k^2 + k + 1)$. Hence

$$3 \mid \underbrace{(k^3 + 2k) + 3(k^2 + k + 1)}_{=(k+1)^3 + 2(k+1)}$$

as desired. So, by induction, 3 divides $n^3 + 2n$ for all positive integers n . $\square$

5.2 “Definition by induction”/recursion

Example 5.10. The sum of the first n positive integers

$$\underbrace{1 + 2 + \cdots + n}_{\text{definition by induction}}$$

is $\frac{1}{2}n(n+1)$.

Note: This is the same as the proposition

$$\sum_{i=1}^n i = \frac{1}{2}n(n+1).$$

Exercise 5.11. Prove this by induction.

Exercise 5.12. Prove that for all positive integers n

$$\sum_{i=1}^n \frac{1}{i(i+1)} = \frac{n}{n+1}.$$

5.3 Strong induction

Axiom 5.13 (The strong induction principle). Let $P(n)$ be a statement involving a general positive integer n . Then $P(n)$ is true for all $n \geq 1$ if

- (i) $P(1)$ is true, and
- (ii) “[$P(n)$ holds for all positive integers $n \leq k$] $\implies P(k+1)$ ” for all positive integers k .

Usually, the reason to use strong induction is that the inductive step requires more than one of the previous $P(n)$. For example, to prove that $P(k+1)$ holds, one may need to use both $P(k)$ and $P(k-1)$. Often, this means that we need more than one base case. This is because, to prove $P(3)$ using the inductive step, we would need to know that both $P(2)$ and $P(1)$ are true, so we need both $P(1)$ and $P(2)$ as base cases. This will become clearer with some examples.

Method. To prove $P(n)$ by strong induction, we have to do the following:

1. Figure out how many base cases are required. This is usually equal to the number of previous cases that $P(k+1)$ depends on.
2. **Base case(s):** Prove that $P(1), \dots, P(b)$ are true, where b is the number of base cases from Step 1.
3. **Inductive hypothesis:** Assume that $P(n)$ holds for all positive integers $n \leq k$, where k is a positive integer.
4. **Inductive step:** Using the inductive hypothesis, deduce that $P(k+1)$ is true.

Here is an example requiring two base cases.

Example 5.14 (Fibonacci sequence). Define the number u_n , for positive integers n as follows:

$$\begin{aligned} u_1 &= 1 \\ u_2 &= 1 \\ u_{k+1} &= u_{k-1} + u_k \quad \text{for } k \geq 2 \end{aligned}$$

Proposition 5.15 (Binet formula). Define $\alpha = \frac{1+\sqrt{5}}{2}$ (this is the famous golden ratio) and $\beta = \frac{1-\sqrt{5}}{2}$. Then

$$u_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}.$$

Proof. We proceed by strong induction.

(1) **Base cases.** ($n = 1$): Note that $u_1 = 1$ by definition, and

$$\frac{\alpha^1 - \beta^1}{\sqrt{5}} = \frac{1 + \sqrt{5} - (1 - \sqrt{5})}{2\sqrt{5}} = 1$$

So $u_1 = \frac{\alpha^1 - \beta^1}{\sqrt{5}}$.

($n = 2$): $u_2 = 1$, while

$$\frac{\alpha^2 - \beta^2}{\sqrt{5}} = \frac{(\alpha - \beta)(\alpha + \beta)}{\sqrt{5}} = 1 = u_2.$$

(2) **Inductive step.** Suppose the formula

$$u_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}$$

is true for all positive integers $n \leq k$, where $k \geq 2$. We have

$$\begin{aligned} u_{k+1} &= u_{k-1} + u_k && \text{(by definition)} \\ &= (\alpha^{k-1} - \beta^{k-1} + \alpha^k - \beta^k) / \sqrt{5} && \text{(by inductive hypothesis)} \\ &= [\alpha^{k-1}(1 + \alpha) - \beta^{k-1}(1 + \beta)] / \sqrt{5}, \end{aligned}$$

but $1 + \alpha = \alpha^2$ and $1 + \beta = \beta^2$ (check this). So

$$u_{k+1} = [\alpha^{k-1} \cdot \alpha^2 - \beta^{k-1} \cdot \beta^2] / \sqrt{5} = \frac{\alpha^{k+1} - \beta^{k+1}}{\sqrt{5}}$$

as required for our induction proof. Hence $u_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}$ for all positive integers n . $\square$

Question 5.16. Why strong induction? And why did we need two base cases?

The definition of the Fibonacci sequence depends on the previous two steps. In other words, to define u_{k+1} , we need to know the values of both u_k and u_{k-1} . This tells us that assuming $P(k)$ alone is not enough to prove $P(k+1)$: we need strong induction.

The reason for the two base cases is that if we wanted to prove $P(2)$ using the inductive step from the proof above, we would need to use both u_1 and u_0 . This is the problem: u_0 does not exist, since the sequence starts at u_1 ! So the inductive step is **not valid** for $P(2)$, meaning it needs to have its own base case. From $P(3)$ onward, this is not a problem.

Useful tip. To know whether you have enough base cases, ask yourself for which values of k your inductive step works. If there is some value of k for which your inductive step does not make sense, go back and add that value of k as an additional base case. If you're ever in doubt, having more base cases does not make your proof incorrect, so you can always add more.

6 Set theory

6.1 (Informal) definition and basic properties

Definition 6.1. A *set* is a well-defined collection of objects.

Example 6.2.

- $\mathbb{Z}$: set of all integers.
- $\mathbb{N}$: set of all natural numbers (nonnegative integers) $0, 1, 2, 3, \dots$
- $\mathbb{Z}^+$: set of all positive integers $1, 2, 3, \dots$
- $\mathbb{Q}$: set of all rational numbers.
- $\mathbb{R}$: set of all real numbers.
- $\mathbb{C}$: set of all complex numbers.

Notation 6.3. The notation $x \in E$ means “ x is an element of E ” (E is a set).

To denote the proposition $\neg(x \in E)$ we write

$$x \underbrace{\notin}_{\text{does not belong to}} E.$$

Ways of specifying a set:

- (1) Simply listing the elements.

Example 6.4.

$$\begin{aligned} A &= \{1, 7, 3/4\} \\ &= \{7, 1, 3/4\} \quad (\text{order does not matter}) \\ &= \{7, 7, 1, 1, 1, 3/4\} \quad (\text{repeating elements does not change } A) \end{aligned}$$

Example 6.5. $\mathbb{Z}^+ = \{1, 2, 3, \dots\}$.

(2) Using conditional definitions.

Example 6.6. The notation

$$B = \{n \in \mathbb{Z} \mid 0 < n < 6\}$$

is a different way of writing $B = \{1, 2, 3, 4, 5\}$.

(3) Using a constructive definition.

Example 6.7. We have

$$\begin{aligned} C &= \{n^2 \mid n \in \mathbb{Z}\} \\ &= \{0, 1, 4, 9, \dots\} \end{aligned}$$

The rationals can be defined as

$$\mathbb{Q} = \{a/b \mid a \in \mathbb{Z}, b \in \mathbb{Z}, b \neq 0\}.$$

Definition 6.8. The *empty set*, denoted by $\emptyset$, is the unique set with no elements at all.

Example 6.9. $\emptyset = \{x \in \mathbb{R} \mid x^2 + x + 1 = 0\}$

Definition 6.10. Given two sets A and B , we say A is a *subset* of B , denoted

$$A \subseteq B \quad (\text{or } B \supseteq A)$$

when every element of A is also an element of B . That is

$$(x \in A) \implies (x \in B).$$

Remark 6.11. In the book, $A \subset B$ means that A is a *proper* subset of B , in other words, $(A \subseteq B) \wedge (A \neq B)$. Other authors use $A \subset B$ to mean the same as $A \subseteq B$. I therefore avoid using the symbol $\subset$ completely and will stick to the symbol $\subseteq$ to mean “subset” and $\subsetneq$ to mean “proper subset”.

Note that:

- (i) $(x \in A) \iff (\{x\} \subseteq A)$.
- (ii) $(A = B) \iff [(A \subseteq B) \wedge (B \subseteq A)]$.
- (iii) $(P(a) \implies Q(a) \text{ for all } a \in A) \iff \{a \in A \mid P(a)\} \subseteq \{a \in A \mid Q(a)\}$.
- (iv) $(A \subseteq B) \wedge (B \subseteq C) \implies (A \subseteq C)$.
- (v) $\emptyset \subseteq A$ for all sets A .

6.2 Operations on sets

Definition 6.12. 1. The *intersection* of two sets A and B is the set of elements belonging to both A and B

$$A \cap B := \{x \mid x \in A \textbf{ and } x \in B\}.$$

2. We say A and B are *disjoint* if $A \cap B = \emptyset$.

3. The *union* of two sets A and B is the set of elements belonging to A or B

$$A \cup B := \{x \mid x \in A \textbf{ or } x \in B\}.$$

4. The *difference* of two sets A and B is the set of elements belonging to A but not B

$$A \setminus B := \{x \mid x \in A \text{ and } x \notin B\}.$$

Remark 6.13. Often $A - B$ is used in place of $A \setminus B$.

In general the set differences $A \setminus B$ and $B \setminus A$ are not equal, as the following example demonstrates.

Example 6.14. Let $A = \{1, 2, 3\}$, $B = \{1, 2\}$, then

$$A \setminus B = \{3\}$$

and

$$B \setminus A = \emptyset.$$

Here are some basic properties of these operations.

Lemma 6.15. *Let A be a set. Then the following hold.*

1. $A \cap A = A \cup A = A$,
2. $A \cap \emptyset = \emptyset$,
3. $A \cup \emptyset = A$,
4. $A \setminus A = \emptyset$,
5. $A \setminus \emptyset = A$.

Proof. Exercise. □

When proving equalities of sets involving the operations from Definition 6.12, it is often useful to make a truth table. This yields a quick proof of such equalities, but you should be aware that this method only works in situations that are very similar to the example we present next. In general, to prove that two sets A and B are equal, the method that will always work is proving that $A \subseteq B$ and that $B \subseteq A$.

Proposition 6.16. *Given two sets A and B , the sets $A \cap B$, $B \setminus A$, $A \setminus B$ are pairwise disjoint. Moreover $A \cup B = (A \cap B) \cup (A \setminus B) \cup (B \setminus A)$.*

Proof. Consider the truth table

$x \in A$	$x \in B$	$x \in A \cap B$	$x \in A \setminus B$	$x \in B \setminus A$
T	T	T	F	F
T	F	F	T	F
F	T	F	F	T
F	F	F	F	F

and note that each row in the last 3 columns has at most one T. This proves that $A \cap B$, $A \setminus B$, $B \setminus A$ are pairwise disjoint.

Now consider the truth table:

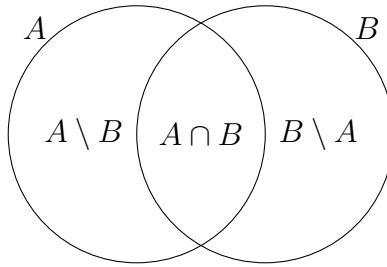
$x \in A$	$x \in B$	$x \in (A \cap B) \cup (A \setminus B) \cup (B \setminus A)$	$x \in (A \cup B)$
T	T	T	T
T	F	T	T
F	T	T	T
F	F	F	F

which proves that

$$A \cup B = (A \cap B) \cup (A \setminus B) \cup (B \setminus A).$$

□

Illustration via Venn diagrams:



Definition 6.17. The *power set* of a set X , denoted $\mathcal{P}(X)$, is the set of all subsets of X . In symbols:

$$A \in \mathcal{P}(X) \iff A \subseteq X.$$

Example 6.18.

- If $X = \{1\}$, $\mathcal{P}(X) = \{\emptyset, \{1\}\}$.
- If $X = \{a, b\}$,

$$\mathcal{P}(X) = \{\emptyset, \underbrace{\{a\}, \{b\}}_{\text{singletons}}, \{a, b\}\}.$$

- If $X = \{1, 2, 3\}$,

$$\mathcal{P}(X) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$

Definition 6.19. Given a fixed *universal set* U and a set $A \in \mathcal{P}(U)$, the *complement* of A , denoted by A^c , is

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

Theorem 6.20. Let U be a universal set and let $A, B, C \in \mathcal{P}(U)$. Then the following hold.

(i) **Associativity:**

$$\begin{aligned} A \cup (B \cup C) &= (A \cup B) \cup C, \\ A \cap (B \cap C) &= (A \cap B) \cap C. \end{aligned}$$

(ii) **Commutativity:** $A \cup B = B \cup A$ and $A \cap B = B \cap A$.

(iii) **Distributivity:**

$$\begin{aligned} A \cup (B \cap C) &= (A \cup B) \cap (A \cup C), \\ A \cap (B \cup C) &= (A \cap B) \cup (A \cap C). \end{aligned}$$

(iv) **De Morgan's laws:**

$$\begin{aligned} (A \cup B)^c &= A^c \cap B^c, \\ (A \cap B)^c &= A^c \cup B^c. \end{aligned}$$

(v) **Complement:** $A \cup A^c = U$, $A \cap A^c = \emptyset$.

(vi) **Double complement:** $(A^c)^c = A$.

We will prove $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, the rest are an exercise.

Proof that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. We could do this using truth tables, like we did before, but this time we use the other method: proving that each set is a subset of the other.

(I) We will first prove that $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$. If $x \in A \cap (B \cup C)$ then $x \in A$ and $x \in (B \cup C)$. Moreover, as $x \in (B \cup C)$ then $x \in B$ or $x \in C$. We consider both cases: if $x \in B$, then $x \in A \cap B$ (since $x \in A$). Similarly, if $x \in C$, then $x \in A \cap C$. Thus $x \in (A \cap B) \cup (A \cap C)$, and so $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

(II) We now prove that $A \cap (B \cup C) \supseteq (A \cap B) \cup (A \cap C)$. Suppose that $x \in (A \cap B) \cup (A \cap C)$, then $x \in A \cap B$ or $x \in A \cap C$. In the first case $x \in A$ and $x \in B$, which implies $x \in B \cup C$. In the second case ($x \in A \cap C$), $x \in A$ and $x \in C$, hence $x \in B \cup C$. Thus, in both cases, $x \in A$ and $x \in B \cup C$ so $x \in A \cap (B \cup C)$. $\square$

Exercise 6.21. Prove the other parts of Theorem 6.20 using both methods (truth tables and double subset proof).

Exercise 6.22. Prove that

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

7 Quantifiers

7.1 Universal statements

Sometimes a predicate $P(a)$ (where a takes values in the set A) is true for some values of a and false for others. On the other hand:

Definition 7.1. If $P(a)$ is true for all values of a in A , we say that $P(a)$ is a *universal statement*. We use the notation

$$\forall a \in A, P(a)$$

($\forall$: “for every”/“for each”/“for all”) to mean $\{a \in A \mid P(a)\} = A$.

Example 7.2. The statement

$$\forall a \in \mathbb{R} \setminus \{0\}, a^2 > 0$$

is equivalent to the statement

$$\{a \in \mathbb{R} \setminus \{0\} \mid a^2 > 0\} = \mathbb{R} \setminus \{0\},$$

and also equivalent to the statement

$$a \in \mathbb{R} \setminus \{0\} \implies a^2 > 0.$$

7.2 Existential statements

Suppose we want to negate the (false) universal statement

$$\forall x \in \mathbb{R}, (x > 3 \implies x > 5).$$

This statement is false because there is an x ($x = 4$) for which $x > 3$ and $x \not> 5$.

Definition 7.3. The notation

$$\exists a \in A: P(a)$$

($\exists$: “there exists”/“for some”/“for at least one”) means

$$\{a \in A \mid P(a)\} \neq \emptyset.$$

The statement above can be read as “there exists an element a in A for which $P(a)$ holds”.

Example 7.4.

- $\exists n \in \mathbb{Z}: n^2 = 9$ is a true statement.
- $\exists n \in \mathbb{Z}: n + 1 = 4.5$ is false.
- $\exists x \in \mathbb{R}: x + 1 = 4.5$ is true.

7.3 Proving statements involving quantifiers

7.3.1 For all statements

Example 7.5. $\forall x \in \mathbb{R}, x^2 \geq 0$.

We already proved this by cases; the idea is to cover **all** possibilities.

Method. To prove a statement of the form: $\forall a \in A, P(a)$, prove the equivalent statement $a \in A \implies P(a)$. In other words:

1. Start with “let $a \in A$ ”.
2. Prove that $P(a)$ holds. You must work with an **arbitrary** element $a \in A$ (in other words, you cannot use any properties of the element a other than the fact that it is an element of the set A).

7.3.2 Existence statements

Method. To prove a statement of the form $\exists a \in A: P(a)$, we just have to find *one* (or more) $a \in A$ such that $P(a)$ holds.

Example 7.6. $\exists x \in \mathbb{R}: x^2 - 2x + 1 = 0$.

Proof. Take $x = 1$, then $x^2 - 2x + 1 = 1^2 - 2 + 1 = 0$. □

7.3.3 Statements involving both quantifiers

A common form for such statements is

$$\forall a \in A, \exists b \in B: P(a, b).$$

To prove such a statement, you should work from the left to the right: every time you see a $\forall a \in A$, you should write “let $a \in A$ ”, and if you see $\exists b \in B$, find an example of an element $b \in B$ for which the remainder of the statement holds.

Example 7.7. Consider the statement “ $\forall$ even integers n , $\exists q \in \mathbb{Z}: n = 2q$ ”. In words: “for every even number n , we can find some (other) number q , such that $n = 2q$ ”.

(Of course, this is the definition of even numbers).

7.4 Disproving statements involving quantifiers

To disprove a statement of the form “ $\forall a \in A, P(a)$ ” we just have to find a counterexample. That is, we prove the statement

$$\exists a \in A: \neg P(a),$$

which is the negation of $\forall a \in A, P(a)$.

Example 7.8. To disprove $(\forall x \in \mathbb{R}, x^2 > 0)$ we just have to note that $0 \in \mathbb{R}$ and $0^2 \not> 0$.

To disprove a statement of the form $\exists a \in A: P(a)$ we again have to prove its negation, which is

$$\neg(\exists a \in A: P(a)) \iff \forall a \in A, \neg P(a).$$

7.5 Statements involving more than one free variable

- $\forall a \in A, \forall b \in B, P(a, b).$

Example 7.9. $\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z} \setminus \{0\}, \frac{a}{b} \in \mathbb{Q}.$

(This follows from the definition of $\mathbb{Q}$.)

- $\exists a \in A: \exists b \in B: P(a, b)$

Example 7.10.

$$\exists m \in \{1, 2, 3\}: \exists n \in \{2, 3, 4\}: \frac{m}{n} = \frac{6}{8}.$$

Proof. $3 \in \{1, 2, 3\}, 4 \in \{2, 3, 4\}$ and $\frac{3}{4} = \frac{6}{8}.$ □

- $\forall a \in A, \exists b \in B: P(a, b)$

Example 7.11. $\forall m \in \mathbb{Z}, \exists n \in \mathbb{Z}: m < n.$

Proof. Let $m \in \mathbb{Z}$. Then $n = m + 1 \in \mathbb{Z}$ and $m < m + 1.$ □

- $\exists b \in B: \forall a \in A, P(a, b).$

Example 7.12. $\exists x \in \mathbb{R}: \forall y \in \mathbb{R}, xy = y.$

Proof. Take $x = 1 \in \mathbb{R}$, then $\forall y \in \mathbb{R}, 1 \cdot y = y.$ □

- $\forall b \in B, \exists a \in A: P(a, b).$

Example 7.13. $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}: y = x^2.$

7.6 The Cartesian product of two sets

Definition 7.14. The *Cartesian product* of two sets X and Y , denoted by $X \times Y$ is the set of all *ordered* pairs (x, y) where $x \in X, y \in Y$.

$$X \times Y = \{(x, y) \mid x \in X, y \in Y\}.$$

Remark 7.15. $(x_1, y_1) = (x_2, y_2)$ if and only if $x_1 = x_2$ and $y_1 = y_2.$

Example 7.16. $A = \{1, 2\}, B = \{a, b, c\}$

$$\begin{aligned} A \times B &= \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}, \\ B \times A &= \{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)\}. \end{aligned}$$

Notice: $A \times B \neq B \times A.$

Remark 7.17. When $X = Y$, we have $X \times Y = X \times X = \underbrace{X^2}_{\text{notation}}.$

Example 7.18. $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ is the usual 2-dimensional space.

7.7 Cartesian products and predicates $P(a, b)$

Example 7.19. Let $x \in \mathbb{R}$, $y \in \mathbb{R}$ and consider the predicate $P(x, y)$: $y = 2x$, and note

$$\{(x, y) \in \mathbb{R}^2 \mid P(x, y)\} = \{(x, y) \in \mathbb{R}^2 \mid y = 2x\} \subseteq \mathbb{R}^2$$

is the line with equation $y = 2x$.

Proposition 7.20. *For all sets A, B, C, D , we have:*

- (i) $A \times (B \cup C) = (A \times B) \cup (A \times C)$,
- (ii) $A \times (B \cap C) = (A \times B) \cap (A \times C)$,
- (iii) $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$,
- (iv) $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$.

Proof of (i).

$$\begin{aligned} (x, y) \in A \times (B \cup C) &\iff [(x \in A) \wedge (y \in B \cup C)] \\ &\iff (x \in A) \wedge ((y \in B) \vee (y \in C)) \\ &\iff [(x \in A) \wedge (y \in B)] \vee [(x \in A) \wedge (y \in C)] \\ &\iff ((x, y) \in A \times B) \vee ((x, y) \in A \times C) \\ &\iff (x, y) \in (A \times B) \cup (A \times C). \end{aligned}$$

□

Exercise 7.21.

- Do the remaining proofs of Proposition 7.20.
- Find an example of A, B, C, D , so that

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

8 Functions

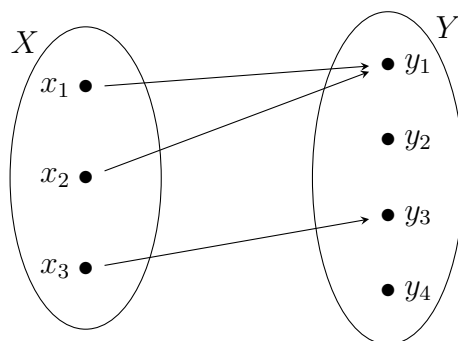
Definition 8.1. Let X and Y be two sets. A *function*, *map*, or *mapping* from X to Y is the assignment of a *unique* element of Y to each element of X . We write

$$f: X \rightarrow Y, \quad x \mapsto \underbrace{f(x)}_{\substack{\text{value of } f \text{ at } x \\ \text{ / image of } x \text{ under } f}}$$

to mean that the element $y = f(x) \in Y$ is assigned to $x \in X$.

We call X the *domain* of f , and we call Y its *codomain*.

8.1 Pictorial representation



Here $f(x_1) = y_1$, $f(x_2) = y_1$, $f(x_3) = y_3$.

Note: Every x in the domain X has an image $f(x)$. On the other hand, elements in the codomain can be the image of one, or more elements of the domain. They can also **not** be the image of any x .

Example 8.2. There are 8 functions from $X = \{a, b, c\}$ to $Y = \{d, e\}$.

x	a	b	c
$f_1(x)$	d	d	d
$f_2(x)$	d	d	e
$f_3(x)$	d	e	d
$f_4(x)$	d	e	e
$f_5(x)$	e	d	d
$f_6(x)$	e	d	e
$f_7(x)$	e	e	d
$f_8(x)$	e	e	e

So here, $f_1(a) = f_1(b) = f_1(c) = d$ while $f_4(a) = d$, $f_4(b) = f_4(c) = e$.

In the example above, the domain and codomain were different sets. That need not be the case.

Example 8.3. Let

$$f: \mathbb{R} \rightarrow \mathbb{R}, \quad x \mapsto 2x.$$

Example 8.4. Let $A = \{a, b\}$, and

$$g: A \rightarrow A.$$

In fact, we can have exactly 4 functions from A to A .

Exercise 8.5. List these 4 functions.

Definition 8.6. Given a set X , the *identity function*

$$\text{id}_X: X \rightarrow X$$

is given by $\text{id}_X(x) = x \ \forall x \in X$.

Important comment. The domain and codomain of a function are *needed* to define it.

Functions with different domain or codomain are different functions even if they have the same ‘formula’.

Notation 8.7. We write

$$\mathbb{R}_{\geq 0} := \{x \in \mathbb{R} \mid x \geq 0\}$$

for the set of nonnegative real numbers.

Example 8.8. Let

$$\begin{aligned} f_1: \mathbb{R} &\rightarrow \mathbb{R}, & x &\mapsto x^2, \\ f_2: \mathbb{R}_{\geq 0} &\rightarrow \mathbb{R}, & x &\mapsto x^2, \\ f_3: \mathbb{R} &\rightarrow \mathbb{R}_{\geq 0}, & x &\mapsto x^2, \\ f_4: \mathbb{R}_{\geq 0} &\rightarrow \mathbb{R}_{\geq 0}, & x &\mapsto x^2. \end{aligned}$$

These 4 functions are different.

Example 8.9. Often, when we are working with functions on the real numbers, we do not specify the domain and codomain.

Consider $f_1(x) = \frac{x^2}{x-1}$.

Here, we have to exclude $x = 1$ from the domain (and think of $f_1: \mathbb{R} \setminus \{1\} \rightarrow \mathbb{R}$) or we have to extend it, by doing something like

$$f_2(x) = \begin{cases} \frac{x^2}{x-1}, & x \neq 1 \\ 3\pi, & x = 1. \end{cases}$$

Example 8.10 (The modulus function). The function

$$f: \mathbb{R} \rightarrow \mathbb{R}, \quad x \mapsto |x|$$

is defined via

$$f(x) = \begin{cases} x, & x \geq 0 \\ -x, & x < 0. \end{cases}$$

8.2 Equality of functions

Definition 8.11. The functions $f: X \rightarrow Y$ and $g: X \rightarrow Y$ are *equal* when $f(x) = g(x) \forall x \in X$.

Note: For this definition, f and g must have the same domain and codomain.

8.3 Restrictions of functions

Definition 8.12. Let $f: X \rightarrow Y$ and let $A \subseteq X$. We can define $g: A \rightarrow Y$ via

$$g(x) = f(x) \quad \forall x \in A.$$

Such a function is called the *restriction* of f to A , and denoted $f|_A$.

8.4 Compositions of functions

Definition 8.13. Let $f: X \rightarrow Y$ and $g: Y \rightarrow Z$. We can define a function $h: X \rightarrow Z$ via $h(x) = g(f(x)) \forall x \in X$. The function h is called the *composition* (or *composite*) of f and g , and is denoted $g \circ f: X \rightarrow Z$, with

$$(g \circ f)(x) = g(f(x)) \quad \forall x \in X.$$

$$g \circ f: \quad X \xrightarrow{f} Y \xrightarrow{g} Z$$

Example 8.14. The function

$$f: \mathbb{R} \rightarrow \mathbb{R}, \quad x \mapsto (2x)^2$$

satisfies $f = g \circ h$ where

$$g: \mathbb{R} \rightarrow \mathbb{R}, \quad x \mapsto x^2$$

and

$$h: \mathbb{R} \rightarrow \mathbb{R}, \quad x \mapsto 2x.$$

Proof. $(g \circ h)(x) = g(h(x)) = g(2x) = (2x)^2 = f(x) \forall x \in \mathbb{R}.$ □

Comment. Notice that $(h \circ g)(x) = 2x^2$, so that $h \circ g \neq g \circ h$.

Proposition 8.15. Let $f: X \rightarrow Y$, $g: Y \rightarrow Z$ and $h: Z \rightarrow W$ be functions. Then

$$(i) \quad (h \circ g) \circ f = h \circ (g \circ f): X \rightarrow W \quad (\text{associativity}).$$

$$(ii) \quad f \circ \text{id}_X = f = \text{id}_Y \circ f: X \rightarrow Y.$$

Proof. (i) We have

$$\begin{aligned} ((h \circ g) \circ f)(x) &= (h \circ g)(f(x)) \\ &= h(g(f(x))) \quad \forall x \in X. \end{aligned}$$

Similarly

$$\begin{aligned} (h \circ (g \circ f))(x) &= h((g \circ f)(x)) \\ &= h(g(f(x))) \quad \forall x \in X. \end{aligned}$$

Therefore $h \circ (g \circ f) = (h \circ g) \circ f$.

(ii) Exercise. □

8.5 Sequences

Definition 8.16. A function $f: \mathbb{Z}^+ \rightarrow A$ is called a *sequence* (in the set A).

Example 8.17.

- $f: \mathbb{Z}^+ \rightarrow \mathbb{Z}^+, n \mapsto n^2$,
- $f: \mathbb{Z}^+ \rightarrow \mathbb{R}, n \mapsto \frac{n}{n+1}$,
- The Fibonacci sequence,
- $f: \mathbb{Z}^+ \rightarrow \mathbb{R}, n \mapsto \sum_{i=1}^n i$.

Definition 8.18. Let $f: \mathbb{Z}^+ \rightarrow \mathbb{R}$ be a sequence. We say the sequence is *null*, written $\lim_{n \rightarrow \infty} f(n) = 0$, when

$$\forall \varepsilon \in \mathbb{R}^+, \exists N \in \mathbb{Z}^+ \text{ such that } \forall n \in \mathbb{Z}^+ (n \geq N \implies |f(n)| < \varepsilon).$$

One way to interpret this: for any choice of positive real number ε , you can find a positive integer N (that can depend on ε) so that $|f(N)| < \varepsilon$, $|f(N+1)| < \varepsilon$, $|f(N+2)| < \varepsilon$, and so on. Since this is true for any $\varepsilon > 0$ (as small as we like), we can think of the sequence as converging to 0.

Example 8.19. Prove that $\lim_{n \rightarrow \infty} \frac{1}{n} = 0$.

Proof. We would like to prove that

$$\forall \varepsilon \in \mathbb{R}^+, \exists N \in \mathbb{Z}^+ \text{ such that } \forall n \in \mathbb{Z}^+ (n \geq N \implies \left| \frac{1}{n} \right| < \varepsilon).$$

To that end, let $\varepsilon > 0$, and choose a positive integer N with $N > \frac{1}{\varepsilon}$, so that $\frac{1}{N} < \varepsilon$. Then, for all $n \geq N$, we have $\left| \frac{1}{n} \right| = \frac{1}{n} \leq \frac{1}{N} < \varepsilon$, so we are done. $\square$

8.6 The image of a function

Definition 8.20. Let $f: X \rightarrow Y$ be a function. The *image* of f , denoted $\text{Im}(f)$ is defined by

$$\text{Im}(f) := \{f(x) \mid x \in X\}.$$

Thus, $\text{Im}(f) \subseteq Y$ consists of those elements of Y that can be reached from X . In other words,

$$[(y \in \text{Im}(f)) \iff (\exists x \in X: f(x) = y)].$$

8.7 The graph of a function

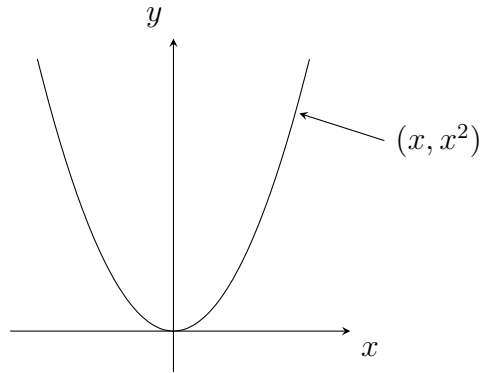
Definition 8.21. Let $f: X \rightarrow Y$ be a function. The *graph* of f , denoted by G_f is defined by

$$G_f := \{(x, y) \in X \times Y \mid y = f(x)\}.$$

Example 8.22.

$$f: \mathbb{R} \rightarrow \mathbb{R}, \quad x \mapsto x^2$$

$$G_f = \{(x, x^2) \mid x \in \mathbb{R}\}$$



9 Types of functions: injections, surjections, and bijections

Definition 9.1. Let $f: X \rightarrow Y$ be a function. We say that f is an *injection* (or a *one-to-one function*) if

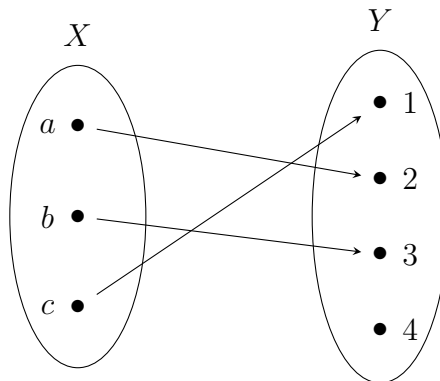
$$\forall x_1, x_2 \in X, x_1 \neq x_2 \implies f(x_1) \neq f(x_2)$$

or equivalently, if

$$\forall x_1, x_2 \in X, f(x_1) = f(x_2) \implies x_1 = x_2.$$

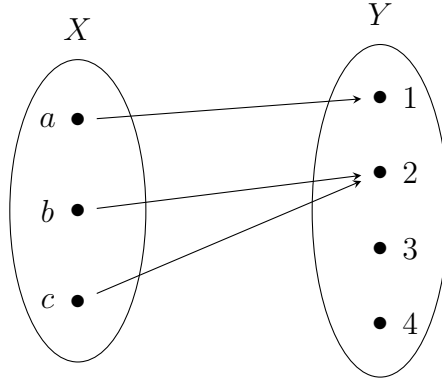
Example 9.2.

- $f: X \rightarrow Y$ given by



is an injection.

- On the other hand:



is not an injection because $f(b) = f(c)$ and $b \neq c$.

Definition 9.3. Let $f: X \rightarrow Y$ be a function. We say that f is a *surjection* (or an *onto function*) if

$$\forall y \in Y, \exists x \in X \text{ such that } f(x) = y.$$

In a sense, this says that we can ‘reach’ all elements of Y .

The two examples above did **NOT** depict surjective functions because in each case there was no x , such that $f(x) = 4$.

Definition 9.4. If $f: X \rightarrow Y$ is both injective and surjective, we say it is a *bijection*.

Definition 9.5. Given a function $f: X \rightarrow Y$, a *pre-image* of $y \in Y$ is an element $x \in X$, such that $f(x) = y$.

Remark 9.6. We can always modify a function $f_1: X \rightarrow Y$ so it is surjective by replacing the codomain Y with the image of f_1 , i.e. by considering $f_2: X \rightarrow \text{Im}(f_1)$, with $f_2(x) = f_1(x) \forall x \in X$.

Example 9.7. Determine if the function

$$f: \mathbb{R} \rightarrow \mathbb{R}, \quad x \mapsto 2x + 3$$

is an injection, bijection, surjection.

Solution. First, let us determine whether f is injective. Consider $x_1, x_2 \in \mathbb{R}$ with $f(x_1) = f(x_2)$. Then

$$(2x_1 + 3 = 2x_2 + 3) \iff (2x_1 = 2x_2) \iff (x_1 = x_2).$$

So we have shown that $f(x_1) = f(x_2) \implies x_1 = x_2$, so f is injective.

Second, let us determine whether f is surjective. Let $y \in \mathbb{R}$. We would like to determine whether there exists $x \in \mathbb{R}$ with $f(x) = y$. But

$$2x + 3 = y \iff x = \frac{y - 3}{2},$$

and $\frac{y-3}{2} \in \mathbb{R}$, so $\forall y \in \mathbb{R}, \exists x \in \mathbb{R}: 2x + 3 = y$. Thus f is surjective. As f is both injective and surjective, it is a bijection.

More efficient solution. Let y be an element of the codomain $\mathbb{R}$. Then,

$$\begin{aligned} x \text{ is a pre-image of } y &\iff y = f(x) = 2x + 3 \\ &\iff x = \frac{y - 3}{2}. \end{aligned}$$

This shows that each $y \in \mathbb{R}$ has exactly one pre-image in $\mathbb{R}$, namely

$$x = \frac{y - 3}{2},$$

so f is a bijection.

Exercise 9.8. Consider

$$f: \mathbb{R} \rightarrow \mathbb{R}, \quad x \mapsto x^2.$$

Determine if f is one-to-one and if f is onto.

Repeat this exercise with

$$(1) \ f: \mathbb{R} \rightarrow \mathbb{R}_{\geq 0}, \ x \mapsto x^2,$$

$$(2) \ f: \mathbb{R} \rightarrow \mathbb{R}, \ x \mapsto x^3 + 1.$$

Example 9.9.

$$f: \mathbb{R} \rightarrow \mathbb{R}, \quad x \mapsto 4x^2 - 4x + 2$$

Determine if f is one-to-one and if f is onto.

Solution. (1) Injectivity. Let $x_1, x_2 \in \mathbb{R}$ be such that $f(x_1) = f(x_2)$. That is

$$\begin{aligned} (4x_1^2 - 4x_1 + 2 = 4x_2^2 - 4x_2 + 2) &\iff (x_1^2 - x_1 = x_2^2 - x_2) \\ &\iff (x_1 - x_2)(x_1 + x_2) - (x_1 - x_2) = 0 \\ &\iff (x_1 - x_2)(x_1 + x_2 - 1) = 0 \\ &\implies (x_1 = x_2) \vee (x_1 = -x_2 + 1). \end{aligned}$$

In particular, taking $x_1 = 1$ and $x_2 = 0$ shows that f is *not* injective, because $f(1) = f(0) = 2$ and $1 \neq 0$.

(2) Surjectivity. Notice that

$$\begin{aligned} 4x^2 - 4x + 2 &= 4x^2 - 4x + 1 + 1 \\ &= (2x - 1)^2 + 1 \\ &\geq 1. \end{aligned}$$

Thus $y = 0$ does not have a pre-image. So f is not surjective.

9.1 Bijections and inverses

Definition 9.10. A function $f: X \rightarrow Y$ is *invertible* if there is a function $g: Y \rightarrow X$ such that

$$f(x) = y \iff x = g(y) \quad \forall x \in X, y \in Y.$$

g is called the *inverse* of f .

Example 9.11. The function $f: \mathbb{R} \rightarrow \mathbb{R}$, given by $f(x) = 2x + 3$ is invertible because $2x + 3 = y \iff x = \frac{y-3}{2} \quad \forall x, y \in \mathbb{R}$. Here, $g(y) = \frac{y-3}{2}$.

Theorem 9.12. A function $f: X \rightarrow Y$ is invertible if and only if it is a bijection. Moreover, if f is invertible, its inverse function is unique.

Proof. (I) Proof that ‘ f is invertible $\implies f$ is bijective’. Suppose f is invertible, then there is a function $g: Y \rightarrow X$ such that $y = f(x) \iff x = g(y) \quad \forall x \in X, y \in Y$.

(a) We will now show that f is injective. To that end, let $x_1, x_2 \in X$ be such that $f(x_1) = f(x_2)$. Then $x_1 = g(f(x_1)) = g(f(x_2)) = x_2$, so $x_1 = x_2$ and f is *injective*.

(b) Now, we will show that f is surjective. Let y be any element of Y , and set $x = g(y)$. Then $f(x) = y$. So we have shown that $\forall y \in Y, \exists x \in X: f(x) = y$, i.e., *surjectivity*.

By (a) and (b), f is bijective.

(II) Proof that ‘ f is bijective $\implies f$ is invertible’. Suppose f is bijective and let $y \in Y$ be any element of Y . By bijectivity of f , there exists *one unique* element $x \in X$ such that $f(x) = y$. We define $g: Y \rightarrow X$ by letting $g(y)$ be this unique element x . Since x is unique, g is a well-defined function. By construction, we have

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

so f is invertible and g is its inverse.

(III) Proof that ‘ f is invertible $\implies$ its inverse is unique’. Suppose $g_1, g_2: Y \rightarrow X$ are both inverses of $f: X \rightarrow Y$, and suppose, for a contradiction, that $g_1 \neq g_2$. Then there is at least one element $y \in Y$ such that $g_1(y) \neq g_2(y)$. Let $x_1 = g_1(y)$ and $x_2 = g_2(y)$. Then

$$\begin{aligned} x_1 = g_1(y) &\iff f(x_1) = y \\ \text{and } x_2 = g_2(y) &\iff f(x_2) = y \end{aligned}$$

so that $f(x_1) = f(x_2)$. But f is a bijection, hence one-to-one, so

$$f(x_1) = f(x_2) \implies x_1 = x_2 \implies g_1(y) = g_2(y)$$

contradicting $g_1(y) \neq g_2(y)$. Hence $g_1 = g_2$. □

Proposition 9.13. $f: X \rightarrow Y$ and $g: Y \rightarrow X$ are inverses of each other if and only if

$$g \circ f = \text{id}_X \text{ and } f \circ g = \text{id}_Y.$$

Proof. If f and g are inverses of each other, then

$$y = f(x) \iff x = g(y) \quad \forall x \in X, \forall y \in Y.$$

For any $x \in X$, let $y = f(x)$, then $g(y) = g(f(x)) = x$, i.e. $g \circ f = \text{id}_X$.

Similarly, for any $y \in Y$, let $x = g(y)$ so

$$f(x) = f(g(y)) = y$$

so $f \circ g = \text{id}_Y$. □

10 Counting

10.1 Cardinality of finite sets

When we “count” the elements of a finite set, we are effectively constructing a bijection from the set

$$[n] = \{1, 2, \dots, n\} = \{i \in \mathbb{Z} \mid 1 \leq i \leq n\}$$

to the set being counted.

Definition 10.1. Given a set X , if there is a bijection $f: [n] \rightarrow X$ then we say that the *cardinality* of X (the number of elements in X) is n . We write

$$|X| = n.$$

Example 10.2. Let $X = \{7, 8, 9, 10, 11\}$.

Then $|X| = 5$ because $\exists f: [5] \rightarrow X$, where f is a bijection. In particular, we may choose

$$f(1) = 7, \quad f(2) = 8, \quad f(3) = 9, \quad f(4) = 10, \quad f(5) = 11.$$

Of course, there are many other bijections between $[5]$ and X . Are there bijections between $[m]$ and X with $m \neq 5$? If there were, we would be in trouble, because X would have two different cardinalities.

Proposition 10.3. Suppose $f: [m] \rightarrow X$ and $g: [n] \rightarrow X$ are both bijections. Then $m = n$.

Strategy. Since g is a bijection, g^{-1} is a bijection ($g^{-1}: X \rightarrow [n]$). So $g^{-1} \circ f: [m] \rightarrow [n]$ is a bijection (why?). So we would be done if we can prove that

$$(\text{having a bijection } h: [m] \rightarrow [n]) \implies (m = n). \quad (*)$$

We can prove $(*)$ by showing:

$$(h: [m] \rightarrow [n] \text{ is an injection}) \implies (m \leq n). \quad (**)$$

In particular, to prove $(*)$ using $(**)$ we observe that:

$$\begin{aligned} h \text{ is a bijection} &\implies h \text{ is an injection} \implies m \leq n \\ h \text{ is a bijection} &\implies h^{-1} \text{ is a bijection} \implies h^{-1} \text{ is an injection} \\ &\quad \text{with } h^{-1}: [n] \rightarrow [m] \\ &\implies n \leq m \end{aligned}$$

We would then have $(n \leq m) \wedge (m \leq n) \implies (m = n)$ so we’d be done. So now the whole proof would work provided $(**)$ holds.

Lemma 10.4 (the Pigeonhole Principle). *If there is an injection $[m] \rightarrow [n]$ then $m \leq n$.*

We will prove this lemma shortly. For now, let us assume it is true, and prove the Proposition.

Proof of Proposition 10.3. Since $f: [m] \rightarrow X$ and $g: [n] \rightarrow X$ are bijections, they are invertible and their inverses $f^{-1}: X \rightarrow [m]$ and $g^{-1}: X \rightarrow [n]$ are also bijections.

Thus $g^{-1} \circ f: [m] \rightarrow [n]$ is a bijection, hence an injection, so $m \leq n$ by the Pigeonhole Principle. Similarly, $f^{-1} \circ g: [n] \rightarrow [m]$ is a bijection, hence an injection, so $n \leq m$. Together, $n \leq m$ and $m \leq n$ yield $m = n$. $\square$

Now, let us go back and prove the Pigeonhole Principle.

Proof of the Pigeonhole Principle. We'd like to prove that if $f: [m] \rightarrow [n]$ is injective then $m \leq n$. We will do this by induction on n .

Base case ($n = 1$): Consider $f: [m] \rightarrow [1]$ injective and note that we must then have $f(i) = 1$ for all $i \in [m]$. But injectivity requires $f(i) = f(j) \implies i = j$, so $[m]$ has at most one element, i.e. $m \leq 1 = n$.

Inductive step: Here we *assume* that

$$\underbrace{\forall m (\text{if there is an injection } f_1: [m] \rightarrow [k], \text{ then } m \leq k)}_{P(k)}$$

and we'd like to prove

$$\underbrace{\forall m (\text{if there is an injection } f: [m] \rightarrow [k+1], \text{ then } m \leq k+1)}_{P(k+1)}$$

So we start by assuming that

$$f: \underbrace{[m]}_{\{1, 2, \dots, m\}} \rightarrow \underbrace{[k+1]}_{\{1, \dots, k+1\}}$$

is an injection.

We consider two cases:

- (1) $f(i) \leq k \ \forall i \in [m]$
- (2) $\exists i_0 \in [m]$ such that $f(i_0) = k+1$.

These cases are mutually exclusive, and exhaustive, so if we prove it in each case, we're done.

Case 1: If $f(i) \leq k \ \forall i \in [m]$, we can define $f_1: [m] \rightarrow [k]$ via $f_1(i) = f(i) \ \forall i \in [m]$. Since f is injective, f_1 is also injective (why?). So by the inductive hypothesis $m \leq k < k+1$. So we are done.

Case 2: Suppose $f(i_0) = k+1$ for some $i_0 \in [m]$. Define a new function $g: [m-1] \rightarrow [m]$ by

$$g(i) = \begin{cases} i & \text{when } i < i_0 \\ i+1 & \text{when } i \geq i_0 \end{cases}$$

and notice that g is injective (why?).

Now, let $f_1 = f \circ g: [m-1] \rightarrow [k]$ and notice that f_1 is injective as it is the composition of two injections (proving this is a homework problem). So, by the inductive hypothesis, we have $m-1 \leq k$, and so $m \leq k+1$.

So by induction, we are done. $\square$

Corollary 10.5. *Let X and Y be finite, non-empty sets. If there is an injection $f: X \rightarrow Y$ then $|X| \leq |Y|$.*

Proof. Exercise. □

Example 10.6. If we have a number of pigeons and we place each pigeon in a *separate* pigeonhole, then

$$\text{number of pigeons} \leq \text{number of holes}.$$

Contrapositive: If $|X| > |Y|$, there is *no* injection $f: X \rightarrow Y$. Thus, if $|X| > |Y|$ and $f: X \rightarrow Y$ is a function, then $\exists x_1, x_2$ with $x_1 \neq x_2$ such that $f(x_1) = f(x_2)$.

Example 10.7. If we have more pigeons than pigeonholes, at least two pigeons must share a pigeonhole.

Example 10.8. If you have a drawer with 10 red and 10 blue socks (unpaired), and you are pulling socks from the drawer without looking, what is the minimum number of socks you must draw to guarantee a pair of the same color?

Answer. Three, by the pigeonhole principle. Take $X = \{\text{selected socks}\}$, $Y = \{\text{red, blue}\}$, and let $f: X \rightarrow Y$ send each sock to its color. Then $|Y| = 2$, and we need $|X| \geq 3$ so that we are sure $\exists x_1, x_2: f(x_1) = f(x_2)$ while $x_1 \neq x_2$.

10.2 Some consequences of the pigeonhole principle

Definition 10.9. Given a set X , if $|X| = n$ for a non-negative integer n , then we say X is *finite*. Otherwise, we say X is *infinite*.

Proposition 10.10. *Suppose $f: X \rightarrow [n]$ is an injection. Then X is finite and $|X| \leq n$.*

Proof. Exercise. □

Proposition 10.11. *Suppose $X \subseteq Y$, where Y is a finite set. Then X is also finite and $|X| \leq |Y|$.*

Proof. This is a simple corollary of the previous proposition. Indeed, let $n = |Y|$ so there is a bijection $f: [n] \rightarrow Y$. Let $i: X \rightarrow Y$ be given by $i(x) = x$, and note that i is an injection. Thus $f^{-1} \circ i: X \rightarrow [n]$ is an injection, so by the previous proposition X is finite and $|X| \leq n$. □

Theorem 10.12. *Let X, Y be non-empty finite sets with $|X| < |Y|$ and let $f: X \rightarrow Y$ be a function. Then f is not surjective.*

Theorem 10.13. *Let X and Y be non-empty finite sets with $|X| = |Y|$ and let $f: X \rightarrow Y$ be a function. Then f is an injection if and only if it is surjective.*

The proofs are exercises left to the students.

10.3 Counting principles

Theorem 10.14 (addition principle). *Suppose X and Y are finite sets with $X \cap Y = \emptyset$. Then $X \cup Y$ is finite and $|X \cup Y| = |X| + |Y|$.*

Proof. We will show that $|X| + |Y| = |X \cup Y|$ which implies $X \cup Y$ is finite. Let $|X| = n$, $|Y| = m$. If $X = \emptyset$, then $n = 0$ and $X \cup Y = Y$, and so $|X \cup Y| = |Y| = m + n$. Similarly, the conclusion holds if $m = 0$.

Let's consider now the case $n \neq 0$ and $m \neq 0$. Note that there are bijections

$$\begin{aligned} f: [n] &\rightarrow X \\ g: [m] &\rightarrow Y \end{aligned}$$

and define $h: [n + m] \rightarrow X \cup Y$ via

$$h(i) = \begin{cases} f(i) & 1 \leq i \leq n \\ g(i - n) & n + 1 \leq i \leq m + n \end{cases}$$

and note that h is bijective (why?). So $|X \cup Y| = m + n$. □

Corollary 10.15. *If $X_1, \dots, X_n$ are pairwise disjoint finite sets then*

$$|X_1 \cup X_2 \cup \dots \cup X_n| = \sum_{i=1}^n |X_i|.$$

Proof. By induction (exercise). □

Theorem 10.16 (The multiplication principle). *Let X, Y be finite sets. Suppose $|X| = n$, $|Y| = m$, then $|X \times Y| = mn$.*

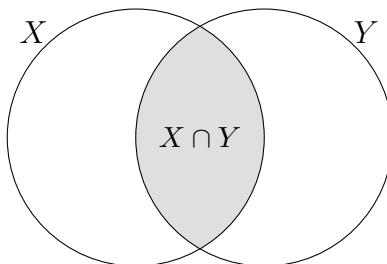
Proof. Exercise. □

10.4 The inclusion-exclusion principle

10.4.1 The case of two sets X and Y

Theorem 10.17. *Let X and Y be finite sets, then*

$$|X \cup Y| = |X| + |Y| - |X \cap Y|.$$



Proof. Recall that $X \cup Y = (X \setminus Y) \cup (X \cap Y) \cup (Y \setminus X)$ and that $X \setminus Y$, $Y \setminus X$, $X \cap Y$ are pairwise disjoint.

So by the addition principle

$$|X \cup Y| = |X \setminus Y| + |Y \setminus X| + |X \cap Y|. \quad \textcircled{1}$$

However $X = (X \setminus Y) \cup (X \cap Y)$ so

$$|X| = |X \setminus Y| + |X \cap Y| \quad \textcircled{2}$$

and similarly

$$|Y| = |Y \setminus X| + |X \cap Y|. \quad \textcircled{3}$$

Combining ①, ②, ③, we obtain

$$|X \cup Y| = |X| + |Y| - |X \cap Y|. \quad \square$$

10.4.2 General inclusion-exclusion principle

Theorem 10.18. Let $A_1, \dots, A_n$ be finite sets, and for $I = \{i_1, i_2, \dots, i_r\} \subseteq [n]$, define

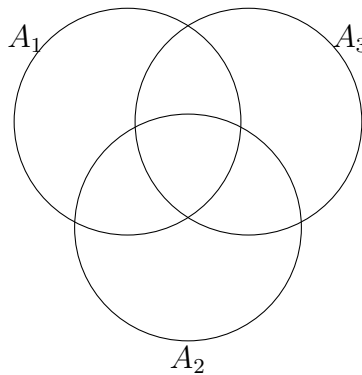
$$A_I = \bigcap_{i \in I} A_i = A_{i_1} \cap A_{i_2} \cdots \cap A_{i_r},$$

then

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{I \subseteq [n], I \neq \emptyset} (-1)^{|I|-1} |A_I|.$$

So for example,

$$\begin{aligned} |A_1 \cup A_2 \cup A_3| &= |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| \\ &\quad - |A_2 \cap A_3| - |A_1 \cap A_3| + |A_1 \cap A_2 \cap A_3| \end{aligned}$$



Example 10.19. Suppose we have 144 tiles, each of which is either triangular or square, either red or blue, and either wooden or plastic. Suppose there are

- 68 wooden tiles

- 69 red tiles
- 75 triangular tiles

and

- 36 red wooden tiles
- 40 triangular wooden tiles
- 38 red triangular tiles

and 23 red wooden triangular tiles. How many blue plastic square tiles are there?

Solution. Let

$$\begin{aligned} A_1 &= \{\text{blue tiles}\} \\ A_2 &= \{\text{plastic tiles}\} \\ A_3 &= \{\text{square tiles}\} \end{aligned}$$

We want $|A_1 \cap A_2 \cap A_3|$, which we will compute using the inclusion-exclusion principle. First, we observe that $(A_1 \cap A_2 \cap A_3)^c = A_1^c \cup A_2^c \cup A_3^c$, so now, we want

$$\begin{aligned} |A_1^c \cup A_2^c \cup A_3^c| &= \underbrace{|A_1^c|}_{69} + \underbrace{|A_2^c|}_{68} + \underbrace{|A_3^c|}_{75} - \underbrace{|A_1^c \cap A_2^c|}_{36} - \underbrace{|A_1^c \cap A_3^c|}_{38} \\ &\quad - \underbrace{|A_2^c \cap A_3^c|}_{40} + \underbrace{|A_1^c \cap A_2^c \cap A_3^c|}_{23} \\ &= 121. \end{aligned}$$

Therefore

$$|A_1 \cap A_2 \cap A_3| = 144 - |A_1^c \cup A_2^c \cup A_3^c| = 144 - 121 = 23.$$

So we have 23 blue plastic square tiles.

11 Counting sets of functions

Goal. Given two sets X and Y with $|X| = m$ and $|Y| = n$, we want to know how many different functions $X \rightarrow Y$ there are.

Example 11.1. $X = \{1, 2\}$, $Y = \{a, b, c\}$ we have 3^2 possible functions $f: X \rightarrow Y$ (why?)

Definition 11.2. Given two sets X and Y , the set of functions from X to Y is denoted

$$\mathcal{F}(X, Y).$$

Proposition 11.3. *Let X and Y be finite sets with $|X| = m$, $|Y| = n$, then the number of functions $X \rightarrow Y$ is n^m .*

Proof. By induction on m (exercise).

(The idea is that for each $x \in X$ there are n possibilities for $f(x)$ among the elements of Y . As there are m elements of X , the total number of possibilities is $n \times n \times \cdots \times n = n^m$.) $\square$

Now that we know the number of functions in $\mathcal{F}(X, Y)$, what about the number of injections, bijections, or surjections?

Proposition 11.4. *Let X and Y be non-empty sets with $|X| = m$, $|Y| = n$, then the number of injections in $\mathcal{F}(X, Y)$ (the set of injections is denoted $\text{Inj}(X, Y)$) is*

$$\underbrace{n(n-1) \cdots (n-m+1)}_{\text{called falling factorial}}.$$

Notice that

$$(n)_m := n(n-1) \cdots (n-m+1) = \begin{cases} n! & \text{when } m = n \\ 0 & \text{when } m > n \\ \frac{n!}{(n-m)!} & \text{when } m \leq n. \end{cases}$$

Proof of Proposition 11.4. Again, by induction on m (exercise). $\square$

Definition 11.5. Given a set X , a bijection $X \rightarrow X$ is called a *permutation* of X .

Corollary 11.6. *Given a set X , $|X| = n > 0$, the number of permutations of X is $n!$.*

Proof. Every injection between two finite sets of equal cardinality is a bijection, by Theorem 10.13. So we can apply Proposition 11.4 with $Y = X$ and obtain that the number of permutations is $(n)_n = n!$. $\square$

11.1 Counting sets of subsets

Recall $\mathcal{P}(X) = \{A \mid A \subseteq X\}$.

Proposition 11.7. *If X is a finite set, then*

$$|\mathcal{P}(X)| = 2^{|X|}.$$

Idea (of proof). Each $x \in X$ either belongs or does not belong to a given subset of X (2 possibilities for each x). There are $|X|$ elements of X , so $2 \times 2 \times \cdots \times 2 = 2^{|X|}$ subsets.

Proof. Exercise. $\square$

Definition 11.8. Given a set X and a non-negative integer r , we denote

$$\mathcal{P}_r(X) = \{A \mid A \subseteq X, |A| = r\}.$$

Example 11.9. If $X = \{1, 2, 3\}$, then

$$\begin{aligned}\mathcal{P}_0(X) &= \{\emptyset\} \\ \mathcal{P}_1(X) &= \{\{1\}, \{2\}, \{3\}\} \\ \mathcal{P}_2(X) &= \{\{1, 2\}, \{1, 3\}, \{2, 3\}\} \\ \mathcal{P}_3(X) &= \{\{1, 2, 3\}\} = \{X\}. \\ \mathcal{P}_r(X) &= \emptyset, \quad r \geq 4.\end{aligned}$$

Definition 11.10. We define the *binomial coefficient*

$$\binom{n}{r} := |\mathcal{P}_r(X)| \quad \text{where } |X| = n.$$

Example 11.11. From our previous example

$$\begin{aligned}\binom{3}{0} &= 1, & \binom{3}{1} &= 3, & \binom{3}{2} &= 3, & \binom{3}{3} &= 1, \\ \binom{3}{r} &= 0 \text{ when } r \geq 4.\end{aligned}$$

Proposition 11.12. When n and r are non-negative integers

- (i) $\binom{n}{r} = 0$ if $r > n$
- (ii) $\binom{n}{0} = 1$, $\binom{n}{1} = n$, $\binom{n}{n} = 1$
- (iii) $\binom{n}{r} = \binom{n}{n-r}$ when $0 \leq r \leq n$

Proof of (iii). There is a bijection

$$\mathcal{P}_r(X) \rightarrow \mathcal{P}_{n-r}(X), \quad A \mapsto A^c = X \setminus A.$$

So

$$|\mathcal{P}_r(X)| = |\mathcal{P}_{n-r}(X)|$$

and

$$\binom{n}{r} = \binom{n}{n-r}.$$

□

11.2 Evaluating binomial coefficients

Proposition 11.13. Let n, r be integers such that $1 \leq r \leq n$, then

$$\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}.$$

Visualization: Pascal's triangle

	$r = 0$	$r = 1$	$r = 2$	$\cdots$	
$n = 0$	$\binom{0}{0}$ 1				
$n = 1$	$\binom{1}{0}$ 1	1	$\binom{1}{1}$		
$n = 2$	$\binom{2}{0}$ 1	2	1		
$n = 3$	1	3	3	1	
$n = 4$	1	4	6	4	1
	$\vdots$	$\binom{4}{2} = \binom{3}{1} + \binom{3}{2}$		$\ddots$	

A more efficient way to compute binomial coefficients is the following.

Theorem 11.14.

$$\binom{n}{r} = \frac{n!}{r!(n-r)!} \quad \text{when } 0 \leq r \leq n$$

Theorem 11.15 (The Binomial Theorem). *For all $a, b \in \mathbb{R}$ and $n \in \mathbb{N}$,*

$$\begin{aligned} (a+b)^n &= \sum_{i=0}^n \binom{n}{i} a^{n-i} b^i \\ &= a^n + \cdots + \binom{n}{i} a^{n-i} b^i + \cdots + b^n \end{aligned}$$

Example 11.16.

$$\begin{aligned} \bullet \quad (a+b)^2 &= \binom{2}{0} a^2 b^0 + \binom{2}{1} a^1 b^1 + \binom{2}{2} a^0 b^2 \\ &= a^2 + 2ab + b^2 \\ \bullet \quad (a+b)^3 &= \binom{3}{0} a^3 b^0 + \binom{3}{1} a^2 b^1 + \binom{3}{2} a^1 b^2 + \binom{3}{3} a^0 b^3 \\ &= a^3 + 3a^2 b + 3ab^2 + b^3 \end{aligned}$$

Proof of Binomial theorem. By induction (exercise). □

Corollary 11.17.

$$\sum_{i=0}^n \binom{n}{i} = 2^n$$

Proof. Set $a = b = 1$ in binomial theorem. □

12 The division theorem

Theorem 12.1. For all $a, b \in \mathbb{Z}$ with $b > 0$, there exist unique $q, r \in \mathbb{Z}$ with $0 \leq r < b$ and

$$a = b \underbrace{q}_{\text{quotient}} + \underbrace{r}_{\text{remainder}}.$$

Proof. (1) **Existence:** The case $b = 1$ is trivial as $a = 1 \cdot \overset{b}{1} \cdot \overset{q}{a} + \overset{r}{0}$. So consider $b > 1$ and let

$$A = \{a - bq \mid q \in \mathbb{Z}, a - bq \geq 0\}.$$

Note that $A \neq \emptyset$ because

$$\begin{aligned} &\text{if } a \geq 0, \quad a - 0 \cdot b \in A \\ &\text{if } a < 0, \quad a - ab = \underbrace{a}_{<0} \underbrace{(1-b)}_{<0} \in A. \end{aligned}$$

So A is a non-empty set of non-negative integers, and it therefore has a minimum element r , with

$$r = a - bq \quad \text{for some } q \in \mathbb{Z}.$$

So

$$a = bq + r.$$

To see that $r < b$, suppose, for a contradiction, that $r \geq b$. Then $m = r - b$ satisfies $0 \leq m < r$ and $m = a - (q+1)b$, so $m \in A$, contradicting the minimality of r .

(2) **Uniqueness:** Suppose

$$a = q_1 b + r_1 = q_2 b + r_2$$

with $0 \leq r_1 < b$ and $0 \leq r_2 < b$ and assume without loss of generality that $r_2 \geq r_1$. So

$$r_2 - r_1 = (q_1 - q_2)b \implies b \mid r_2 - r_1$$

Since $r_2 - r_1 \geq 0$, either $r_2 - r_1 \geq b$ or $r_2 - r_1 = 0$. But $r_2 - r_1 < b$ (why?), so $r_1 = r_2$, and hence $q_1 = q_2$ (why?). $\square$

Example application:

Proposition 12.2. For all integers a , we have $(3 \mid a^2) \iff (3 \mid a)$.

Proof. “ $\Leftarrow$ ”: If $3 \mid a$ then $a = 3b$ for some integer b and $a^2 = (3b)^2 = 3(3b^2)$ so $3 \mid a^2$.

“ $\Rightarrow$ ”: By the division theorem

$$a = 3q + r \quad \text{where } r = 0, 1, \text{ or } 2.$$

Suppose that $3 \mid a^2$. We want to show that $r = 0$. Suppose, for a contradiction, that $a = 3q + 1$ or $a = 3q + 2$.

If $a = 3q + 1$ then

$$\begin{aligned} a^2 &= (3q + 1)^2 = 9q^2 + 6q + 1 \\ &= 3(3q^2 + 2q) + 1 \end{aligned}$$

So, by the uniqueness part of the division theorem, 3 does not divide a^2 , which is a contradiction.

If $a = 3q + 2$ then

$$\begin{aligned} a^2 &= (3q + 2)^2 = 9q^2 + 12q + 4 \\ &= 3(3q^2 + 4q + 1) + 1 \end{aligned}$$

So, by the uniqueness part of the division theorem, 3 does not divide a^2 , which is a contradiction. $\square$

Another application:

Theorem 12.3. *There are infinitely many primes.*

Proof. We will use the *fact* that every positive integer $k \geq 2$ can be written as a product of primes (we will prove this afterwards). Our proof will be by contradiction. Suppose that there are only finitely many primes, say $p_1, p_2, \dots, p_n$.

Let $a = \prod_{i=1}^n p_i + 1$. By the fact above, a is a product of primes, so there is an $i \in \{1, \dots, n\}$ such that $p_i \mid a$. This means that $a = p_i q + 0$ for some $q \in \mathbb{Z}$, while also

$$a = p_i \left(\prod_{\substack{j=1 \\ j \neq i}}^n p_j \right) + 1$$

where $0 \leq 1 < p_i$. So dividing a by p_i gives both remainder 0 and remainder 1, which contradicts the uniqueness part of the division theorem. So, there are infinitely many primes. $\square$

Theorem 12.4. *Every integer n , $n \geq 2$, is a product of primes.*

Comment. If n is prime, we will consider it a product of primes (itself).

Proof. We will prove this by strong induction.

Base case: ($n = 2$) 2 is prime so the proposition is true in this case.

Inductive step: Let $k \geq 2$. We want to show that

(any integer m , $2 \leq m \leq k$ can be written as a product of primes)

$\implies$

(any integer m , $2 \leq m \leq k + 1$ can be written as a product of primes).

This is true for $2 \leq m \leq k$ by the inductive hypothesis, so it remains to show that $k + 1$ can be written as a product of primes.

Two cases:

(I) $k + 1$ is prime. In this case we're done.

(II) $k + 1$ is *not prime*.

In this case $k + 1$ has a divisor b with $1 < b < k + 1$. Thus $k + 1 = bq$ where $1 < b, q < k + 1$. So

$$k + 1 = \underbrace{bq}_{\substack{\text{less than } k+1 \\ \text{and greater than } 1}}$$

By the inductive hypothesis, b and q can each be written as a product of primes, so $k + 1$ is also a product of primes. $\square$