MAT 511: Fundamental Concepts of Math

Written by Yongquan Zhang

Last revisited: Summer 2024

What is mathematics? One might suggest that it is the tool that we use to model our universe. Or perhaps it is the study of objects and relations. From more concrete areas like game theory and social choice theory, to incredibly abstract ones like arithmetic geometry and category theory, mathematicians study a VAST range of topics. But there are some commonalities that underpin all of math, which we will try to convey in this class.

We will start with propositional logic and set theory, the foundation upon which almost *all* mathematics builds upon. While abstraction and generality are important, we will also illustrate the theory with some easy-to-understand examples (mostly in arithmetics).

We will then talk about functions, another ubiquitous concept in math. The functions we study here will be a bit more general than what one might learn in calculus.

The next chunk of topics involve numbers and counting. We will talk about different number systems (integers, rational numbers, real numbers) and how they are constructed. We will also discuss some basic combinatorics, counting the number of certain objects, and do some "infinite counting", attempting to compare the size of different infinite sets. This is a fascinating topic, and one of its pioneer is German mathematician George Cantor, who brought the idea of different infinities into the mainstream.

Finally, to apply what we have done in a familiar setting, we will do some linear algebra.

Part I: Mathematical statements and proofs

1 The language of mathematics

If you read a math book or paper, you may encounter some or all of the following terms: definition, theorem, conjecture, proof, examples, counterexamples, axioms, etc. Many of these are examples of *propositions*. A proposition, by definition, is a sentence that is either true or false (but not both). We will understand the idea of proposition through a plethora of examples.

(1) $1 + 1 = 2$.

(2) 3.5 is an integer.

(3) 5 is a prime number.

All of these are propositions. The first and third are true, but the second is false. However, for someone who does not know what a "prime number" is, the third is arguably not a proposition, since there is no way to determine its meaning. This underlines the importance of *definitions* in

mathematics. While "prime" is a universally accepted term, there are many esoteric terms that have to be defined to be understood.

Definition 1.1. An integer larger than 1 is called a *prime number* if its only positive factors are 1 and itself.

Examples include 2, 3, 5, 7, 11, etc. Non-examples include 4, 6, 8, 9, 10, 12, etc.

(4) For every integer n, $n^2 + n + 1$ is prime.

This is an example of a "universal statement", signified by "for every", "for all", and other similar language. In fact, this is a false proposition. To show that a universal statement is false, one needs to find a *counterexample*, i.e. an example where the conclusion does not hold: when $n = 4$, $n^2 + n + 1 = 16 + 4 + 1 = 21$, which is not a prime.

(5) $x^2 - 2x > 0$.

This is not a proposition, since different values of x give different truth values (and there is no indication of "for all x" or "there exists x"). But if we assign a value to x, it becomes a proposition. Sentences of this type are called *predicates*, and x a *free variable*.

A *(mathematical) statement* is a proposition or a predicate. When we talk about generalities instead of specific statements, it is helpful to use letters P, Q to denote propositions, and $P(x), Q(m, n)$ to denote predicates with free variables. Below is another predicate.

(6) $m^2 > n$.

(7) π is a special number.

This is not a proposition, at least not without defining what "special" means. If we make an *ad hoc* definition that a number is special if it is between 3 and 4, then this becomes a proposition (a true one in fact!). But by itself, we cannot make a judgement on its truth.

Simple statements can be combined to make more complicated ones using "logical connectives". There are five of them. We will introduce each one with examples.

(8) π is a number between 3 and 4.

Another way to write this sentence is the following: $\pi > 3$ and $\pi < 4$. This is an example of the *conjunction* of two statements P, Q, denoted by $P \wedge Q$. This construction is also simply called *logical and*. The statement $P \wedge Q$ is true only when both P and Q are true:

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

Here T means true, and F means false. Such a table is called a *truth table*, and each entry a *truth value*.

(9) $3 \leq 3$.

Another way to write this sentence is the following: $3 = 3$ or $3 < 3$. This is an example of the *disjunction* of two statements P, Q, denoted by $P \vee Q$. This construction is also simply called *logical or*. The statement $P \vee Q$ is true when at least one of P and Q is true:

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

In particular $3 \leq 3$ is a true statement, which may be a bit counterintuitive.

(10) π is not an integer.

This is an example of the *negation* or *denial* of a statement P, or simply called *logical not*.

P	$\neg P$
T	F
F	T

The assumption that either P is true or $\neg P$ is true is called *the law of excluded middle*. While this is an intuitive law, in mathematics one does not have to assume it to be true. However in this course, we do accept this law.

With these three connectives in hand, we can make some more complicated statements. Here are some examples and their truth tables.

Example 1.2. Construct truth tables for $\neg(P \wedge Q)$ and $(\neg P) \vee (\neg Q)$.

Solution. The truth table for $\neg(P \wedge Q)$ is as follows:

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

and the truth table for $(\neg P) \vee (\neg Q)$ is as follows:

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

□

Note that the truth values for the two statements are always the same, regardless of what truth values for P and Q have. In this case, we call them *(logically) equivalent*, and say $\neg(P \wedge Q)$ is equivalent to $(\neg P) \vee (\neg Q)$.

We also have the following equivalence, which we leave as an exercise:

Exercise 1.3. $\neg(P \vee Q)$ is equivalent to $(\neg P) \wedge (\neg Q)$.

The two equivalences are collectively called *DeMorgan's law*. You may know (or not) another DeMorgan's law in set theory, and we will talk about their connections when we get to set theory.

DeMorgan's law is useful for constructing the denial of conjunctions and disjunctions. For example, the negation of "$\pi > 3$ and $\pi < 4$" is "$\pi \leq 3$ or $\pi \geq 4$", which is much more useful than just saying "not ($\pi > 3$ and $\pi < 4$)". Below is an exercise you can try:

Exercise 1.4. Find the denial of the following statement: π is an integer and e is a real number.

Example 1.5. Construct truth tables for $P \vee (\neg P)$ and $P \wedge (\neg P)$.

Solution. The combined truth table for the two statements is as follows:

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

□

Note that $P \vee (\neg P)$ is always true, while $P \wedge (\neg P)$ is always false. The former is an example of a *tautology*, and the latter a *contradiction*.

Example 1.6. Find all pairs $(x, y) \in \mathbb{R}^2$ so that "$x + y \geq 0$ and $x - y \leq 2$" is a tautology.

Remark 1.7. We make a remark on notation. Here $\in$ means "belongs to", which is a commonly used notation in set theory. There are many common notations for certain set of numbers (collection of numbers), including:

- The set of natural numbers $\mathbb{N} = \{1, 2, 3, \ldots\}$ (note that as a convention for this course, we do not include 0!).
- The set of integers $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}$.
- The set of rational numbers $\mathbb{Q}$ that in addition also include numbers like $2/3$, $4/5$, etc.
- The set of real numbers $\mathbb{R}$.
- The set of pairs of real numbers $\mathbb{R}^2$.

Thus $(x, y) \in \mathbb{R}^2$ simply means "a pair of of real numbers x, y".

Solution to Example 1.6. For the statement to be a tautology, we need $x + y \geq 0$ and $x - y \leq 2$ both to be true. That is we need to find pairs (x, y) satisfying $y \geq -x$ and $y \geq x - 2$. In the coordinate plane, it is the shaded region in Figure 1. □

We now return to introduce more examples of propositions.

(11) If a real number x satisfies $x^2 > 4$ then $x > 2$.

Such a statement is called an *implication*. An implication is often of the form "if P then Q", where P, Q are two statements, which we denote by $P \Rightarrow Q$. The truth table for implication is as follows:

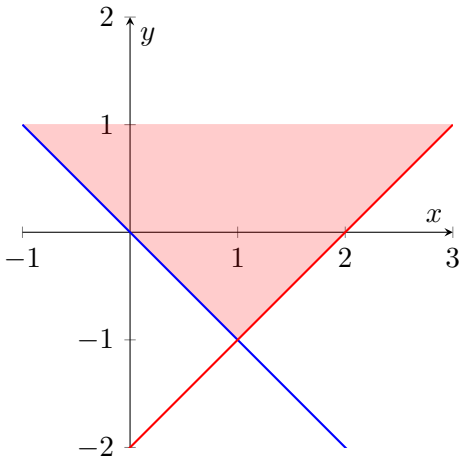


Figure 1: Region for Example 1.6.

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

The last two rows might be a bit counterintuitive, but if the assumption of an implication is outrageous (false) then the conclusion can be anything, just like one may say "If you are Chris Evans, then I am Superman".

Here is another equivalence you can show as an exercise:

Exercise 1.8. $P \Rightarrow Q$ is equivalent to $(\neg P) \vee Q$.

As a consequence we have

Example 1.9. $\neg(P \Rightarrow Q)$ is equivalent to $P \wedge \neg Q$.

Proof. Indeed, the previous exercise states that $P \Rightarrow Q$ is equivalent to $(\neg P) \vee Q$, and hence $\neg(P \Rightarrow Q)$ is equivalent to $\neg((\neg P) \vee Q)$. Applying DeMorgan's law, we know this is equivalent to $P \wedge \neg Q$, as desired. □

This example provides a useful way to construct the denial of an implication.

(12) $x^2 > 4$ if and only if $x > 2$ or $x < -2$.

Such a statement is called an *equivalence*. The equivalence of two statements P and Q is denoted by $P \Leftrightarrow Q$. By definition, $P \Leftrightarrow Q$ means $P \Rightarrow Q$ and $Q \Rightarrow P$. From this, we can construct its truth table:

P	Q	$P \Leftrightarrow Q$
T	T	T
T	F	F
F	T	F
F	F	T

That is, an equivalence is true when the two statements share the same truth value.

Remark 1.10. Note that DeMorgan's law may be stated as follows: $\neg(P \vee Q) \Leftrightarrow (\neg P \wedge \neg Q)$ is a tautology, as is $\neg(P \wedge Q) \Leftrightarrow (\neg P \vee \neg Q)$.

(13) $n > 3 \Rightarrow n > 0$.

Technically this is a predicate; however, for any real number n, this implication is always true, as supported by the following truth table:

	$n > 3$	$n > 0$	$n > 3 \Rightarrow n > 0$
$n > 3$	T	T	T
$0 < n \leq 3$	F	T	T
$n \leq 0$	F	F	T

So one can argue that this is a true proposition. This is an example of a *universal implication*. A more apparent and unambiguous way to treat it as a proposition is to write explicitly a universal statement as follows:

(14) For any real number n, $n > 3$ implies $n > 0$.

The denial of this statement would be existential: there exists a real number n such that $n > 3$ and $n \leq 0$ (note that Example 1.9 provides the way to negate an implication). More generally, the denial of the statement "For any real number n, $P(n)$ implies $Q(n)$" is "There exists a real number n such that $P(n)$ and not $Q(n)$".

Both universal and existential statements can be written in symbols only. We use $\forall$ to mean "for all", and $\exists$ to mean "there exists". Hence the statement above can be written in symbols as follows:

- $\forall n \in \mathbb{R}, n > 3 \Rightarrow n > 0$.

And its negation can be written as

- $\exists n \in \mathbb{R}, n > 3 \wedge n \leq 0$.

Summary. In this section, we introduced propositions and predicates, collectively called statements, as basic units of the language of mathematics. Starting from simple statements, we can construct more complicated ones using five logical connectives: disjunction, conjunction, negation, implication, and equivalence.

Exercise 1.11. Here are some exercises for logical equivalence, some of which appeared in your homework.

1. $P \wedge Q$ is logically equivalent to $Q \wedge P$; $P \vee Q$ is logically equivalent to $Q \vee P$.
2. $P \wedge P$ is logically equivalent to P; $P \vee P$ is logically equivalent to P.
3. $(P \wedge Q) \wedge R$ is logically equivalent to $P \wedge (Q \wedge R)$. In particular, we can just write $P \wedge Q \wedge R$ to denote either. Similarly, $(P \vee Q) \vee R$ is logically equivalent to $P \vee (Q \vee R)$.
4. $(P \wedge Q) \vee R$ is logically equivalent to $(P \vee R) \wedge (Q \vee R)$; $(P \vee Q) \wedge R$ is logically equivalent to $(P \wedge R) \vee (Q \wedge R)$.

2 Disjunctive normal forms

The *disjunctive normal form* (DNF for short) is a preferred way of writing a complicated composite statement into an equivalent form. In particular, a statement in disjunctive normal form is the disjunction of a number of conjunctions, where each conjunction is made from letters or denial of letters. Here are some examples and non-examples.

1. P is in DNF, since it is the disjunction of just one statement (with itself if you want).
2. $P \vee Q$, $P \wedge Q$ are both in DNF. In fact, $P \vee Q \vee R$, $P \wedge Q \wedge R$, $P \vee \neg Q \vee R$, $P \wedge \neg Q \wedge R$ are all in DNF. Notice that in these examples, we have either all $\wedge$ or all $\vee$.
3. $P \vee (Q \wedge R)$ is in DNF.
4. $P \wedge (Q \vee R)$ is not in DNF. However, it is equivalent to $(P \wedge Q) \vee (P \wedge R)$, which is in DNF.
5. $P \Rightarrow Q$ is not in DNF. However, it is equivalent to $(\neg P) \vee Q$, which is in DNF.
6. $\neg(P \wedge Q \wedge R)$ is not in DNF. However, we have the following logical equivalences:

$$\neg(P \wedge Q \wedge R) \Leftrightarrow \neg(P \wedge Q) \vee \neg R \Leftrightarrow \neg P \vee \neg Q \vee \neg R.$$

   This last equivalent statement $\neg P \vee \neg Q \vee \neg R$ is in DNF.

7. $P \vee (Q \wedge (R \vee S))$ is not in DNF, but it is easy to put it in DNF: $P \vee (Q \wedge (R \vee S)$ is equivalent to $P \vee (Q \wedge R) \vee (Q \wedge S)$.

3 Implications and proofs

Recall that we can construct an implication $P \Rightarrow Q$ from two statements P and Q. In an implication $P \Rightarrow Q$, the statement P is called the *hypothesis* or *antecedent*, and Q is called the *conclusion* or *consequent*. In full sentences, $P \Rightarrow Q$ may be read as:

- If P then Q;
- Q if P;
- P implies Q;
- P only if Q;
- Q whenever P;
- P is sufficient for Q;
- Q is necessary for P.

Combining some of the terms above, $P \Leftrightarrow Q$ may be read as

- P if and only if (iff) Q;
- P is equivalent to Q;
- P is necessary and sufficient for Q;
- P precisely when Q.

Given an implication $P \Rightarrow Q$, its *converse* is the statement $Q \Rightarrow P$, its *inverse* is the statement $\neg P \Rightarrow \neg Q$, and its *contrapositive* is the statement $\neg Q \Rightarrow \neg P$.

Using truth table, we can easily see that $P \Rightarrow Q$ is equivalent to $\neg Q \Rightarrow \neg P$. So instead of showing $P \Rightarrow Q$ is true, we may always show its contrapositive is true. When we use this method,

we should explicitly state what the contrapositive is and that we are proving this statement instead. For example, the contrapositive of the statement

$$a^2 + b^2 > 2ab \Rightarrow a \neq b$$

is $a = b \Rightarrow a^2 + b^2 \leq 2ab$. This is easily shown to be true, as $a = b \Rightarrow a^2 + b^2 = 2ab$.

We have talked about universal implications. Universal implications are bread and butter of *(mathematical) proofs*. A proof is a logical argument establishing the truth of some statement. The steps of a proof are implications. But one has to start from somewhere. This is the idea of *axiomatization*. We accept certain statements, called *axioms*, to be true. From there, we then establish the truth of others. Along the way, we also make useful *definitions*, which can also be a starting point of a proof. The statements proven to be true are called lemmas, propositions, or theorems, depending on their significance. One of the earliest examples of axiomatization is Euclid's *Elements*, especially his treatment of Euclidean geometry, which bears his name.

In this course, we will mostly talk about numbers and arithmetic. We need to set up some axioms and make some definitions to start proving things. Before going into details, let's see an example.

Proposition 3.1. *51 is an odd number.*

To prove this proposition, clearly one needs to define what an odd number is. We can define oddity as follows:

Definition 3.2. An integer n is said to be *odd* if $n = 2k + 1$ where k is another integer.

Under this definition, we have the following proof:

Proof. Since $51 = 2 \times 25 + 1$, it is odd by definition. □

On the other hand, below is another common definition of oddity:

Definition 3.3. An integer is *even* if it is divisible by 2, and is *odd* if it is not even.

This definition depends on the definition of divisibility:

Definition 3.4. Given two integers a, b, we say a *divides* b (or b *is divisible by* a) if $b = aq$ for some integer q.

Under this definition, we give another proof:

Proof. Let q be an integer. If $q \leq 25$, then $2q \leq 50 < 51$. If $q \geq 26$, then $2q \geq 52 > 51$. So 51 is not divisible by 2, and by definition, odd. □

We are using some properties of numbers here: for example $q \leq 25 \Rightarrow 2q \leq 50$ follows from the fact that we can multiply both sides of an inequality by a positive number. Such properties are probably taught in high school or earlier, and regarded as something simply true.

We now give some axioms for real numbers below. These will be assumed true throughout the class.

Axiom 3.5 (Arithmetic operations)**.** *Given two real numbers a, b, they have a sum $a + b$ and a product ab which are also real numbers, satisfying the following properties:*

(i) (Commutativity) $a + b = b + a$, $ab = ba$.

(ii) (Associativity) $(a + b) + c = a + (b + c)$, $(ab)c = a(bc)$. *In particular, writing* $a + b + c$ *and* abc *is unambiguous.*

(iii) (Distributivity) $a(b + c) = ab + ac$, $(a + b)c = ac + bc$. (Note that it may seem redundant to write both equalities here considering commutativity, but we want to stress that each of these properties are independent of each other.)

(iv) (Zero) $a + 0 = 0 + a = a$.

(v) (Unity) $a \cdot 1 = 1 \cdot a = a$.

(vi) (Negation and subtraction) *The equation* $a+x = 0$ *has a unique solution* $x = -a$. *Subtraction* $b - a$ *is then defined as* $b + (-a)$.

(vii) (Inverse and division) *If* $a \neq 0$, *the equation* $ax = 1$ *has a unique solution* $x = a^{-1}$. *Division* b/a *is then defined as* $b \cdot a^{-1}$.

Axiom 3.6 (Ordering)**.** (i) (Trichotomy) *For each pair of real numbers* a, b, *one and only one of the following is true:* $a < b$, $a = b$, *or* $a > b$.

(ii) (Additive law) *For any real numbers* a, b, c,

$$a < b \Leftrightarrow a + c < b + c.$$

(iii) (Multiplicative law) *For any real numbers* a, b, c,

$$a < b \Leftrightarrow ac < bc \quad \text{if } c > 0;$$
$$a < b \Leftrightarrow ac > bc \quad \text{if } c < 0.$$

(iv) (Transitive law) *For any real numbers* a, b, c,

$$a < b \text{ and } b < c \Leftrightarrow a < c.$$

Another useful notation for real numbers is the absolute value:

Definition 3.7. The absolute value $|a|$ of a real number a is defined as follows:

$$|a| = \begin{cases} a & \text{if } a \geq 0 \\ -a & \text{if } a < 0 \end{cases}$$

Now we are ready to prove some statements for real numbers.

Proposition 3.8. *For any real number* a, $a \cdot 0 = 0 \cdot a = a$.

Proof. First note that by commutativity, $a \cdot 0 = 0 \cdot a$. So we only need to show $a \cdot 0 = 0$. By property of zero, we have $0 + 0 = 0$. So

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$$

by distributivity. Now subtracting $a \cdot 0$ from both sides, we conclude

$$0 = a \cdot 0 - a \cdot 0 = (a \cdot 0 + a \cdot 0) - a \cdot 0 = a \cdot 0 + (a \cdot 0 - a \cdot 0) = a \cdot 0 + 0 = a \cdot 0,$$

as desired. □

Note that it is best practice to write full sentences when constructing a proof.

Proposition 3.9. *For any real number a, we have $a \leq |a|$.*

Proof. If $a \geq 0$, then $|a| = a$ and we are done. If $a < 0$, then $|a| = -a$. We then need to show $a \leq -a$. Indeed, since $a < 0$, we have $2a < 0$, and hence $a = 2a - a < -a$. This implies $a \leq -a$, as desired. □

Note that in this proof, we first break the argument into two different cases. In the second case, it is easier to construct proof if we start from the conclusion and find logical implications backwards. These are two important proof techniques we will explore in this course.

Proposition 3.10. *For any real numbers a, b, if $0 < a < b$, then $a^2 < b^2$.*

Proof. Since $a < b$ and $a > 0$ we have $a^2 < ab$. Similarly $ab < b^2$. By transitivity, we conclude that $a^2 < b^2$. □

Here are some other properties of real numbers one can prove

Proposition 3.11. (1) *For any real numbers a, b, we have $(-a) \cdot b = a \cdot (-b) = -ab$, and $(-a)(-b) = ab$.*

(2) *For any real number a, $|a|^2 = a^2$.*

(3) *For any real numbers a, b, c, d, if $a < b$ and $c < d$, then $a + c < b + d$. The same holds if we replace $<$ by $\leq$.*

(4) *For any real number a, if $a \neq 0$, then $a^2 > 0$.*

4 Methods of proofs

We have seen some different ways of constructing a proof. In this section, we are going to review those, and introduce some more.

4.1 Direct proof

This is the most straightforward way to write a proof. To prove the implication $P \Rightarrow Q$, we assume P is true and argue that Q is also true. We have seen many examples of this, here is another:

Proposition 4.1. *For any real number a, $-(-a) = a$.*

Proof. Since $a + (-a) = (-a) + a = 0$, the roles of a and $-a$ are symmetric. In particular, by Axiom 3.5 (vi), $a = -(-a)$. □

Proof by cases. A specific way to construct a direct proof is proof by cases. The logical foundation behind the method is as follows. If we are trying to prove $(P \vee Q) \Rightarrow R$, i.e. the hypothesis consists of several disjoint cases, we can prove a logically equivalent statement: $(P \vee Q) \Rightarrow R$ is equivalent to $(P \Rightarrow R) \wedge (Q \Rightarrow R)$. So we need prove two implications $P \Rightarrow R$ and $Q \Rightarrow R$ are both true. We have already seen some examples, here are some more:

Proposition 4.2. *For any real number a, $|-a| = |a|$.*

Proof. If $a \geq 0$, then $-a \leq 0$, and $|-a| = -(-a) = a = |a|$. If $a < 0$, then $-a > 0$ and hence $|-a| = -a = |a|$, as desired. □

Proposition 4.3. *If $a \neq 0$, then $a^2 > 0$.*

Proof. By Trichotomy Law, if $a \neq 0$, then either $a > 0$ or $a < 0$. If $a > 0$, then $a^2 > a \cdot 0 = 0$. If $a < 0$, then $a^2 = (-a)^2 > (-a) \cdot 0 = 0$, as desired. □

Remark 4.4. We have attempted to prove many properties of real numbers from Axioms 3.5 and 3.6. It is impractical (and impossible!) to prove every property of real numbers in class. From now on, we will be a bit less strict about arguing from axioms. As long as we are using familiar properties of real numbers from Precalculus, we accept them without proof.

Constructing proofs backwards. Sometimes it is easier to start from the conclusion, and go backwards to find statements that lead to it. After we arrive at a statement that follows easily from the hypothesis, we can then reorganize our notes to write down a direct proof. As you get more proficient at proof-writing, it is possible to leave the backward arguments as they are. But right now, it is very important to be careful about the direction of the implication here, so reorganizing arguments in the forward direction helps to make sure all the implications are correct.

Proposition 4.5. *Let a, b be real numbers, then $a \neq b$ implies $a^2 + b^2 > 2ab$.*

Going backwards. To show $a^2 + b^2 > 2ab$, we need to show $a^2 - 2ab + b^2 > 0$, which is equivalent to $(a-b)^2 > 0$. But this follows from the hypothesis: since $a \neq b$, we have $a - b \neq 0$, so by the previous proposition, $(a-b)^2 > 0$. Now we are ready to write a direct proof. □

Proof. Since $a \neq b$, we have $a-b \neq 0$. By the previous proposition, $(a-b)^2 > 0$. Thus $a^2-2ab+b^2 > 0$, and hence $a^2 + b^2 > 2ab$, as desired. □

4.2 Proof by contradiction

The idea of proof by contradiction is simple: if we want to prove P is true, we assume, by contradiction, $\neg P$ is true. If we can show $\neg P \Rightarrow Q$, where Q is clearly false (e.g. a contradiction), then $\neg P$ must be false as well. This then means P is true, as desired.

There are two types of statements that are often easier to prove by contradiction. We are going to discuss them both.

Negative statements. Often we can prove a negative statements using proof by contradiction. Let's start with an example:

Proposition 4.6. *There do not exist integers m, n so that $2m + 4n = 105$.*

Proof. Suppose, by contradiction, that such integers exist. Then $105 = 2m + 14n = 2(m + 7n)$ even, but clearly it is odd. This is a contradiction! Therefore such integers do not exist. □

An entirely analogous proof considering divisibility by 7 gives:

Proposition 4.7. *There do not exist integers m, n so that $14m + 21n = 100$.*

Implications. Some implications are easier to prove by contradiction, e.g. when the conclusion is a negative statement. If we want to show $P \Rightarrow Q$ is true by contradiction, we need to assume $\neg(P \Rightarrow Q)$ is true. Since $P \Rightarrow Q$ is equivalent to $(\neg P) \vee Q$, $\neg(P \Rightarrow Q)$ is equivalent to $P \wedge (\neg Q)$. So using proof by contradiction, we can assume both P and $\neg Q$ are true, so we have more to work with. This sometimes makes proof easier. Let's see an example.

Proposition 4.8. *Let a, b be real numbers. Then $a \neq b$ if and only if $a^2 + b^2 > 2ab$.*

Proof. We have already done the direction $\Rightarrow$. For the direction $\Leftarrow$, suppose by contradiction that there exist a, b so that $a = b$ and $a^2 + b^2 > 2ab$. Then $a^2 + b^2 = 2a^2 = 2ab$, a contradiction! Therefore $a^2 + b^2 > 2ab$ implies $a \neq b$, as desired. □

We emphasize here that an "if and only if" statement is the conjunction of two implications, in both directions. So we need to prove both of them.

4.3 Proof by contrapositive

We have talked about proving a statement by proving its contrapositive. Here is another example:

Proposition 4.9. *If $a \leq b$ and $b \leq a$, then $a = b$.*

Proof. The contrapositive of the statement is if $a \neq b$, then $a > b$ or $a < b$. This is just the Trichotomy Law. □

4.4 Proving "or" statements

Proof by contrapositive is just one method of showing a logically equivalent statement instead of the original one. Here is another. Suppose we want to show $P \vee Q$. Since $P \vee Q$ is equivalent to $\neg P \Rightarrow Q$, we can instead show this implication. Let's see an example:

Proposition 4.10. *Let a, b be real numbers. Then $ab = 0$ if and only if $a = 0$ or $b = 0$.*

Proof. The $\Leftarrow$ direction is straightforward. For the $\Rightarrow$ direction, assume $a \neq 0$. Then since $ab = 0$ and $a \neq 0$, we have $b = a^{-1} \cdot 0 = 0$, as desired. □

Note that we want to show $ab = 0 \Rightarrow (a = 0 \vee b = 0)$, which is equivalent to $ab = 0 \Rightarrow (a \neq 0 \Rightarrow b = 0)$. So we should use both $ab = 0$ and $a \neq 0$ as hypothesis.

5 Necessary and sufficient conditions

As discussed before, when we have $P \Rightarrow Q$, we say P is a sufficient condition for Q, and Q is a necessary condition for P. In particular, if we have $P \Leftrightarrow Q$, we say P is a necessary and sufficient condition for Q. For example, we have proved the following: "$a^2 + b^2 > 2ab$" is a necessary and sufficient condition for "$a \neq b$".

As another example, consider the statement "the triangle is isosceles".

- The statement "the triangle has two equal angles" is a necessary and sufficient condition for "the triangle is isosceles";

- The statement "the angle sum of the triangle is 180°" is necessary but not sufficient for "the triangle is isosceles";
- The statement "the triangle is equilateral" is sufficient but not necessary for "the triangle is isosceles".

In other words, necessary and sufficient condition describes exactly the same set of objects, necessary but not sufficient condition describes a strictly larger set of objects, and sufficient but not necessary condition describes a strictly smaller set of objects.

6 Quantified statements

We have talked about statements of the form "for every..." or "for all...", and how to prove such statements previously. In this section, we systematically study *quantified statements* and how to prove them.

Universal statements. Let $P(a)$ be a predicate with free variable a taking values in the set A (for now, think about A as a set of numbers, say $\mathbb{R}$). A universal statement is of the form "For any $a \in A$, $P(a)$ is true." We can write this statement in symbols:

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

Here $\forall$ is called the universal quantifier symbol, which can be read as "for any", "for all", or "for every". Below is a universal statement we have proved, written in symbols:

$$\forall (a \in \mathbb{R}) \wedge (a \neq 0), a^2 > 0.$$

Existential statements. An existential statement is of the form "For some $a \in A$, $P(a)$ is true." We can write this in symbols:

$$\exists a \in A, P(a).$$

Here $\exists$ is called the existential quantifier symbol. which can be read as "there exists", "for some", "for at least one".

A special type of existential statements comes in the following form: there exists a unique $x \in A$ so that $P(x)$. This is really the conjunction of two statements: an existential statement and a uniqueness statement. Uniqueness here means we can only find no more than one x so that $P(x)$ is true. Symbolically, we can write

$$\exists! a \in A, P(a).$$

where the exclamation point ! signifies uniqueness.

Proving or disproving quantified statements. To prove a universal statement $\forall a \in A, P(a)$, we show the implication $a \in A \Rightarrow P(a)$. We have done several examples.

To prove an existential statement $\exists a \in A, P(a)$, we only need to find an example where $P(a)$ is true. This is *proof by example*. We will see an example later.

To disprove a universal statement, i.e. to show a universal statement is false, we need to show that the negation of the universal statement is true. We've talked about the negation of a universal statement being an existential statement. That is, $\neg(\forall a \in A, P(a)) \Leftrightarrow \exists a \in A, \neg P(a)$. Therefore, we need to find an example where $P(a)$ is false. Such an example is called a *counterexample*.

To disprove an existential statement, we need to show the negation is true. The negation of $\exists a \in A, P(a)$ is a universal statement: $\forall a \in A, \neg P(a)$. So we need to show the implication $a \in A \Rightarrow \neg P(a)$.

Examples. We now go through several examples.

Example 6.1. Prove or disprove: $\forall x \in \mathbb{R}, x^2 > 2$.

Solution. This is false. Since $1 \in \mathbb{R}$ while $1^2 = 1 < 2$, we have a counterexample. □

Example 6.2. Prove or disprove: $\exists a \in \mathbb{R}, a^2 = 2$.

Solution. This is true. We may take $a = \sqrt{2}$ as an example. □

Example 6.3. Prove or disprove: $\exists x \in \mathbb{R}, x^2 = -1$.

Solution. This is false, since for any $x \in \mathbb{R}$, $x^2 > 0 > -1$. □

Example 6.4. Prove or disprove: $\exists x \in \mathbb{R}, x^2 + x - 3 = 0$.

Solution. This is true. The discriminant of the quadratic equation is given by $\Delta = 1^2 - 4(-3) = 13 > 0$, so it does have a solution. □

Example 6.5. Prove or disprove: $\exists! x \in \mathbb{R}, x^2 + x - 3 = 0$.

Solution. This is false. The discriminant of the quadratic equation is > 0, so it has two distinct solutions, not a unique one. □

Example 6.6. Prove or disprove: $\forall x \in \mathbb{R}, x^2 + 6x + 10 > 0$.

Solution. This is true. The discriminant of the quadratic equation is $\Delta = 6^2 - 4 \cdot 10 = -4 < 0$, so it has no real solutions. The graph of the function $y = x^2 + 6x + 10$ is a parabola opening upwards, and does not cross the x-axis. In particular, its value is always > 0. □

Predicates with multiple quantifiers. Let $P(a, b)$ be a predicate with free variables $a \in A$, $b \in B$. Then we can make quantified statements as follows:

- $\forall a \in A, \forall b \in B, P(a, b)$. To prove this, we need to show $(a \in A) \wedge (b \in B) \Rightarrow P(a, b)$. To disprove this, we need to find an counterexample pair. So the negation is $\exists a \in A, \exists b \in B, \neg P(a, b)$
- $\exists a \in A, \exists b \in B, P(a, b)$. To prove this, we need to find an example pair a, b. To disprove this, we need to show its negation is true, which is a universal statement: $\forall a \in A, \forall b \in B, \neg P(a, b)$
- $\forall a \in A, \exists b \in B, P(a, b)$. To prove this, we need to find an example $b \in B$ for any $a \in A$, which may well be different for different a. To disprove this, we need to find a counterexample $a_0 \in A$, where for any $b \in B$, $P(a_0, b)$ is false. Note that negating such a statement is easy enough: the negation is $\exists a \in A, \forall b \in B, \neg P(a, b)$.
- $\exists a \in A, \forall b \in B, P(a, b)$. To prove this, we need to find an example $a_0 \in A$, so that $P(a_0, b)$ is true for all $b \in B$. To disprove this, we need to show that for any $a \in A$, there exists an example $b \in B$ (depending on a), so that $P(a, b)$ is false. That is, the negation is given by $\forall a \in A, \exists b \in B, \neg P(a, b)$.

We now see some examples.

Example 6.7. Prove or disprove:

(1) $\forall m \in \mathbb{N}, \exists n \in \mathbb{N}, m < n$.

(2) $\exists m \in \mathbb{N}, \forall n \in \mathbb{N}, m < n$.

(3) $\forall m \in \mathbb{N}, \forall n \in \mathbb{N}, m < n$.

(4) $\exists m \in \mathbb{N}, \exists n \in \mathbb{N}, m < n$.

Solution. (1) This is true. Indeed, for any $m \in \mathbb{N}$, take $n = m + 1$, we have $m < n$.

(2) This is false. Indeed, for any $m \in \mathbb{N}$, take $n = 1$, then $m \geq n$.

(3) This is false. Indeed, for $m = 2$ and $n = 1$ we have $m \geq n$.

(4) This is true. Indeed, we can take $m = 1$ and $n = 2$.

□

7 The induction principle

7.1 The induction principle and its variants

Induction is another method of proof for statements involving natural numbers[1]. Basic rules of arithmetic and ordering are often not enough to show some properties hold for *all* natural numbers, What these axioms fail to capture is the idea that natural numbers can be constructed from 1 and successively adding 1: we start from 1, and then get 2, and then 3, and so on. This is the main idea behind the induction principle:

Axiom 7.1 (Induction principle)**.** *Suppose $P(n)$ is a statement involving a general positive integer n. Then $P(n)$ is true for all positive integers $n = 1, 2, 3, \ldots$ if*

(i) *$P(1)$ is true;*

(ii) *The implication $P(k) \Rightarrow P(k + 1)$ is true for all positive integers k.*

Some terminology: $n+1$ is called the *successor* of an integer n (and n the *predecessor* of $n+1$). The first part (i) in the induction principle is often called *the base case*, and the second part (ii) *the inductive step*.

In the inductive step, we assume $P(k)$ is true and show that $P(k + 1)$ is also true. The idea is then that since $P(1)$ is true by the base case, then $P(2)$ is true by the inductive step, and then $P(3)$ is true, and $P(4)$ is true, and so on.

Let's see an example.

Proposition 7.2. *For all positive integers n, we have $n \leq 2^n$.*

Proof. We prove by induction on n.

Base case When $n = 1$, we have $2^n = 2 > 1$. So the statement holds for $n = 1$.

Inductive step Suppose now as inductive hypothesis that $k \leq 2^k$ is true for a positive integer k. Then

$$2^{k+1} = 2^k \cdot 2 \geq 2k = k + k \geq k + 1.$$

[1]In this course, natural numbers are $1, 2, 3, \ldots$. But this is not universally agreed upon. Some mathematicians include 0 as well.

Therefore the statement is also true for $n = k + 1$.

Conclusion Hence by induction, $n \leq 2^n$ for all positive integers n. □

Note that it is not enough to just check the statement is true for 1, 2, 3, or even up to 10000000, since we need to show it is true for *all* positive integers, and there are infinitely many of them.

We remark that it is generally good practice to be explicit about using induction. It is also helpful to label the base case and the inductive step. After becoming more familiar with the method, you can be less rigid about the structure, but it is prudent to be a bit more careful right now when first learning induction.

Here is another example:

Proposition 7.3. *For any positive integer n, $n^2 + n$ is even.*

Proof. We prove by induction on n.

Base case When $n = 1$, $n^2 + n = 1 + 1 = 2$ is even. So the statement is true for $n = 1$.

Inductive step Suppose as inductive hypothesis that $k^2 + k$ is even for some positive integer k. Then

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

is even, since it is the sum of two even numbers.

Conclusion Hence by induction, $n^2 + n$ is even for all positive integers n. □

We do one more example in the same vein:

Proposition 7.4. *For any natural number n, $n^3 - n + 3$ is divisible by 3.*

Proof. We prove by induction on n.

Base case When $n = 1$, $n^3 - n + 3 = 3$ is divisible by 3. So the statement is true for $n = 1$.

Inductive step Suppose as inductive hypothesis that $k^3 - k + 3$ is divisible by 3 for some natural number k. Then

$$(k + 1)^3 - (k + 1) + 3 = k^3 + 3k^2 + 3k + 1 - k - 1 + 3 = (k^3 - k + 3) + 3(k^2 + k)$$

is divisible by 3 as well, since it is the sum of two multiples of 3.

Conclusion Hence by induction, $n^3 - n + 3 = 3$ is divisible by 3 for all positive integers n. □

Some variations. Here are some variations of the induction principle.

1. Change base case. We don't have to start with $n = 1$. The same method works if we want to prove a statement $P(n)$ involving integers $\geq n_0$. Instead of checking $P(1)$, we check $P(n_0)$. Then the inductive step tells us that $P(n)$ is true for $n = n_0, n_0 + 1, n_0 + 2, \ldots$

Proposition 7.5. *For any integer $n \geq 4$, $n^2 \leq 2^n$.*

Proof. We prove by induction on n.

Base case When $n = 4$, we have $n^2 = 4^2 = 16 = 2^4 = 2^n$. So the statement holds for $n = 4$.

Inductive step Suppose as an inductive hypothesis $k^2 \leq 2^k$ for some integer $k \geq 4$. Then $2^{k+1} \geq 2k^2$. To show $2^{k+1} \geq (k + 1)^2$, it is enough to show that $2k^2 \geq (k + 1)^2$. This is equivalent to $2k^2 \geq k^2 + 2k + 1$, which is equivalent to $k^2 - 2k + 1 \geq 2$, which is equivalent to $(k - 1)^2 \geq 2$. Since $k \geq 4$, $k - 1 \geq 3$, so $(k - 1)^2 \geq 9 > 2$, as desired. So the statement holds for $n = k + 1$ as well.

Conclusion Hence by induction, $n^2 \leq 2^n$ for any integer $n \geq 4$. □

2. Other integer sequences. We can also apply induction to some integer sequences depending on natural numbers. Here is an example:

Proposition 7.6. *For any positive odd integer n, $n^2 - 1$ is divisible by 8.*

Note that a positive odd integer is of the form $n = 2k + 1$ for an integer $k \geq 0$. Then

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

So the original statement is equivalent to the following: for any integer $k \geq 0$, $4(k^2 + k)$ is divisible by 8. We can then apply induction to prove this. The proof is omitted, since it is very standard.

Alternatively, we can adopt the following proof scheme:

(1) Show that the statement is true for $n = 1$.

(2) Show that $P(n) \Rightarrow P(n + 2)$.

Then similar to the basic idea of induction, we have $P(1)$ is true, then $P(3)$ is true, then $P(5)$, etc.

This also suggests an idea to prove a statement $P(n)$ is true for all integers:

(1) Show that the statement is true for $n = 1$.

(2) Show that $P(n) \Rightarrow P(n + 1)$, and $P(n) \Rightarrow P(n - 1)$.

Of course, for negative integers, we can also just set $m = -n$ and apply the usual induction.

Some caveats. We remark that when proving a statement by induction, both steps (the base case and the inductive step) are very important. Moreover, in the inductive step, we are not showing the truth of $P(n)$ by itself, but rather the implication $P(k) \Rightarrow P(k + 1)$. Since we do not know the truth of $P(n)$ at this stage other than the base case, it is important to use *only* the inductive hypothesis and nothing else.

Here is an example of a flawed application of induction, proving an obviously false statement:

Claim 7.7. *$2^n = 2$ for any integer $n \geq 0$.*

Proof. We prove by induction on n.

Base case When $n = 1$, $2^n = 2^1 = 2$, as desired.

Inductive step Suppose as an inductive hypothesis that $2^k = 2$ for some $k \geq 0$. Then

$$2^{k+1} = 2^k \cdot 2 = 2^k \cdot \frac{2^k}{2^{k-1}} = 2 \cdot \frac{2}{2} = 2.$$

So the statement holds for $n = k + 1$ as well.

Conclusion Hence by induction, $2^n = 2$ for any integer $n \geq 0$. □

There are two issues with the proof. First, the base case is $n = 0$ not $n = 1$. Second, in the inductive step, $2^{k-1} = 2$ is also used; this is *not* part of the inductive hypothesis.

Here is another example of induction, involving multiple variables where we induct on one of them:

Proposition 7.8. *For any natural number n and real number $x > -1$, we have $(1 + x)^n \geq 1 + nx$.*

Proof. Note that the statement involves natural numbers, so we can still do induction on n (although not on x).

Base case When $n = 1$, the left hand side of the inequality gives $1 + x$, as does the right hand side.

Inductive step Suppose as an inductive hypothesis that the statement is true when $n = k$, i.e. $(1 + x)^k \geq 1 + kx$ for all $x > -1$. When $n = k + 1$, we have

$$(1 + x)^{k+1} = (1 + x)(1 + x)^k \geq (1 + x)(1 + kx),$$

since $1 + x > 0$, and by the inductive hypothesis $(1 + x)^k \geq (1 + kx)$. Then

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

Hence $(1 + x)^{k+1} \geq 1 + (k + 1)x$, i.e. the statement holds for $n = k + 1$. By induction, the original statement holds for all $n \in \mathbb{N}$. □

Strong induction. Sometimes the truth of $P(k+1)$ is hard to establish from just $P(k)$, and one might need more precedents as inductive hypothesis. This is the idea of strong induction:

Axiom 7.9 (Strong Induction principle)**.** *Suppose $P(n)$ is a statement involving a general positive integer n. Then $P(n)$ is true for all positive integers $n = 1, 2, 3, \ldots$ if*

(i) *$P(1)$ is true;*

(ii) *The implication $[P(n)$ is true for all $n \leq k] \Rightarrow P(k + 1)$ is true for all positive integers k.*

We will see some examples in the next section. It is not hard to show that strong induction is equivalent to regular induction.

7.2 Definition by induction

How do we define $1 + 2 + 3 + \cdots + n$ rigorously? While most of us understand this expression means adding up the first n natural numbers, but in the expression $\cdots$ is a bit ambiguous, and can lead to confusion in more complicated situations. The idea of induction can be used to define such expressions.

Definition 7.10. Given a sequence of numbers $a(1), a(2), a(3), \ldots$, the sum $\sum_{i=1}^{n} a(i)$ for any positive integer n is defined inductively:

(i) $\sum_{i=1}^{1} a(i) = a(1)$;

(ii) $\sum_{i=1}^{k+1} a(i) = \sum_{i=1}^{k} a(i) + a(k + 1)$ for $k \geq 1$.

Again, the idea is that by the base case, the expression is defined for $n = 1$, and then by the inductive step, the expression is defined for $n = 2, 3, 4$, and so on.

Here are some familiar expressions defined inductively:

Definition 7.11. For any real number x, the powers x^n for any non-negative integer n is defined inductively by:

(i) $x^0 = 1$;

(ii) $x^{k+1} = x^k \cdot x$ for $k \geq 0$.

In particular, in this definition, $0^0 = 1$, which is definitely not something universally agreed upon. In the expression x^n, the number x is called the *base*, and n is called the *exponent*.

Definition 7.12. For any non-negative integer n, the factorial $n!$ is defined inductively by

(i) $0! = 1$;

(ii) $(k+1)! = k! \cdot (k+1)$ for $k \geq 0$.

For statements involving expressions defined inductively, induction is often a pretty apt method of proof. For example, we have

Proposition 7.13. *For any positive integer n,* $\displaystyle\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

Proof. We prove by induction on n. The base case $n = 1$ is easy. Suppose as inductive hypothesis that $\displaystyle\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$ for some positive integer k. Then

$$\sum_{i=1}^{k+1} i = \sum_{i=1}^{k} i + k + 1 = \frac{k(k+1)}{2} + k + 1 = (k+1)\left(\frac{k}{2} + 1\right) = \frac{(k+1)(k+2)}{2}$$

as desired. So the statement holds for any positive integer n by induction. □

Note that the proof is not written in the exact template from the last section. As we move forward in the course, we can be a bit loose about the exact format of the proof, as long as it is clear that both the base case and the inductive step are taken care of.

Here are some more statements that can be proved using induction:

Proposition 7.14. (1) *Let x, y be real numbers. Then $(xy)^n = x^n y^n$ for any integer $n \geq 0$.*

(2) *Let x be a real number. Then $x^{m+n} = x^m x^n$ for any integers $m, n \geq 0$.* (This can be shown by induction on just n.)

The Fibonacci sequence. The Fibonacci sequence is a famous sequence of integers that can be defined inductively. Named after 12th to 13th century mathematician Fibonacci, the sequence has many interesting properties.

Definition 7.15. The n-th Fibonacci number u_n is defined inductively as follows: $u_1 = u_2 = 1$, and $u_{k+1} = u_{k-1} + u_k$ for any integer $k \geq 2$.

Note that this definition employs the stronger version of induction. The first few Fibonacci numbers are

$$1, 1, 2, 3, 5, 8, 13, \ldots$$

The following closed formula for u_n, was first discovered by 19th century French mathematician Jacques Philippe Marie Binet:

Proposition 7.16 (Binet's formula)**.** *The n-th Fibonacci number is given by*

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

where $\alpha = \dfrac{1+\sqrt{5}}{2}$*, and* $\beta = \dfrac{1-\sqrt{5}}{2}$*.*

Proof. It is not hard to see that α, β are roots of the quadratic polynomial $x^2 - x - 1 = 0$. In particular $\alpha^2 = \alpha + 1$ and $\beta^2 = \beta + 1$.

We prove the formula by induction on n. Note that the inductive step only starts to work when $k \geq 2$ in the definition of Fibonacci numbers, so we need to show two base cases. When $n = 1$, $\alpha - \beta)/\sqrt{5} = \sqrt{5}/\sqrt{5} = 1 = u_1$. When $n = 2$,

$$(\alpha^2 - \beta^2)/\sqrt{5} = \left(\frac{6+2\sqrt{5}}{4} - \frac{6-2\sqrt{5}}{4}\right)/\sqrt{5} = 1 = u_2.$$

So both cases are true. Now suppose by induction that $u_n = (\alpha^n - \beta^n)/\sqrt{5}$ for all $n \leq k$ for some integer $k \geq 2$. Then

$$\begin{aligned} u_{k+1} = u_k + u_{k-1} &= \frac{\alpha^k - \beta^k}{\sqrt{5}} + \frac{\alpha^{k-1} - \beta^{k-1}}{\sqrt{5}} \\ &= \frac{1}{\sqrt{5}}\left(\alpha^{k-1}(1+\alpha) - \beta^{k-1}(1+\beta)\right) \\ &= \frac{1}{\sqrt{5}}\left(\alpha^{k-1}\alpha^2 - \beta^{k-1}\beta^2\right) \\ &= \frac{\alpha^{k+1} - \beta^{k+1}}{\sqrt{5}}, \end{aligned}$$

as desired. So Binet's formula holds for all positive integers by induction. □

Here is another example:

Proposition 7.17. *For any integers* $m \geq 2$ *and* $n \geq 1$*, we have*

$$u_{m+n} = u_{m-1}u_n + u_m u_{n+1}.$$

Proof. We prove by induction on n. The case $n = 1$ is just the definition of Fibonacci sequence $u_{m+1} = u_{m-1} + u_m$. When $n = 2$, we want to show $u_{m+2} = u_{m-1}u_2 + u_m u_3 = u_{m-1} + 2u_m$. We can prove this by applying the recursive relation twice:

$$u_{m-1} + 2u_m = u_{m-1} + u_m + u_m = u_{m+1} + u_m = u_{m+2}.$$

Suppose the statement holds for all $n \leq k$ where k is some integer ≥ 2. Then

$$\begin{aligned} u_{m+k+1} = u_{m+k} + u_{m+k-1} &= u_{m-1}u_k + u_m u_{k+1} + u_m u_{k-1} + u_m u_k \\ &= u_{m-1}(u_k + u_{k-1}) + u_m(u_{k+1} + u_k) \\ &= u_{m-1}u_{k+1} + u_m u_{k+2}, \end{aligned}$$

as desired. So by induction, the statement holds for all $n \geq 1$. □

MAT 511: Fundamental Concepts of Math

Written by Yongquan Zhang

Last revisited: Summer 2024

Part II: Sets and functions

We have talked about the logical foundation of mathematics in Part I, and introduced many methods of proof. In Part II, we are going to talk about the most basic objects mathematicians study, sets and functions.

1 (Naïve) set theory

Essentially all objects mathematicians study can be defined as elements of some sets. The language of set theory is ubiquitous in every branch of mathematics, and many math-adjacent subjects as well. Here, we are going to study the basic notations of set theory, as well as some set-theoretic operations. While we will try to be as rigorous as possible, a completely rigorous treatment of set theory via axioms is difficult and much more than we actually need in this class, so we will study a version of "naïve" set theory.

For those interested, the most common adopted axiomatic system for set theory is ZF or ZFC (Zermelo-Fraenkel-Choice), named after German mathematician E. Zermelo and German-born Israeli mathematician A. Fraenkel. The additional "C" is for Axiom of Choice, which is a somewhat controversial axiom that some mathematicians prefer to avoid, since it leads to some highly counterintuitive results. Most mathematicians however do accept Choice.

Sets. A *set* is a well-defined collection of objects, usually denoted by a single capital letter. The members of a set are called *elements*. If x is an element of the set X, we write $x \in X$. The negation of the statement $x \in X$ is $x \notin X$, i.e x is not an element of X.

We are going to deal with number sets a lot. Here are some commonly used notations for important number sets:

$\mathbb{Z}$	the set of integers (comes from German "Zahlen")
$\mathbb{N}$ or $\mathbb{Z}^+$	the set of natural numbers / positive integers
$\mathbb{Z}^{\geq}$ or $\mathbb{Z}^{\geq 0}$	the set of nonnegative integers
$\mathbb{Q}$	the set of rational numbers
$\mathbb{R}$	the set of real numbers
$\mathbb{R}^+$	the set of positive real numbers
$\mathbb{R}^{\geq}$ or $\mathbb{R}^{\geq 0}$	the set of nonnegative real numbers
$\mathbb{C}$	the set of complex numbers

For example, we can write $2 \in \mathbb{Q}$ and $\sqrt{2} \notin \mathbb{Q}$, and so on.

Specifying a set. There are three ways to define a set, i.e. to specify what elements a set contains. They are:

- Listing its elements. For example,

$$A = \{1, 3, \pi, -14\},$$

where we list all elements of a set A in bracket. Note that the order in which we list elements is not important, and repeating the same element more than once also makes no difference. In other words

$$\{1, 1, 3, 3, \pi, \pi, \pi, -14\} \text{ and } \{3, 1, -14, \pi\}$$

all specify the same set A. We can also list elements of some infinite sets:

$$\mathbb{N} = \{1, 2, 3, 4, \ldots\}$$

- Conditional definition. We can define a set by writing down a condition that elements of the set satisfy. That is we can define a set

$$A = \{a \in X | P(a)\}$$

where $P(a)$ is a predicate with a free variable a, whose value ranges in X. Then the set above contains only and every a so that $P(a)$ is true. In other words

$$a \in A \Leftrightarrow P(a)$$

As a concrete example, we have

$$\mathcal{E} = \{n \in \mathbb{Z} | n \text{ is divisible by } 2\} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$$

is the set of even numbers. We remark that $\mathcal{E}$ is an object, and not a statement, while $2 \in \mathcal{E}$ is a statement (a true one at that!)

There are some commonly used shorthands for subsets of real numbers defined by inequalities:

$$\begin{aligned}
(a, b) &= \{x \in \mathbb{R} | a < x < b\} \text{ “an } \textit{open interval}\text{”} \\
[a, b] &= \{x \in \mathbb{R} | a \leq x \leq b\} \text{ “a } \textit{closed interval}\text{”} \\
[a, b) &= \{x \in \mathbb{R} | a \leq x < b\} \\
(a, b] &= \{x \in \mathbb{R} | a < x \leq b\} \\
(a, +\infty) &= \{x \in \mathbb{R} | x > a\} \\
[a, +\infty) &= \{x \in \mathbb{R} | x \geq a\} \\
(-\infty, a) &= \{x \in \mathbb{R} | x < a\} \\
(-\infty, a] &= \{x \in \mathbb{R} | x \leq a\}
\end{aligned}$$

- Constructive. We can define a set by giving a formula or an algorithm for its elements. For example, the set of even numbers can also be defined as

$$\mathcal{E} = \{2n | n \in \mathbb{Z}\}.$$

Some other examples include

$$\{n^2 | n \in \mathbb{Z}\} = \{0, 1, 4, 9, 16, \ldots\}, \quad \mathbb{Q} = \left\{ \frac{p}{q} \middle| p, q \in \mathbb{Z}, q \neq 0 \right\}.$$

Equality of sets. Two sets A and B are *equal*, written $A = B$, if they contain exactly the same elements. In other words $A = B$ means

$$x \in A \Leftrightarrow x \in B.$$

In ZFC, this is one of the axioms called Axiom of Extensionality.

For example we have

$$\{x \in \mathbb{R} | x^2 - x - 2 = 0\} = \{-1, 2\},$$

since $x^2 - x - 2 = 0$ iff $x = -1$ or $x = 2$.

Empty set. The *empty set* $\emptyset$ is the unique set containing no elements at all. For example we have

$$\{x \in \mathbb{R} | x^2 = -1\} = \emptyset,$$

since no real number squared equals to -1.

Subsets. Given sets A, B, we say A is a *subset* of B (or B is a *superset* of A), written as $A \subseteq B$ or $B \supseteq A$, if every element of A is an element of B. In logical terms, $A \subseteq B$ iff $x \in A \Rightarrow x \in B$. If furthermore, A and B are unequal (i.e. B contains some elements not in A), we say A is a *proper* subset of B, and write $A \subsetneq B$

We remark that $a \in A \Leftrightarrow \{a\} \subseteq A$, that is, a is an element of A if and only if the *singleton* $\{a\}$ containing one element is a subset of A.

If two sets are conditionally defined by predicates, say

$$\{a \in A | P(a)\} \text{ and } \{a \in A | Q(a)\}$$

then

"For any $a \in A, P(a) \Rightarrow Q(a)$" is equivalent to $\{a \in A | P(a)\} \subseteq \{a \in A | Q(a)\}$

Here are some more properties about subsets:

- If $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$.
- $A \subseteq A$ for any set A.
- $\emptyset \subseteq A$ for any set A.
- $A \subseteq \emptyset$ iff $A = \emptyset$.
- $A = B$ iff $A \subseteq B$ and $B \subseteq A$.

Power set. The *power set* of a set X, denoted by $\mathcal{P}(X)$, is the set of all subsets of X. Thus

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

As an example, let $X = \{1, 2, 3\}$. Then

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

By properties of subsets, we have the following

- $\emptyset \in \mathcal{P}(X)$ and $X \in \mathcal{P}(X)$ for any set X.

Note that $\mathcal{P}(\emptyset) = \{\emptyset\} \neq \emptyset$, as $\{\emptyset\}$ is a set containing one element, the empty set.

Set operations. Here are some common set operations.

1. Intersection. The *intersection* of two sets A and B, denoted by $A \cap B$, is the set containing elements in both A and B. In other words:

$$A \cap B = \{x | x \in A \text{ and } x \in B\}.$$

   In logical terms

$$x \in A \cap B \Leftrightarrow x \in A \wedge x \in B.$$

   Note the similarity between notations $\cap$ and $\wedge$. We say A and B are *disjoint* if $A \cap B = \emptyset$.

2. Union. The *union* of two sets A and B, denoted by $A \cup B$, is the set containing elements in A or in B. In other words,

$$A \cup B = \{x | x \in A \text{ or } x \in B\}.$$

   In logical terms,

$$x \in A \cup B \Leftrightarrow x \in A \vee x \in B.$$

   Again notice the similarity between $\cup$ and $\vee$.

3. Difference. The *difference* of A and B, denoted by $A - B$ or $A \backslash B$, is the set containing elements in A but not in B. In other words

$$A - B = \{x | x \in A \text{ and } x \in B\}.$$

4. Complement. Often, we fix an ambient set X, called the *universal set*, and work with subsets of this set (e.g. we often work with subsets of real numbers). Once we fix a universal set X, the *complement* of a set $A \in \mathcal{P}(X)$, denoted by A^c, is the set $X - A = U \setminus A$. In other words

$$A^c = \{x \in X | x \notin A\}.$$

   In logical terms,

$$x \in A^c \Leftrightarrow x \notin A.$$

We remark that complement and difference are closely related. Given a universal set X so that $A, B \subseteq X$, then $A - B = A \cap B^c$.

The goal now is to illustrate some properties of set operations. In all of them we will assume that the sets are a subset of a fixed universal set X, i.e. all the sets will be elements of $\mathcal{P}(X)$.

Proposition 1.1. *For any sets A, B, we have*

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

Moreover $A \cap B$, $A - B$, $B - A$ are pairwise disjoint.

Proof. This can be proved using truth tables:

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

Note that the last two columns are exactly the same, so $x \in A \cup B$ iff $x \in (A \cap B) \cup (A - B) \cup (B - A)$, which means

$$A \cup B = (A \cap B) \cup (A - B) \cup (B - A)$$

as desired. Moreover, in the third to fifth column, there is at most one true for each row. This means that any two of the three sets $A \cap B, A - B, B - A$ do not contain common elements. □

Theorem 1.2. *Let X be a fixed universal set. Suppose $A, B, C \in \mathcal{P}(X)$. Then we have the following identities:*

(1) *(Associativity) $A \cup (B \cup C) = (A \cup B) \cup C$, $A \cap (B \cap C) = (A \cap B) \cap C$;*

(2) *(Commutativity) $A \cup B = B \cup A$, $A \cap B = B \cap A$;*

(3) *(Distributivity) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;*

(4) *(De Morgan's Laws) $(A \cup B)^c = A^c \cap B^c$, $(A \cap B)^c = A^c \cup B^c$.*

Note that many of these can be proved using the corresponding logical equivalence. For example, De Morgan's laws translate exactly to De Morgan's laws in logic we studied in Part I. As a historical note, De Morgan's laws were first observed independently by British mathematician Augustus De Morgan, and American Mathematician Benjamin Peirce, who is regarded as the first American research mathematician.

Another way to prove these is to show both $\subseteq$ and $\supseteq$. We now prove the first identity in (3) as an example:

Proof. $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$:

Let $x \in A \cup (B \cap C)$. Then either $x \in A$ or $x \in B \cap C$. If $x \in A$, then $x \in A \cup B$ and $x \in A \cup C$, so $x \in (A \cup B) \cap (A \cup C)$, as desired. If $x \in B \cap C$, then $x \in B$ and $x \in C$. Therefore $x \in A \cup B$ and $x \in A \cup C$, and so $x \in (A \cup B) \cap (A \cup C)$ as well.

$A \cup (B \cap C) \supseteq (A \cup B) \cap (A \cup C)$:

Let $x \in (A \cup B) \cap (A \cup C)$. Then $x \in A \cup B$ and $x \in A \cup C$. To show that $x \in A \cup (B \cap C)$, it is equivalent to show that $x \notin A$ implies $x \in B \cap C$. Indeed, suppose now $x \notin A$. Then $x \in B$ and $x \in C$, and so $x \in B \cap C$, as desired. □

Proposition 1.3. *For any sets A, B, C, D, we have*

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

Proof. We can again prove using truth tables, logical equivalences, or the method above. For this, we can also use the set-theoretic identities in Theorem 1.2. Indeed,

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

as desired □

Proposition 1.4. *Let A, B, C be sets. Show that $(A \cap B) - C = A \cap (B - C)$.*

Proof. Let $x \in (A \cap B) - C$. Then $x \in A \cap B$ and $x \notin C$. Thus $x \in A$, and $x \in B$, and $x \notin C$. Since $x \in B$ and $x \notin C$, we have $x \in B - C$. At the same time $x \in A$, so $x \in A \cap (B - C)$. Thus $(A \cap B) - C \subseteq A \cap (B - C)$.

Conversely, let $x \in A \cap (B - C)$. Then $x \in A$ and $x \in B - C$. Hence $x \in A$ and at the same time $x \in B$ and $x \notin C$. Since $x \in A$ and $x \in B$, we know $x \in A \cap B$. Since in addition $x \notin C$, we have $x \in (A \cap B) - C$. Hence $A \cap (B - C) \subseteq (A \cap B) - C$.

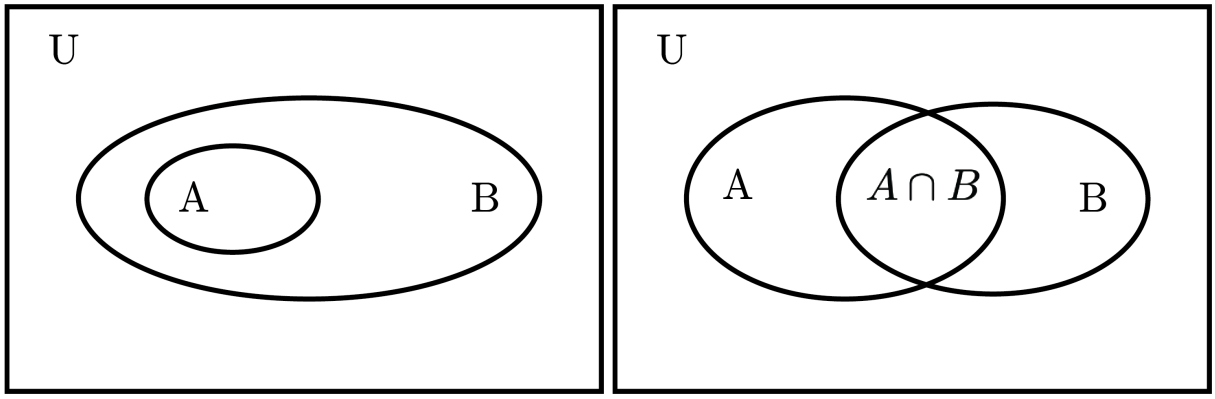
Since we have both inclusion, we conclude that the two sets are equal.

Alternatively, choose a universal set X so that $A, B, C \subseteq X$. Then

$$(A \cap B) - C = (A \cap B) \cap C^c = A \cap (B \cap C^c) = A \cap (B - C),$$

as desired. □

Venn diagram. Venn diagrams are useful to illustrate set relations and set identities. In a Venn diagram, we draw a large rectangle to signify the universal set, and a bubble for each set. The common part of two bubbles is the intersection, and two bubbles combined become the union. See Figure 1 some simple examples.



(a) A Venn diagram for $A \subseteq B$ (b) A Venn diagram for $A \cap B$

Figure 1: Some Venn diagrams

The set-theoretic identities proved above can be illustrated by Venn diagrams. Indeed, Prop. 1.1 can be seen in Figure 2. And the first identity in (3) of Theorem 1.2 can be illustrated as in Figure 3.

Cartesian product. Given sets X and Y, the *Cartesian product* of X and Y, denoted by $X \times Y$, is the set of all ordered pairs (x, y) where $x \in X$, and $y \in Y$, i.e.

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

By ordered pairs we mean that $(x_1, y_1) = (x_2, y_2)$ if and only if $x_1 = x_2, y_1 = y_2$. The components x and y in (x, y) are called its *coordinates*. When $X = Y$, we simply write $X^2 = X \times X$. This notation may be familiar to those with some knowledge of two dimensional Cartesian plane, since we write $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$.

We can, of course, form $X \times Y \times Z$, and $X \times Y \times Z \times W$, and so on, as ordered triples, quadruples, etc. Similarly, $X^n = X \times X \times \cdots \times X$ consists of ordered n-tuples $(x_1, x_2, \ldots, x_n)$ of elements in X.

Here are some properties of Cartesian products:

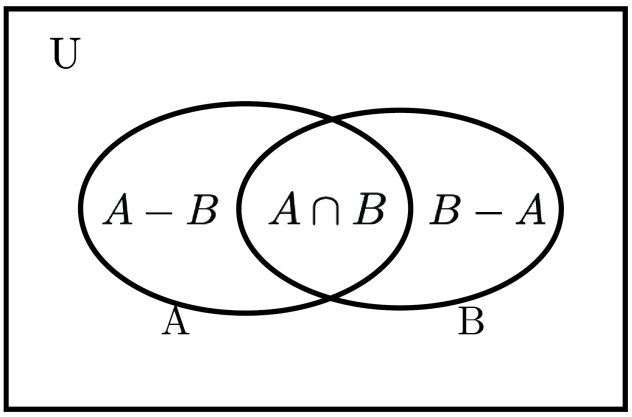


Figure 2: The three mutually disjoint parts of $A \cup B$

Theorem 1.5. *Let $A, C \subset X$ and $B, D \subset Y$ be sets. Then we have*

(1) $A \times (B \cup C) = (A \times B) \cup (A \times C)$;

(2) $A \times (B \cap C) = (A \times B) \cap (A \times C)$;

(3) $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$;

(4) $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$;

These can be proved using arguments we give for Part (3) of Theorem 1.2. For example, we show:

Proof. For Part (1), we first show $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$. Let $(x, y) \in A \times (B \cup C)$. Then $x \in A$ and $y \in B \cup C$. So $y \in B$ or $y \in C$. In the first case $(x, y) \in A \times B$, and in the second case, $(x, y) \in A \times C$. So we always have $(x, y) \in (A \times B) \cup (A \times C)$, as desired.

Conversely, if $(x, y) \in (A \times B) \cup (A \times C)$, then either $(x, y) \in A \times B$ or $(x, y) \in A \times C$. In the first case, we have $x \in A$ and $y \in B$. Since $B \subseteq B \cup C$, we have $y \in B \cup C$ as well. Hence $(x, y) \in A \times (B \cup C)$. The second case similarly leads to $(x, y) \in A \times (B \cup C)$, as desired.

All other parts are similar. □

For Part (4), we comment on the fact that the other inclusion is not necessarily true. For example, if $A = \{1\}, B = \{2\}, C = \{3\}, D = \{4\}$, then $(A \times B) \cup (C \times D) = \{(1, 2), (3, 4)\}$, while $(A \cup C) \times (B \cup D) = \{(1, 2), (1, 4), (3, 2), (3, 4)\}$.

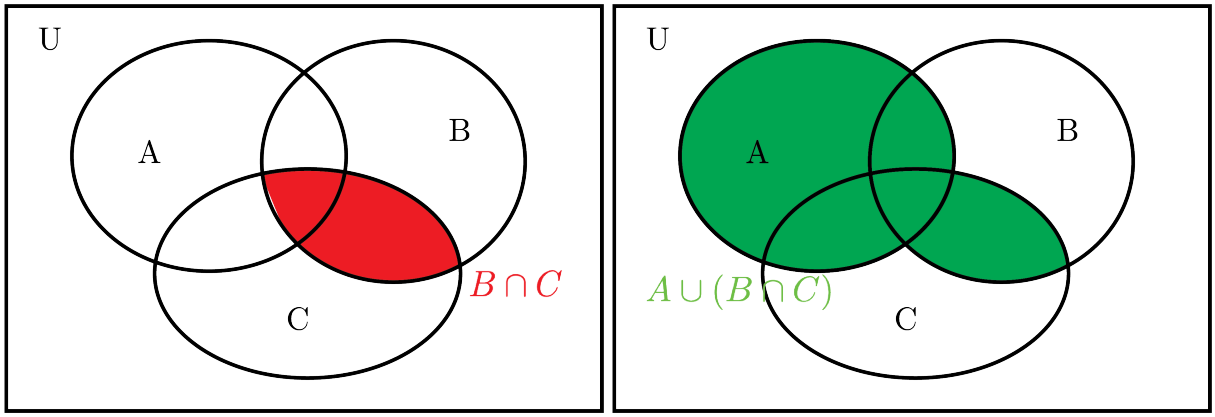
What conditions do we need to impose so that we have equality in Theorem 1.5 (4)?

A comment on axiomization. As we have mentioned at the beginning, we are not doing a rigorous treatment of set theory via axioms, but rather a naive and intuitive version. Here we make a comment on why such an approach ran into problems when mathematicians attempted to lay firm foundation for the theory.

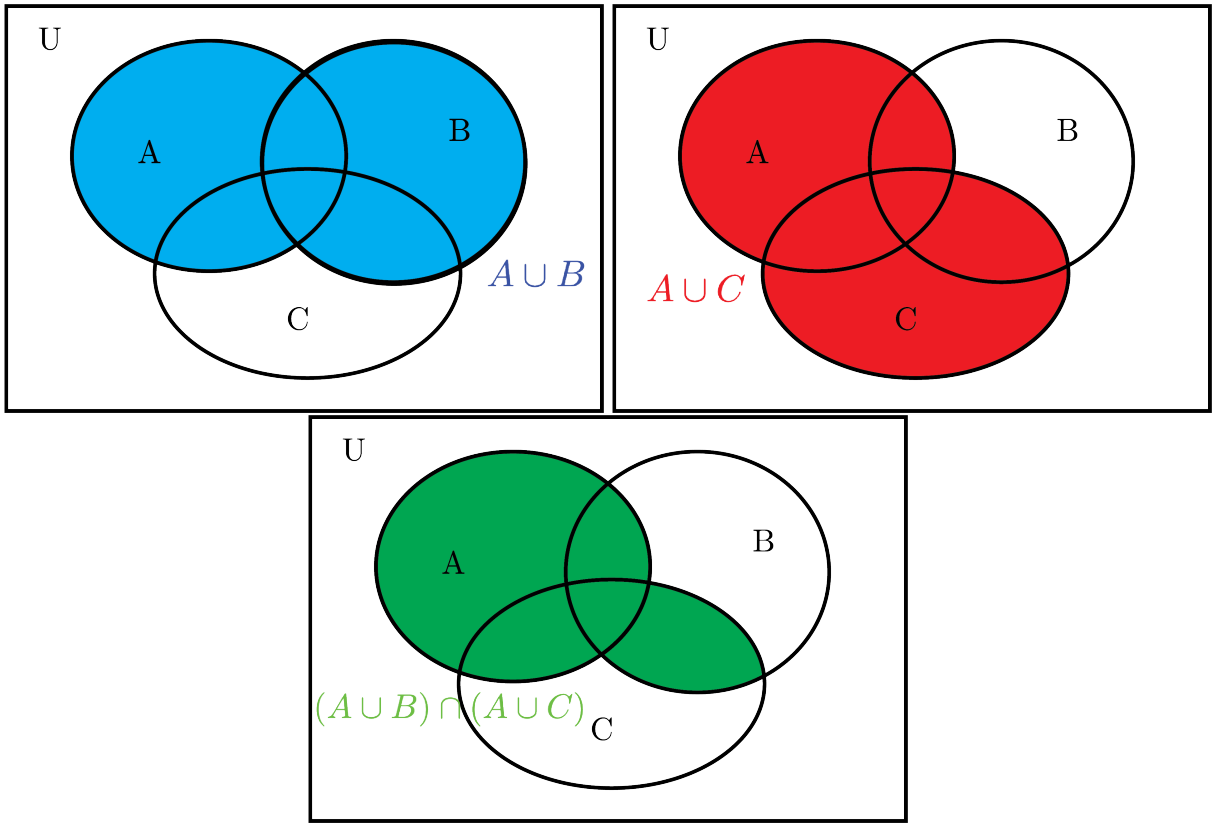
Consider the following conditional definition

$$\mathcal{S} = \{X | X \text{ is a set so that } X \notin X\}.$$

Note that most sets we have seen satisfy $X \notin X$, so if $\mathcal{S}$ is a set, then it is not empty. But then we have a paradox as follows. If $\mathcal{S} \in \mathcal{S}$, then by definition of $\mathcal{S}$, we must have $\mathcal{S} \notin \mathcal{S}$. On the other hand, if $\mathcal{S} \notin \mathcal{S}$, then $\mathcal{S} \in \mathcal{S}$. This is the so-called Russell's Paradox, named after British



(a) The set $A \cup (B \cap C)$



(b) The set $(A \cup B) \cap (A \cup C)$

Figure 3: Venn diagrams to illustrate $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

mathematician Bertrand Russell. In modern axiomatic set theory (e.g. Zermelo-Fraenkel-Choice "ZFC"), $\mathcal{S}$ is not a set, thus resolving the issue raised by the paradox.

2 Functions

Function is another fundamental concept in mathematics, used throughout different branches. You may be familiar with the concept from Calculus or Precalculus, and it is useful to have those examples at the back of your mind, but we are treating functions very generally.

Definition 2.1. Suppose X, Y are sets. A *function* (or a *mapping*) from X to Y is the assignment of a unique element of $y \in Y$ to each element of X. The set X is called the domain of f, and Y the codomain of f.

We write $f : X \to Y$ to denote a function with its domain and codomain. Suppose $f(x) \in Y$ is assigned to $x \in X$, then we write $x \mapsto f(x)$. Here $y = f(x)$ is called the *value* of f at $x \in X$, or the *image* of $x \in X$ under f.

There are many ways to specify a function. The easiest way is to list the value $f(x)$ for each x, say in a table. We can also think about f as connecting an element $x \in X$ to a point $y \in Y$, in such a way that exactly one line starts at each $x \in X$, while the number of lines ending at some $y \in Y$ may be zero, one, or more. We can also think of a function as assigning elements of $x \in X$ into boxes labelled by elements of Y. Each $x \in X$ can only be put into one box, but each box may contain zero, one, or more than one elements. We refer to the textbook for some pictorial representations of these ideas.

Two functions $f, g : X \to Y$ are *equal*, written as $f = g$, if $f(x) = g(x)$ for any $x \in X$. Note that they must have the same domain and codomain by default.

Image and graph. The *image* of a function $f : X \to Y$ denoted by $\mathrm{Im}(f)$, is the subset of codomain Y consisting of those elements which are values of f. That is

$$\mathrm{Im}(f) = \{f(x) | x \in X\}.$$

The *graph* of a function f, denoted by G_f, is the subset of the Cartesian product $X \times Y$ defined by

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

This agrees with the usual definition of graphs for functions defined over a subset of $\mathbb{R}$.

Examples of functions.

Example 2.2. Let $X = \{a, b, c\}$ and $Y = \{d, e\}$. Then there are 8 different functions from X to Y. We can list them in a table as follows:

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

We will talk more about counting functions in the next part.

Example 2.3 (Constant functions)**.** Given sets X, Y and $y_0 \in Y$, there is a *constant function* $C_{y_0} : X \to Y$ defined by

$$C_{y_0}(x) = y_0 \quad \forall x \in X.$$

Equivalently, C_{y_0} is the unique function from X to Y so that $\mathrm{Im}(C_{y_0}) = \{y_0\}$.

Example 2.4 (Identity functions)**.** Domain and codomain may be the same set for a function. Given a set X, the *identity function* $\mathrm{id}_X : X \to X$ is defined by

$$\mathrm{id}_X(x) = x \quad \forall x \in X.$$

Most common and efficient way of describing a function is to give a formula, as one would do for most functions in Calculus or Precalculus. It is important, however, to make clear what domain and codomain are.

Example 2.5. The following four functions are given by the same formula, but are not equal since they have different domains or codomains:

(i) $f_1 : \mathbb{R} \to \mathbb{R}$, $f_1(x) = x^2$;

(ii) $f_2 : \mathbb{R}^{\geq 0} \to \mathbb{R}$, $f_2(x) = x^2$;

(iii) $f_3 : \mathbb{R} \to \mathbb{R}^{\geq 0}$, $f_3(x) = x^2$;

(iv) $f_4 : \mathbb{R}^{\geq 0} \to \mathbb{R}^{\geq 0}$, $f_4(x) = x^2$.

They have different properties. For example, two real numbers in the domain of f_1 is mapped to 1, while only one number in the domain of f_2 is mapped to 1. We will make this distinction explicit in the next section.

Example 2.6. The function $g : [1, +\infty) \to \mathbb{R}$ defined by $g(x) = x^2$ has image $\mathrm{Im}(g) = [1, +\infty)$, as can be seen from its graph. On the other hand, the function $h : [-1, +\infty) \to \mathbb{R}$ defined by $h(x) = x^2$ has image $\mathrm{Im}(g) = [0, +\infty)$.

Example 2.7. In calculus, a common convention is the following: if a function defined by a formula in real numbers is given *without* domain or codomain, then the domain is taken to be the largest possible subset where the formula makes sense, and the codomain is taken to be $\mathbb{R}$. For example, under this convention, the function

$$f(x) = \frac{x^2 + x - 2}{x - 1}$$

is defined over domain $\mathbb{R} - \{1\}$, with codomain $\mathbb{R}$. However, we will usually specify the domain and codomain explicitly.

Note that when $x \neq 1$,

$$f(x) = \frac{x^2 + x - 2}{x - 1} = \frac{(x-1)(x+2)}{x-1} = x + 2.$$

So the same function may have different formulas. We may define an *extension* of f by assigning the value 3 to $x = 1$. The we get a function $f_2 : \mathbb{R} \to \mathbb{R}$ given by the formula $f_2(x) = x + 2$. Note that an extension needs not be continuous, so the following function is also an extension of f:

$$f_3(x) = \begin{cases} \dfrac{x^2 + x - 2}{x - 1} & \text{if } x \neq 1, \\ 19 & \text{if } x = 1. \end{cases}$$

Example 2.8 (Modulus function)**.** We have already seen an example of functions defined using different formulas for subsets of the domain: the absolute value, or the modulus function, is a function from $\mathbb{R}$ to $\mathbb{R}^{\geq 0}$ defined by

$$|x| = \begin{cases} x & \text{if } x \geq 0, \\ -x & \text{if } x \leq 0. \end{cases}$$

Note that the value for $x = 0$ is defined twice, but the formulas agree when $x = 0$, so it is still well-defined.

Example 2.9 (Restriction)**.** Given a function $f : X \to Y$ and a subset $A \subseteq X$, we can define a function $g : A \to Y$ by

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

This is called the *restriction* of f to A, which we denote by $f|_A$.

Example 2.10 (Inclusion)**.** Given a set X, let A be a subset. Then we can define the *inclusion of A into X*, denoted by $i_A : A \to X$ as follows:

$$i_A(a) = a \quad \forall a \in A.$$

In other words $i_A = \mathrm{id}_X|_A$.

Example 2.11 (Sequences)**.** A function $f : \mathbb{Z}^+ \to A$ is called a *sequence* in the set A. For example, we have the Fibonacci sequence $u(n) = u_n$ from Part I, which can be viewed as a function from $\mathbb{Z}^+$ to $\mathbb{Z}^+$.

Composition of functions. Let X, Y, Z be sets, and $f : X \to Y$ and $g : Y \to Z$ be functions. Then we can define a function $h : X \to Z$ by

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

This function is called the composite of f and g, denoted by $g \circ f$.

Example 2.12. Let $f(x) = x + 1$ and $g(x) = x^2$ be two functions from $\mathbb{R}$ to $\mathbb{R}$. Then

$$g \circ f(x) = (x + 1)^2 \text{ and } f \circ g(x) = x^2 + 1.$$

So $g \circ f \neq f \circ g$. In particular, composition is in general *not* commutative!

Example 2.13. Let $f : X \to Y$ be a function, and $A \subseteq X$. Then $f|_A = f \circ i_A$.

Example 2.14. Let $f(x) = x^2 + 1$ and $g(x) = 1/x$. Then the domain and codomain of f are both $\mathbb{R}$. On the other hand, the domain of g is $\mathbb{R} - \{0\}$ and its codomain is $\mathbb{R}$. Technically speaking $g \circ f$ is not defined, but since the image of f is $[1, +\infty)$, which is contained in the domain of g, $g(f(x))$ always makes sense. So we still define $g \circ f(x) = g(f(x))$ as a function from $\mathbb{R}$ to $\mathbb{R}$. As a matter of fact $g \circ f(x) = 1/(x^2 + 1)$.

Here are some properties of composition that can be checked from definition easily:

Proposition 2.15. *Suppose $f : X \to Y$, $g : Y \to Z$, $h : Z \to W$ are functions. Then*

(1) $(h \circ g) \circ f = h \circ (g \circ f) : X \to Z$. *In other words, composition is associative.*

(2) $f \circ \mathrm{id}_X = f = \mathrm{id}_Y \circ f : X \to Y$.

Image and preimage of sets. Let $f : X \to Y$ be a function. Given any subset A of X, its *image* under f is a subset of Y, defined by

$$f(A) = \{f(x)|x \in A\}.$$

In particular, we have $f(X) = \mathrm{Im}(f)$, and $f(A) = \mathrm{Im}(f|_A)$.

Given a subset B of Y, its *preimage* under f is a subset of X, defined by

$$f^{-1}(B) = \{x|f(x) \in B\}.$$

Note that if $B \cap \mathrm{Im}(f) = \emptyset$, then $f^{-1}(B) = \emptyset$. The preimage of a singleton $\{y\}$

$$f^{-1}(\{y\}) = \{x|f(x) = y\}$$

may contain none, one, or more elements. Any element in $f^{-1}(\{y\})$ is also called a preimage of y.

The following theorem relates unions, images and preimages.

Theorem 2.16. *Let $f : X \to Y$ be a function. Suppose $A, B \subseteq X$ and $C, D \subseteq Y$. Then*

(1) $f(A \cup B) = f(A) \cup f(B)$;

(2) $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$;

(3) $f(A \cap B) \subseteq f(A) \cap f(B)$;

(4) $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$.

Proof. We will give a complete proof of Part (1), and a partial proof of Part (2). The rest is left as an exercise.

For (1), let $y \in f(A \cup B)$. Then $y = f(x)$ for some $x \in A \cup B$. Now we have $x \in A$ or $x \in B$. For the former case, we then have $y = f(x) \in f(A)$. For the latter case, we have $y = f(x) \in f(B)$. Since $f(A) \subseteq f(A) \cup f(B)$ and $f(B) \subseteq f(A) \cup f(B)$, in both cases we conclude that $y \in f(A) \cup f(B)$. Thus $f(A \cup B) \subseteq f(A) \cup f(B)$, as desired.

Conversely, let $y \in f(A) \cup f(B)$. Then either $y \in f(A)$ or $y \in f(B)$. In the former case $y = f(x)$ for some $x \in A$. Since $A \subseteq A \cup B$, we conclude that $y \in f(A \cup B)$. In the latter case, we can similarly conclude $y \in f(A \cup B)$. Thus $f(A) \cup f(B) \subseteq f(A \cup B)$.

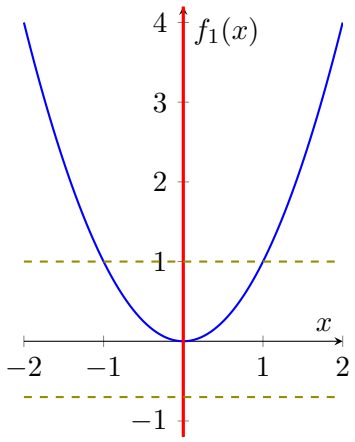
Therefore $f(A \cup B) = f(A) \cup f(B)$, as desired.

For (2), we only show $\subseteq$. Let $x \in f^{-1}(C \cup D)$. Then $f(x) \in C \cup D$. Hence either $f(x) \in C$ or $f(x) \in D$. For the former case we have $x \in f^{-1}(C)$. For the latter case we have $x \in f^{-1}(D)$. In both cases we have $x \in f^{-1}(C) \cup f^{-1}(D)$. Thus $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$ as desired. □

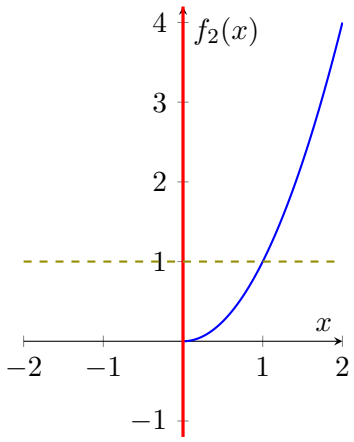
We also comment on Part (3). The two sets may not be equal like the other cases. Indeed, consider $f(x) = x^2$ from $\mathbb{R}$ to $\mathbb{R}$. If we set $A = [0, \infty)$ and $B = (-\infty, 0)$, then $A \cap B = \varnothing$. So $f(A \cap B) = \varnothing$. On the other hand $f(A) = [0, \infty)$ and $f(B) = (0, \infty)$ and so $f(A) \cap f(B) = (0, \infty)$.

3 Injection, surjection, bijection

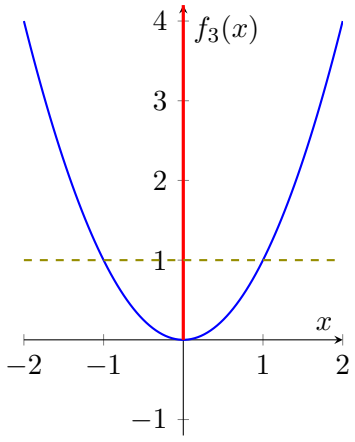
Recall the four functions defined in Example 2.5. We can draw their graphs as in Figure 4



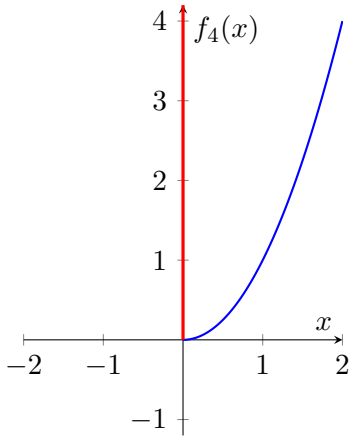
(a) The graph of f_1



(b) The graph of f_2



(c) The graph of f_3



(d) The graph of f_4

Figure 4: The graphs of f_1, f_2, f_3, f_4. The codomain of each function is colored red.

We first look at f_1 and f_2. If we draw a horizontal line at a point y in the image of either function, say at $y = 1$, we notice that the line intersects the graph of f_1 at two points, while it only intersects the graph of f_2 and one point. We now introduce a concept that precisely captures this difference.

Definition 3.1. A function $f : X \to Y$ is said to be *injective* (or *one-to-one*, or as a noun, an *injection*) if for any $y \in Y$, at most one $x \in X$ is mapped to y under f. More precisely, f is injective if

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

or equivalently, using contrapositive,

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

Another equivalent way of defining injectivity is that $f^{-1}(\{y\})$ is a singleton for any $y \in \mathrm{Im}(f)$. We show

Proposition 3.2. *The function $f_2 : \mathbb{R}^{\geq 0} \to \mathbb{R}$ is injective.*

Proof. Let $x_1, x_2 \in \mathbb{R}^{\geq 0}$. Suppose $f_2(x_1) = f_2(x_1)$. Then $x_1^2 = x_2^2$. Therefore we have $(x_1 - x_2)(x_1 + x_2) = 0$. Thus either $x_1 + x_2 = 0$, or $x_1 - x_2 = 0$. For the first case, since $x_1, x_2 \geq 0$, we must have $x_1 = x_2 = 0$. For the second case, we immediately have $x_1 = x_2$. So $x_1 = x_2$ in either case. This implies that f_2 is injective, as desired. □

Proposition 3.3. *The function $f_1 : \mathbb{R} \to \mathbb{R}$ is not injective.*

Proof. We find a counterexample violating the definition of injectivity: $f_1(1) = f_1(-1) = 1$ while $1 \neq -1$. □

We now look at f_1 and f_3. Neither is injective, but they are still different in the following sense. For any point y in the codomain, if I draw a horizontal line at y, it always intersects the graph of f_3. This is not true for f_1, since the horizontal line $y = -1$ does not intersect the graph of f_1 at all. We now introduce another concept capturing this difference.

Definition 3.4. A function $f : X \to Y$ is said to be *surjective* (or *onto*, or as a noun, a *surjection*) if for any $y \in Y$, at least one $x \in X$ is mapped to y under f. In other words, f is surjective if

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

An equivalent way of defining surjectivity is that $f^{-1}(\{y\}) \neq \emptyset$ for any $y \in Y$. We show

Proposition 3.5. *The function $f_3 : \mathbb{R} \to \mathbb{R}^{\geq 0}$ is surjective.*

Proof. Let $y \in \mathbb{R}^{\geq 0}$. Then $\sqrt{y} \in \mathbb{R}$ and we have $f_3(\sqrt{y}) = y$. Therefore f_3 is surjective. □

Proposition 3.6. *The function $f_1 : \mathbb{R} \to \mathbb{R}$ is not surjective.*

Proof. Indeed, take $y = -1$, then no $x \in \mathbb{R}$ satisfies $x^2 = y = -1$, since $x^2 \geq 0 > -1$ for any $x \in \mathbb{R}$. □

Finally we look at f_4. It is easy to check that it is both injective and surjective. We have

Definition 3.7. A function $f : X \to Y$ is said to be *bijective* (or *one-to-one and onto*, or as a noun, a *bijection*) if it is both injective and surjective. In other words, f is bijective if

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

Thus f_4 is bijective. A bijective function gives a one-to-one correspondence between elements of X and Y. It seems clear that we can define some kind of "inverse" of f, that reverses the effect of f.

To formalize this idea, we start with

Definition 3.8. Let $f : X \to Y$ be a function. f is said to be *invertible* if there exists a function $g : Y \to X$, so that

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

The function g is said to be an *inverse* of f.

Note by definition, if g is an inverse of f, then g is an inverse of f. We have

Theorem 3.9. *A function $f : X \to Y$ is bijective if and only if f is invertible. Moreover, if f is invertible, then it has a unique inverse.*

Proof. Suppose $f : X \to Y$ is bijective. Then we can define an inverse $g : Y \to X$ as follows. For any $y \in Y$, since $f : X \to Y$ is bijective, there exists a unique $x \in X$ so that $f(x) = y$. Define $g(y) = x$. Then it is clear that $g(f(x)) = g(y) = x$, and $f(g(y)) = f(x) = y$. So g as defined above is indeed an inverse of f.

Suppose now f is invertible, with inverse g. Then $f \circ g = \mathrm{id}_Y$ and $g \circ f = \mathrm{id}_X$. By Problem 4 Part 2, since id_X is injective, we conclude that f is injective. Similarly, by Problem 4 Part 3, since id_Y is surjective, we conclude that f is surjective. Hence f is bijective, as desired. □

Since a bijective function f's inverse is unique, we refer to it as *the* inverse of f, and denote it by f^{-1}.

Composition. The following results are given as exercises in homework, other than Part (2).

Theorem 3.10. *Let $f : X \to Y$ and $g : Y \to Z$ be functions.*

(1) *If both f and g are injective, then $g \circ f$ is also injective.*

(2) *If both f and g are surjective, then $g \circ f$ is also surjective.*

(3) *If both f and g are bijective, then $g \circ f$ is also bijective. Moreover, its inverse is given by $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

Proof. We only show Part (2). Let $z \in Z$. Since g is surjective, we can find $y \in Y$ so that $g(y) = z$. Since f is surjective, we can find $x \in X$ so that $f(x) = y$. Now $g(f(x)) = g(y) = z$, i.e. $g \circ f(x) = z$. Hence $g \circ f$ is surjective, as desired. □

Characteristic functions. Let X be a set, and $A \in \mathcal{P}(X)$. The *characteristic function* of A, denoted by χ_A, is a function from X to $\{0,1\}$ defined by

$$\chi_A(x) = \begin{cases} 1 & \text{if } x \in A, \\ 0 & \text{if } x \notin A. \end{cases}$$

For example $\chi_\varnothing$ is constantly 0, and χ_X is constantly 1. We can think of the assignment $A \mapsto \chi_A$ as a function χ from $\mathcal{P}(X)$ to the following set

$$\mathcal{F}(X) = \{f | f \text{ is a function from } X \text{ to } \{0,1\}\}.$$

That is, $\chi(A) = \chi_A$. We prove

Theorem 3.11. *The function $\chi : \mathcal{P}(X) \to \mathcal{F}(X)$ is a bijection.*

Proof. We prove this by constructing an inverse Φ for χ. Let $f : X \to \{0,1\}$ be a function. Let

$$\Phi(f) = f^{-1}(\{1\}).$$

First, note that $\Phi(\chi(A)) = \Phi(\chi_A) = \chi_A^{-1}(\{1\}) = A$, since $x \in A$ if and only if $\chi_A(x) = 1$. Also $\chi(\Phi(f)) = \chi(f^{-1}(\{1\})) = \chi_{f^{-1}(\{1\})} = f$, since $f(x) = 1$ if and only if $x \in f^{-1}(\{1\})$ if and only if $\chi_{f^{-1}(\{1\})}(x) = 1$.

Thus $\Phi \circ \chi = \mathrm{id}_{\mathcal{P}(X)}$ and $\chi \circ \Phi = \mathrm{id}_{\mathcal{F}(X)}$, as desired. □

MAT 511: Fundamental Concepts of Math

Written by: Yongquan Zhang

Last revisited: Summer 2024

Part III: Number systems and counting

In this third chapter of the course, we have two main goals. On the one hand, we want to introduce the idea of "cardinality" of a set X, which measures the size of X. While it is natural to say the size of a set with finitely many elements is exactly the number of elements it contains, this leads to problems when working with infinite sets. Is $\mathbb{Q}$ larger in size compared to $\mathbb{N}$? What about $\mathbb{R}$? As a matter of fact, we will encounter some rather paradoxical (at least counterintuitive) properties of cardinalities.

On the other hand, the idea of comparing "sizes" naturally leads to the notion of a standard set, or a reference set of a fixed size. Number systems were historically introduced for the purpose of counting, starting with natural numbers. We will briefly describe an axiomatic approach to natural numbers, usually attributed to Italian mathematician Giuseppe Peano. We will then construct the set of integers, rational numbers, and real numbers.

In the process, we will state and proof several results of the German mathematician Georg Cantor, whose ideas revolutsonarized set theory. In particular, we will describe Cantor's famous diagonal arguments on uncountability of real numbers.

1 Counting finite sets: theory and examples

In this section, we want to start with describing the size of sets with finitely many elements. Many results here are very intuitive. We first state some basic results intuitively, and then adopt a more formal approach to prove them at the end. This formal approach can be generalized to the setting of infinite sets.

1.1 Intuitive counting principles with examples

We start with an intuitive definition of "size" of a finite set. The *cardinality* of a finite set X is the number of elements it contains, denoted by $|X|$ or $\text{card}(X)$.

Example 1.1. Let $X = \{1, 2, 3, 4, 5\}$, then $|X| = 5$. More generally, let $\mathbb{N}_n$ be the set $\{1, 2, \ldots, n\}$. Then we have $|\mathbb{N}_n| = n$.

Example 1.2. Consider the set $X = \{n \in \mathbb{N} | n \text{ is an even and less or equal to } 10\}$. Then $X = \{2, 4, 6, 8, 10\}$, so $|X| = 5$.

Example 1.3. Consider the set

$$Y = \{n \in \mathbb{N} | \text{ There exist positive integers } a, b, c \text{ such that } a^n + b^n = c^n\}.$$

Clearly $1 \in Y$, and it is not hard to see $2 \in Y$ (e.g. $3^2 + 4^2 = 5^2$). The fact that $3, 4 \notin Y$ can be proved in elementary ways, understandable to students in this class. However, the fact that $n \notin Y$ whenever $n \geq 3$ is extremely hard, and is known as the Fermat last theorem, settled by A. Wiles using works of K. Ribet and many others. Assuming this, we have $|Y| = 2$.

These two examples showcase the extreme variability in difficulty of counting problems.

Example 1.4. Let $X = \{1, 2, 3\}$. Elements of the power set of X can be listed:

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

So $|\mathcal{P}(X)| = 8$. We will determine the number of subsets of a general finite set in later section.

We now start to introduce some counting principles. The key part of all of them is Theorem 1.5, the additive principle. However, defining the cardinality of a set requires some work. This is addressed in Section 1.2.

Theorem 1.5 (Additive principle)**.** *Let X, Y be finite sets. If X, Y are disjoint, then $X \cup Y$ is a finite set, and*

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

The proof of Theorem 1.5, which we will refer to as the additive principle, will be presented in Section 1.2 (after we properly define the cardinality of a set). However, many counting principles follow from it. We will illustrate some of them.

By using induction and the additive principle, we can show:

Theorem 1.6 (Additive principle, general version)**.** *Suppose n is a natural number. Let $X_1, \ldots, X_n$ be finite sets. If they are pairwise disjoint (that is, $X_i \cap X_j = \emptyset$ when $i \neq j$), then $X_1 \cup X_2 \cup \cdots \cup X$ is a finite set, and*

$$|X_1 \cup X_2 \cup \cdots \cup X_n| = |X_1| + |X_2| + \cdots + |X_n|.$$

Proof. The base case $n = 1$ is trivial. Suppose the statement holds for $n = k$. When $n = k + 1$, we are given $k + 1$ sets $X_1, \ldots, X_k, X_{k+1}$. Since $X_i \cap X_{k+1} = \emptyset$ when $1 \leq i \leq k$, we conclude that

$$(X_1 \cup \cdots \cup X_k) \cap X_{k+1} = (X_1 \cap X_{k+1}) \cup \cdots \cup (X_k \cap X_{k+1}) = \emptyset.$$

By inductive hypothesis, $X_1 \cup \cdots \cup X_k$ is a finite set, and so by additive principle $(X_1 \cup \cdots \cup X_k) \cup X_{k+1}$ is also a finite set, and moreover

$$|X_1 \cup X_2 \cup \cdots \cup X_n| = |X_1 \cup \cdots \cup X_k| + |X_{k+1}| = |X_1| + \cdots + |X_k| + |X_{k+1}|.$$

Hence the statement is also true when $n = k + 1$, as desired.

By induction, the original statement holds for any natural number n. □

As a consequence we have the following multiplicative principle:

Theorem 1.7 (Multiplicative principle)**.** *Let X, Y be finite sets. Then $X \times Y$ is also finite, and*

$$|X \times Y| = |X| \cdot |Y|.$$

Proof. If either X or Y is empty, then $X \times Y$ is empty. Both sides of the equality then equal zero. Suppose now X and Y are nonempty. Assume $|X| = n$ and $|Y| = m$. Write

$$X = \{x_1, \ldots, x_n\}.$$

Then

$$X \times Y = \{x_1\} \times Y \cup \cdots \cup \{x_n\} \times Y.$$

Each $\{x_i\} \times Y$ contains m elements, and clearly $(\{x_i\} \times Y) \cap (\{x_j\} \times Y) = \emptyset$ when $i \neq j$. Applying additive principle, we have $|X \times Y| = mn$, as desired. □

Here is an illustrating example.

Example 1.8. Let X be the set of *ordered* pairs of distinct positive integers (x, y) such that $x, y \leq 9$. Note that $X \subseteq \mathbb{N}_9 \times \mathbb{N}_9$. Moreover

$$\mathbb{N}_9 \times \mathbb{N}_9 = X \cup \{(x, y) \in \mathbb{N}_9 \times \mathbb{N}_9 | x = y\}.$$

By multiplicative principle $|\mathbb{N}_9 \times \mathbb{N}_9| = 81$. The set $Y = \{(x, y) \in \mathbb{N}_9 \times \mathbb{N}_9 | x = y\}$ clearly has 9 elements. By additive principle, $|X| + |Y| = 81$ and so $|X| = 81 - 9 = 72$.

Finally, we can use additive principle to prove the following very useful principle:

Theorem 1.9 (Inclusion-exclusion principle)**.** *Let X and Y be finite sets. Then $X \cup Y$ is finite, and*

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

Proof. Note that we have proved in Part II that

$$X \cup Y = (X - Y) \cup (Y - X) \cup (X \cap Y),$$

and more over $X - Y$, $Y - X$, and $X \cap Y$ are pairwise disjoint. Applying additive principle, we have

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

On the other hand, $X = (X - Y) \cup (X \cap Y)$ and so $|X| = |X - Y| + |X \cap Y|$. Similarly $|Y| = |Y - X| + |X \cap Y|$. Therefore

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

as desired. □

Applying this multiple times, we have the inclusion-exclusion principle for three sets:

Theorem 1.10 (Inclusion-exclusion principle for three sets)**.** *Let X, Y, Z be finite sets. Then $X \cup Y \cup Z$ is finite, and*

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

Using induction, we can show a more general version of inclusion-exclusion. We refer to the text book for the exact formula.

Example 1.11. In a room of 50 people, 30 speak English, 20 speak Spanish, and 25 speak Italian. 10 speak both English and Spanish, 10 speak both English and Italian, and 10 speak both Spanish and Italian. If everyone present speaks at least one of these three languages, we calculate the number of trilingual people using inclusion-exclusion.

Let E, S, I be the set of people who speak English, Spanish, and Italian respectively. Then $|E \cup S \cup I| = 50$, $|E| = 30$, $|S| = 20$, $|I| = 25$, and $|E \cap S| = |S \cap I| = |I \cap E| = 10$. By inclusion-exclusion

$$\begin{aligned}|E \cap S \cap I| &= |E \cup S \cup I| - |E| - |S| - |I| + |E \cap S| + |S \cap I| + |I \cap E| \\ &= 50 - 30 - 20 - 25 + 10 + 10 + 10 = 5\end{aligned}$$

So there are 5 trilingual people in the room.

1.2 A formal approach to counting

When we count elements in a set X, we point our imaginary finger at each object, and say "1, 2, 3, ..." out aloud. Mathematically speaking, we are constructing a function from the set $\{1, 2, 3, \ldots, n\}$ to X. We don't want to count any object more than once, so this function needs to be injective; we also want to count everything, so this function needs to be surjective. This underlines the idea of the following definition:

Definition 1.12. For any natural number n, let $\mathbb{N}_n = \{1, 2, \ldots, n\}$. We say a nonempty set X *has cardinality* n if there exists a bijection

$$f : \mathbb{N}_n \to X,$$

and write $|X| = n$. The cardinality of the empty set $\emptyset$, by definition, is 0.

A set is said to be *finite* if it has cardinality n for some integer $n \geq 0$, and infinite otherwise.

While it may seem frivolous and obvious, we want to make the remark that it is not immediately clear (in the mathematical sense) that cardinality is *well-defined*. A well-defined notion should be clear, precise, and unambiguous. Here, it is not yet trivially obvious that a set cannot have two different cardinalities. In other words, *a priori* there might exist two bijections $f : \mathbb{N}_n \to X$ and $g : \mathbb{N}_m \to X$ with $m \neq n$. The first goal of this section is to show that this cannot happen.

We start with the following lemma:

Lemma 1.13. *If there exists an injection $f : \mathbb{N}_m \to \mathbb{N}_n$, then $m \leq n$.*

Proof. We prove this by induction on n. For the base case, suppose $f : \mathbb{N}_m \to \mathbb{N}_1$ is an injection. Then we must have $m = 1$. Otherwise, $1, 2 \in \mathbb{N}_m$, and $f(1) = f(2) = 1$, a contradiction.

Suppose the statement holds for $n = k$. Let $f : \mathbb{N}_m \to \mathbb{N}_{k+1}$ be an injection. First note that if $m = 1$ then $m \leq k < k + 1$ holds trivially. So we may assume from now on $m \geq 2$.

If $k + 1 \notin \mathrm{Im}(f)$, then we may treat f as a function from $\mathbb{N}_m$ to $\mathbb{N}_k$. By inductive hypothesis, $m \leq k < k + 1$.

Otherwise $k + 1 \in \mathrm{Im}(f)$. Suppose $f(t) = k + 1$, for some $t \in \mathbb{N}_m$. Define a function from $g : \mathbb{N}_{m-1} \to \mathbb{N}_k$ as follows:

$$g(i) = \begin{cases} f(i) & i < t, \\ f(i+1) & i \geq t. \end{cases}$$

In other words, g is the same as f, except it "skips" the value at t. Note that since f is injective, g is injective as well. By inductive hypothesis, $m - 1 \leq k$, and thus $m \leq k + 1$, as desired.

By induction, the statement holds for any natural number n. □

Using this lemma, we can then show the cardinality is well-defined. In other words:

Proposition 1.14. *Let X be a set. If $f : \mathbb{N}_m \to X$ and $g : \mathbb{N}_n \to X$ are both bijections, then $m = n$.*

Proof. Note that $g^{-1} \circ f : \mathbb{N}_m \to \mathbb{N}_n$ is a bijection. In particular, it is injective. By the previous lemma, $m \leq n$. The same argument applies to $f^{-1} \circ g : \mathbb{N}_n \to \mathbb{N}_m$. So $n \leq m$. Therefore we have $m = n$ as desired. □

In Lemma 1.13, we focused on injective functions. Similar results can be proved for surjections:

Proposition 1.15. *If $f : \mathbb{N}_m \to \mathbb{N}_n$ is a surjection, then $m \geq n$.*

Proof. We can mimic the proof of Lemma 1.13 with induction, but here is another way, utilizing a very useful trick: given any surjection $f : X \to Y$ (X, Y need not be finite!), we can construct an injection $g : Y \to X$ so that $f \circ g = \mathrm{id}_Y$. Indeed, for each $y \in Y$, the set $f^{-1}(\{y\})$ is nonempty by surjectivity of f. Choose any element $x_y \in f^{-1}(\{y\})$ and define $g(y) = x_y$. Now $f \circ g(y) = f(g(y)) = f(x_y) = y$. Clearly g is injective. Indeed, if $g(y_1) = g(y_2)$, then $f \circ g(y_1) = f \circ g(y_2)$ and hence $y_1 = y_2$.

Now we can apply this trick to the surjection given in the proposition, and obtain an injection $g : \mathbb{N}_n \to \mathbb{N}_m$. By Lemma 1.13, we have $n \leq m$, as desired. □

Let us record the trick used in the proof above as a lemma. The proof is contained in the argument above.

Lemma 1.16. *Let $f : X \to Y$ be a surjective function. Then there exists an injective function $g : Y \to X$ so that $f \circ g = \mathrm{id}_Y$.*

Theorem 1.17. *Let X, Y be nonempty finite sets.*

(1) *There exists an injection $f : X \to Y$ if and only if $|X| \leq |Y|$.*

(2) *There exists a surjection $f : X \to Y$ if and only if $|X| \geq |Y|$.*

(3) *There exists a bijection $f : X \to Y$ if and only if $|X| = |Y|$.*

Proof. We show (3) first. Suppose $|X| = |Y| = n$. Then there exist bijections $g_1 : \mathbb{N}_n \to X$ and $g_2 : \mathbb{N}_n \to Y$. Now $g_2 \circ g_1 : X \to Y$ is a bijection as well.

Conversely, suppose we have a bijection $f : X \to Y$. Let $|X| = n$. Then there exists a bijection $g : \mathbb{N}_n \to X$. Now $f \circ g : \mathbb{N}_n \to Y$ is also a bijection, and hence $|Y| = n$.

We prove (1) next. Suppose $m = |X| \leq |Y| = n$. Then there exist bijections $g_1 : \mathbb{N}_m \to X$ and $g_2 : \mathbb{N}_n \to Y$. On the other hand, $\mathbb{N}_m \subseteq \mathbb{N}_n$, so the inclusion $i : \mathbb{N}_m \to \mathbb{N}_n$ is an injection. Now $g_2 \circ i \circ g_1^{-1} : X \to Y$ is also an injection, as desired.

Conversely, suppose there exists an injection $f : X \to Y$. Again let $m = |X|$ and $|Y| = n$. Then there exist bijections $g_1 : \mathbb{N}_m \to X$ and $g_2 : \mathbb{N}_n \to Y$. Then we have $g_2^{-1} \circ f \circ g_1 : \mathbb{N}_m \to \mathbb{N}_n$ is also an injection. By Lemma 1.13, we conclude that $m \leq n$.

Part (2) is left as an exercise. □

We can also now prove the additive principle (Theorem 1.5).

Proof of Theorem 1.5. If either X or Y is empty, then the equality holds trivially. Otherwise, since X and Y are finite sets, there exist bijections $f : \mathbb{N}_m \to X$ and $g : \mathbb{N}_n \to Y$ where $m = |X|$ and $n = |Y|$. Consider the following function $h : \mathbb{N}_{m+n} \to X \cup Y$,

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

Clearly h is surjective since f and g are. Moreover, h is injective. Indeed, suppose $h(i) = h(j)$. Then since $X \cap Y = \emptyset$, we must have either both $i, j \leq m$ or both $i, j \geq m+1$. Then $i = j$ by injectivity of f or g. □

In fact, a stronger statement than the forward implication of Part (1) is true,

Lemma 1.18. *Suppose Y is a finite set, and $f : X \to Y$ is an injection. Then X is finite and $|X| \leq |Y|$.*

This can be proved by induction on $|Y|$, similar to the proof of Lemma 1.13. An easy corollary of this lemma is

Corollary 1.19. *Let Y be a finite set. Suppose $X \subseteq Y$. Then X is a finite set and $|X| \leq |Y|$. Moreover, $|X| = |Y|$ if and only if $X = Y$.*

Proof. If $Y = \emptyset$, then $X = \emptyset$ and hence $|X| = 0 = |Y|$. Otherwise, the inclusion $i_X : X \to Y$ is an injection. So by the lemma above, $|X| \leq |Y|$.

For the "moreover" statement, note that if $X = Y$, then clearly $|X| = |Y|$. On the other hand, if $X \subsetneq Y$, then $Y - X$ is nonempty, and hence $|Y - X| \geq 1$. By additive principle, $|Y| = |X| + |Y - X|$, and hence $|X| < |Y|$. □

We also have the corresponding statement for surjection, which we leave as an exercise.

Proposition 1.20. *Suppose X is a nonempty finite set. If there exists a surjection $f : X \to Y$ then Y is a finite set, and $|X| \geq |Y|$.*

2 Properties of finite sets

In this section, we introduce some more properties of finite sets.

We first remark that the "moreover" part in Corollary 1.19 only applies to finite sets. Indeed, for any infinite set, there always exists a proper subset with the same cardinality, as we will show later.

2.1 The pigeonhole principle

Recall that given two nonempty finite set X and Y, if there exists an injection $f : X \to Y$, then $|X| \leq |Y|$. The contrapositive of this statement is

Theorem 2.1 (Pigeonhole principle)**.** *Let X, Y be finite sets. If $|X| > |Y|$, then any function $f : X \to Y$ is not injective. That is, there exists $x_1, x_2 \in X$ such that $f(x_1) = f(x_2)$.*

The idea comes from putting pigeons (or letters) into pigeonholes (or letterboxes). If there are more pigeons than holes, then at least two pigeons have to be in the same hole. Here are some interesting applications of this principle:

Example 2.2. (1) In a room of 13 people, at least 2 share the same birth month. Indeed, there are only 12 months but 13 people, so by pigeonhole principle, at least two have the same birth month.

(2) Similarly in a room of 367 people, at least 2 share the same birthday.

Example 2.3. In a room of n people, if $n \geq 2$, then at least two have the same number of friends in the room. Here we make two assumptions: no one is a friend of themself, and friendship is symmetric (if A is a friend of B, then B is a friend of A).

Indeed, consider the function f that assigns each person in the room their number of friends in the room. Then f has values in $\{0, 1, 2, \ldots, n-1\}$. Note that 0 and $n-1$ cannot both be in $\mathrm{Im}(f)$: if someone has no friend in the room, then no one else can have everyone as friend. So $|\mathrm{Im}(f)| \leq n-1$ while its domain contains n elements. Therefore by pigeonhole principle, at least two people have the same number of friends in the room.

Example 2.4. Let $n \geq 1$ be a natural number. Then for any $(n+1)$ distinct numbers $x_1, \ldots, x_{n+1}$ between 1 and $2n$, two of them add up to exactly $2n+1$.

Indeed, integers between 1 and $2n$ can be divided into n pairs: $\{1, 2n\}, \{2, 2n-1\}, \ldots, \{n, n+1\}$. If we choose $n+1$ distinct numbers, then two of them have to come from the same pair. Note that the two numbers in the same pair add up to $2n+1$, so we have the desired result.

2.2 Surjection and bijection

Similarly we have the following result:

Theorem 2.5. *Let X, Y be nonempty finite sets. If $|X| < |Y|$, then any function $f : X \to Y$ is not surjective.*

Finally, if X, Y are finite sets with $|X| = |Y|$, to show that a function is bijective we only need to show that it is either injective or surjective (this property is **not** true for infinite sets).

Theorem 2.6. *Let X, Y be finite sets. Assume $|X| = |Y|$. Then a function $f : X \to Y$ is injective if and only if it is surjective.*

2.3 Finite sets of real numbers

Let $A \subset \mathbb{R}$ be a nonempty subset of real numbers. Then we say b is a *minimum element* of A if

- $b \in A$; and
- $\forall a \in A, a \geq b$.

We write $b = \min A$. Similarly, we say c is a *maximum element* of A if

- $c \in A$; and
- $\forall a \in A, a \leq c$.

Let us see some examples.

Example 2.7. The set $A = \{-1, -18, 2, 3, 7\}$ has maximum 7 and minimum -18.

Example 2.8. The set of natural numbers has minimum 1, but no maximum, since for any $n \in \mathbb{N}$, we can always find $n + 1 > n$.

Example 2.9. Every nonempty subset of natural numbers contains a minimum element. This is the so-called *well-ordering principle*, and one can show that this principle is equivalent to the induction principle.

Example 2.10. The set of positive reals $\mathbb{R}^+$ contains no maximum nor minimum. In fact, for any $a \in \mathbb{R}^+$, we can always find a larger one (e.g. $2a$), and a smaller one (e.g. $a/2$).

These examples suggest that maximum and minimum may not exist. But if they do, they are unique. Indeed, if c_1 and c_2 are both maximum of the set A, then we immediately have $c_1 \leq c_2$ and $c_2 \leq c_1$ and thus $c_1 = c_2$.

We have the following result regarding finite sets:

Proposition 2.11. *Let A be a finite nonempty subset of real numbers. Then A has a maximum element and a minimum element.*

Proof. We only show the existence of maximum element. The existence of minimum element is entirely similar.

We prove the result by induction on $|A| = n$. The base case is $n = 1$. In this case, the set $A = \{x\}$ is a singleton, and x is its maximum element.

Now suppose as inductive hypothesis that any set of cardinality k has a maximum element. Let A be a set of cardinality $k + 1$. Write $A = \{a_1, \ldots, a_k, a_{k+1}\}$. and set $A' = \{a_1, \ldots, a_k\}$. Since $|A'| = k$, by inductive hypothesis, it has a maximum element $\max A'$. If $a_{k+1} \leq \max A'$, then $\max A = \max A'$. If $a_{k+1} > \max A'$ then $\max A = a_{k+1}$. So in either case, A contains a maximum element, as desired.

By induction, the statement holds for any finite set. □

2.4 Greatest common divisor

Recall that given integers a, d, where $d \neq 0$, if there exists an integer q such that $a = dq$, we say a is a *multiple* of d, and d is a *divisor* (or a factor) of a.

First note that every nonzero integer is a divisor of 0. Suppose $a \neq 0$. Then if $a = dq$, we must have $q \neq 0$ as well. In particular $|q| \geq 1$. Since $|a| = |d| \cdot |q| \geq |d|$, we conclude $-|a| \leq d \leq |a|$. Define the set of divisors

$$D(a) = \{d \in \mathbb{Z} | d \text{ is a divisor of } a\}.$$

Then the argument above implies that $D(a)$ is a finite set when $a \neq 0$.

Here are some properties of divisors:

- For any integer a, $1 \in D(a)$ and $-1 \in D(a)$.
- For any nonzero integer a, $a \in D(a)$ and $-a \in D(a)$.
- For any nonzero integer a, $\max D(a) = |a|$, and $\min D(a) = -|a|$.

We say a is a *prime number* if $a > 1$ and $D(a) = \{-a, -1, 1, a\}$.

Given integers a, b, consider the set $D(a) \cap D(b)$. If a, b are not both zero, then $D(a) \cap D(b)$ is a finite set.

Definition 2.12. Suppose two integers a, b are not both zero. The maximum element $\max(D(a) \cap D(b))$ is called the *greatest common divisor* (or the highest common factor) of a and b. That is, the greatest common divisor d of a and b satisfies:

- d is a common divisor of both a and b;
- Suppose c is another common divisor of a and b, then $c \leq d$.

We write $d = \gcd(a, b)$, or simply $d = (a, b)$. Two integers, not both zero, are said to be *coprime* (or relatively prime), if their greatest common divisor is 1.

Example 2.13. The set of divisors of 15 is $D(15) = \{-15, -5, -3, -1, 1, 3, 5, 15\}$, and the set of divisors of 12 is $D(12) = \{-12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12\}$. Therefore $D(15) \cap D(12) = \{-3, -1, 1, 3\}$. Thus $\gcd(15, 12) = 3$.

The set of divisors of 26 is $D(26) = \{-26, -13, -2, -1, 1, 2, 13, 26\}$. So $D(26) \cap D(15) = \{-1, 1\}$. Thus $\gcd(26, 15) = 1$. So 15 and 26 are relatively prime.

We will introduce a simpler way to find divisors and common divisors of two integers in later parts.

3 Counting functions and subsets

In this section, we apply the counting principles covered in previous sections to determine the cardinality of certain sets of functions and subsets. We will also showcase a useful way of proving certain identities, by "counting the same set twice".

3.1 Counting functions

Let X and Y be nonempty finite sets. Let $\mathrm{Fun}(X, Y)$ be the set of functions from X to Y. That is, $\mathrm{Fun}(X, Y)$ consists of functions $f : X \to Y$. Our first counting result is the following:

Theorem 3.1. *The cardinality of* $\mathrm{Fun}(X, Y)$ *is given by* $|Y|^{|X|}$.

Proof. Let $|X| = m$ and $|Y| = n$. We prove the result by induction on m.

For the base case, when $|X| = 1$, then X is a singleton, say $X = \{x\}$. Then a function $f \in \mathrm{Fun}(X, Y)$ is determined by its value $f(x)$ at x. Define a function $\Phi : \mathrm{Fun}(\{x\}, Y) \to Y$ as follows:

$$\Phi(f) = f(x).$$

Clearly Φ is injective. Indeed, if $\Phi(f_1) = \Phi(f_2)$, we have $f_1(x) = f_2(x)$. Since a function from X to Y is determined by its value at x, we conclude that $f_1 = f_2$, this implies that Φ is injective. Also Φ is surjective. Indeed, for any $y \in Y$, consider the function $f : X \to Y$ defined by $f(x) = y$. Then $\Phi(f) = y$ as desired. So Φ is indeed surjective. Therefore Φ is bijective.

Hence $|\mathrm{Fun}(\{x\}, Y)| = |Y| = n$, as desired.

Now assume that for any set X with $|X| = k$, the statement holds for any nonempty set Y. Assume now $|X| = k + 1$. Choose $a \in X$, and let $X' = X - \{a\}$. Then $|X'| = k$ by additive principle. For any $y \in Y$, we can define the following subset of $\mathrm{Fun}(X, Y)$:

$$\mathrm{Fun}_y(X, Y) = \{f : X \to Y | f(a) = y\}.$$

Clearly $\mathrm{Fun}(X, Y) = \bigcup_{y \in Y} \mathrm{Fun}_y(X, Y)$. Moreover, $\mathrm{Fun}_y(X, Y) \cap \mathrm{Fun}_{y'}(X, Y) = \emptyset$ when $y \neq y'$. So

$$|\mathrm{Fun}(X, Y)| = \sum_{y \in Y} |\mathrm{Fun}_y(X, Y)|.$$

Finally, we have following function Ψ from $\mathrm{Fun}(X', Y)$ to $\mathrm{Fun}_y(X, Y)$. For any $f : X' \to Y$, define $g = \Psi(f)$ as follows:

$$g(x) = \begin{cases} f(x) & \text{if } x \neq a; \\ y & \text{if } x = a. \end{cases}$$

Again, it is easy to see that Ψ is a bijection. So $|\mathrm{Fun}_y(X, Y)| = |\mathrm{Fun}(X', Y)|$, which by inductive hypothesis, is $|Y|^{|X'|} = n^k$. Therefore

$$|\mathrm{Fun}(X, Y)| = \sum_{y \in Y} |\mathrm{Fun}_y(X, Y)| = \sum_{y \in Y} n^k = |Y| \cdot n^k = n \cdot n^k = n^{k+1}.$$

So the statement also holds. By induction, we have the desired result. □

Now consider the set of injective functions from X to Y.

$$\mathrm{Inj}(X, Y) = \{f : X \to Y | f \text{ is injective}\}.$$

Clearly by the Pigeonhole principle, $|\mathrm{Inj}(X, Y)| = 0$ if $|X| > |Y|$. Using a similar inductive argument as above, we can prove:

Theorem 3.2. *Let $|X| = m$ and $|Y| = n$. Then the cardinality of $|\mathrm{Inj}(X, Y)|$ is given by $n(n - 1) \cdots (n - m + 1)$.*

Proof. We again prove by induction on m. The base case is exactly the same as the base case in the previous theorem. In the inductive step, when $|X| = k + 1$, again choose $a \in X$ set $X' = X - \{a\}$. For any $y \in Y$, consider the following subset of $\mathrm{Inj}(X, Y)$:

$$\mathrm{Inj}_y(X, Y) = \{f : X \to Y | f \text{ is injective}, f(a) = y\}.$$

Clearly $\mathrm{Inj}(X, Y) = \bigcup_{y \in Y} \mathrm{Inj}_y(X, Y)$. Moreover, $\mathrm{Inj}_y(X, Y) \cap \mathrm{Inj}_{y'}(X, Y) = \emptyset$ when $y \neq y'$. So

$$|\mathrm{Inj}(X, Y)| = \sum_{y \in Y} |\mathrm{Inj}_y(X, Y)|.$$

We can define a function Ψ from $\mathrm{Inj}(X', Y - \{y\})$ to $\mathrm{Inj}_y(X, Y)$. For any $f : X' \to Y - \{y\}$, define $g = \Psi(f)$ as follows:

$$g(x) = \begin{cases} f(x) & \text{if } x \neq a; \\ y & \text{if } x = a. \end{cases}$$

Again, it is easy to see that Ψ is a bijection. So $|\operatorname{Inj}_y(X,Y)| = |\operatorname{Inj}(X', Y - \{y\})|$, which by inductive hypothesis, is $(n-1)\cdots(n-k)$. Therefore

$$|\operatorname{Inj}(X,Y)| = \sum_{y\in Y} |\operatorname{Inj}_y(X,Y)| = \sum_{y\in Y}((n-1)\cdots(n-k)) = |Y|\cdot(n-1)\cdots(n-k) = n(n-1)\cdots(n-k).$$

So the statement also holds. By induction, we have the desired result. □

The product $n(n-1)\cdots(n-m+1)$ is called a *falling factorial*; there are m factors in the product. We sometimes use the notation

$$(n)_m := n(n-1)\cdots(n-m+1).$$

Note that when $m > n$, then 0 appears as a factor, and so $(n)_m = 0$. This agrees with Pigeonhole principle.

Notice that when $n = m$, $(n)_m = n(n-1)\cdots 1 = n!$. When $n > m$, we also have

$$(n)_m = n(n-1)\cdots(n-m+1) = \frac{n(n-1)\cdots(n-m+1)(n-m)\cdots 1}{(n-m)\cdots 1} = \frac{n!}{(n-m)!}.$$

This formula still works when $n = m$ since $0! = 1$.

Finally, assume $|X| = |Y|$. Then a function $f : X \to Y$ is bijective if and only if it is injective by Theorem 2.6. Let $\operatorname{Bij}(X,Y)$ be the set of bijections from X to Y. We thus have the following counting result:

Corollary 3.3. *Suppose $|X| = |Y| = n$. Then $|\operatorname{Bij}(X,Y)| = |\operatorname{Inj}(X,Y)| = n!$.*

If $|X| = n$, a bijection $f : \mathbb{N}_n \to X$ is sometimes called a *permutation* of X, since it gives a ordering of the elements in X. The corollary above thus implies that there are $n!$ permutations of X.

3.2 Counting subsets

Let X be a finite set. Recall that its power set $\mathcal{P}(X)$ is the set of all subsets of X. For any subset $A \subseteq X$, we have its *characteristic function* $\chi_A : X \to \{0,1\}$ (see Part II for details). We have shown that the function $\chi : \mathcal{P}(X) \to \operatorname{Fun}(X, \{0,1\})$ defined by $\chi(A) = \chi_A$ is a bijection. As a consequence, we have

Corollary 3.4. *Let X be a finite set of cardinality n. Then $|\mathcal{P}(X)| = 2^n$.*

Proof. If $X = \emptyset$, then $\mathcal{P}(X) = \{\emptyset\}$. Thus $|\mathcal{P}(X)| = 1 = 2^0$ as desired. Otherwise, since χ is a bijection, we have by Theorem 3.1,

$$|\mathcal{P}(X)| = |\operatorname{Fun}(X, \{0,1\})| = 2^{|X|},$$

as desired. □

Next we want to count the number of elements in some subset of $\mathcal{P}(X)$. Define

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

that is, $\mathcal{P}_r(X)$ consists of subsets of X of cardinality exactly r. Note that the cardinality $|\mathcal{P}_r(X)|$ only depends on r and $n = |X|$. Indeed, if Y is another set with $|Y| = n$, then there exists a bijection $f : X \to Y$. For any $A \in \mathcal{P}_r(X)$, we have $f(A) \in \mathcal{P}_r(Y)$; similarly for any $B \in \mathcal{P}_r(Y)$, we have $f^{-1}(B) \in \mathcal{P}_r(X)$. Therefore $|\mathcal{P}_r(X)| = |\mathcal{P}_r(Y)|$.

Definition 3.5. The *binomial coefficient* $\binom{n}{r}$ is defined to be the cardinality of $\mathcal{P}_r(X)$, where X is a set of cardinality n.

We read $\binom{n}{r}$ as "n choose r". We have the following properties of binomial coefficients:

Proposition 3.6. *Let n be a nonnegative integer. We have*

(1) $\binom{n}{r} = 0$ *for any integer $r > n$;*

(2) $\binom{n}{0} = \binom{n}{n} = 1$, *and* $\binom{n}{1} = n$;

(3) $\binom{n}{r} = \binom{n}{n-r}$ *for any integer $r = 0, 1, \ldots, n$.*

Proof. Let X be a finite set of cardinality n. For (1), no subset of X has cardinality $> n$.

For (2), the only subset with cardinality 0 is the empty set. So $\binom{n}{0} = 1$. Similarly $\mathcal{P}_n(X) = \{X\}$, since any proper subset A of X has $|A| < |X| = n$. Therefore $\binom{n}{n} = |\mathcal{P}_n(X)| = 1$. Finally, $\mathcal{P}_1(X)$ consists of singletons, so $\binom{n}{n} = |\mathcal{P}_1(X)| = |X| = n$.

For (3), viewing X as the universal set, then taking complement $A \mapsto A^c$ gives a bijection between $\mathcal{P}_r(X)$ and $\mathcal{P}_{n-r}(X)$. (The inverse of this bijection is again taking complement.) Therefore

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

as desired. □

The next proposition is a great showcase of proving an identity by counting the same set twice:

Proposition 3.7. *For any integer $n \geq 0$, we have*

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

Proof. Let X be a finite set of cardinality n. Note that $\mathcal{P}(X) = \bigcup_{i=0}^{n} \mathcal{P}_i(X)$. Moreover, $\mathcal{P}_i(X) \cap \mathcal{P}_j(X) = \emptyset$ when $i \neq j$. So by additive principle,

$$|\mathcal{P}(X)| = \sum_{i=0}^{n} |\mathcal{P}_i(X)| = \sum_{i=0}^{n} \binom{n}{i}.$$

Since we have already counted that $|\mathcal{P}(X)| = 2^n$, the desired result follows. □

Up to this point, we have no consistent way of calculating binomial coefficients other than certain special values. The following proposition gives an inductive way:

Proposition 3.8. *For any integers n and r such that $1 \leq r \leq n$, we have*

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

Proof. Let X be a finite set of cardinality n. Since $n \geq 1$, X contains an element x_1. Let $X' = X - \{x_1\}$. Then $|X'| = n - 1$. We define a function $\Phi : \mathcal{P}_r(X) \to \mathcal{P}_{r-1}(X') \cup \mathcal{P}_r(X')$ as follows

$$\Phi(A) = \begin{cases} A - \{x_1\} & \text{if } x_1 \in A; \\ A & \text{if } x_1 \notin A. \end{cases}$$

Note that in the first case, $\Phi(A) = A - \{x_1\}$ is an element in $\mathcal{P}_{r-1}(X')$. In the second case, $\Phi(A) = A$ is an element in $\mathcal{P}_r(X')$.

We claim that Φ is bijective. Indeed, we can construct an inverse Ψ as follows:

$$\Psi(A) = \begin{cases} A \cup \{x_1\} & \text{if } A \in \mathcal{P}_{r-1}(X'); \\ A & \text{if } A \in \mathcal{P}_r(X'). \end{cases}$$

It is easy to check $\Phi \circ \Psi$ and $\Psi \circ \Phi$ are inverses on respective sets. So Φ is bijective, as desired.

Therefore, together with additive principle, we have

$$\binom{n}{r} = |\mathcal{P}_r(X)| = |\mathcal{P}_{r-1}(X')| + |\mathcal{P}_r(X')| = \binom{n-1}{r-1} + \binom{n-1}{r},$$

as desired. □

This proposition is another showcase of the idea of proving identities via counting twice.

Using this proposition, starting with $\binom{0}{0} = \binom{1}{0} = \binom{1}{1} = 1$, we can inductively calculate the binomial coefficients with $n = 2, 3, 4, \ldots$, taking into consideration that $\binom{n}{0} = \binom{n}{n} = 1$.

Note that for each n, there are $n+1$ binomial coefficients that are not zero, with $r = 0, 1, \ldots, n$. If we put these coefficients in a pyramid, where each row corresponds to all binomial coefficients with the same n listed in order of increasing r, we have the following *Pascal triangle*, named after French mathematician Blaise Pascal:

$$\begin{array}{lccccccccc} n = 0: & & & & & 1 & & & & \\ n = 1: & & & & 1 & & 1 & & & \\ n = 2: & & & 1 & & 2 & & 1 & & \\ n = 3: & & 1 & & 3 & & 3 & & 1 & \\ n = 4: & 1 & & 4 & & 6 & & 4 & & 1 \end{array}$$

Notice that each entry is the sum of the two on its shoulders on the previous line, by the inductive relation we just proved. For example, using this triangle, we have $\binom{4}{2} = 6$, the third entry on the row $n = 4$, and it is the sum of two 3's on the previous line.

For small n, this is quite efficient, since it is much easier to get all coefficients with the same n than calculate those one by one using the explicit formula to be introduced later. But when n is large, this is not as easy. We have

Proposition 3.9. *For any integers n, r such that $0 \leq r \leq n$, we have*

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

Proof. This can be proved by induction on n, with the inductive relation in Proposition 3.8. However, such a proof provides little insight into why the formula works. Instead, we connect this to counting problem that we have already solved.

Let X be a finite set of cardinality n. Consider the set $\mathrm{Inj}(\mathbb{N}_r, X)$, consisting of injections from $\mathbb{N}_r = \{1, 2, \ldots, r\}$ to X. Note that for any $f \in \mathrm{Inj}(\mathbb{N}_r, X)$, $\mathrm{Im}(f)$ is a subset of X of cardinality r. For any $A \in \mathcal{P}_r(X)$, define

$$\mathrm{Inj}_A(\mathbb{N}_r, X) = \{f \in \mathrm{Inj}(\mathbb{N}_r, X) | \, \mathrm{Im}(f) = A\}.$$

In other words $\mathrm{Inj}_A(\mathbb{N}_r, X)$ consists of all injections from $\mathbb{N}_r$ to X whose image is precisely A. Clearly

$$\mathrm{Inj}(\mathbb{N}_r, X) = \bigcup_{A \in \mathcal{P}_r(X)} \mathrm{Inj}_A(\mathbb{N}_r, X),$$

and also for any $A, B \in \mathcal{P}_r(X)$, if $A \neq B$, then $\mathrm{Inj}_A(\mathbb{N}_r, X) \cap \mathrm{Inj}_B(\mathbb{N}_r, X) = \emptyset$. So by additive principle,

$$|\,\mathrm{Inj}(\mathbb{N}_r, X)| = \sum_{A \in \mathcal{P}_r(X)} |\,\mathrm{Inj}_A(\mathbb{N}_r, X)|.$$

Finally, note that we can treat any function in $\mathrm{Inj}_A(\mathbb{N}_r, X)$, as a function in $\mathrm{Inj}(\mathbb{N}_r, A)$. Since $|\,\mathrm{Inj}(\mathbb{N}_r, A)| = r!$ and $|\,\mathrm{Inj}(\mathbb{N}_r, X)| = \dfrac{n!}{(n-r)!}$, we have

$$\frac{n!}{(n-r)!} = |\,\mathrm{Inj}(\mathbb{N}_r, X)| = \sum_{A \in \mathcal{P}_r(X)} r! = \binom{n}{r} r!$$

which immediately gives

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

as desired. □

Application of binomial coefficients. The numbers $\binom{n}{r}$ appear as coefficients in expansion of n-power of the binomial $a+b$, lending them the name "binomial coefficients". The exact statement is:

Theorem 3.10. *Let n be any natural number, then*

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i.$$

For example, setting $n = 2$ we have the familiar $(a+b)^2 = a^2 + 2ab + b^2$, and setting $n = 3$ we have $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$. Note that the coefficients in the expansion appear in order in the corresponding row of the Pascal triangle.

Proof. We prove this by induction on n. The base case $n = 1$ is trivial. Suppose the statement holds for $n = k$. Then for $n = k + 1$, we have

$$\begin{aligned}
(a+b)^{k+1} &= (a+b)\cdot(a+b)^k = (a+b)\cdot\sum_{i=0}^{n}\binom{k}{i}a^{k-i}b^i \\
&= \sum_{i=0}^{k}\binom{k}{i}a^{k+1-i}b^i + \sum_{i=0}^{k}\binom{k}{i}a^{k-i}b^{i+1} \\
&= \sum_{i=0}^{k}\binom{k}{i}a^{k+1-i}b^i + \sum_{j=1}^{k+1}\binom{k}{j-1}a^{k+1-j}b^j \\
&= a^{k+1} + \sum_{i=1}^{k}\binom{k}{i}a^{k+1-i}b^i + \sum_{j=1}^{k}\binom{k}{j-1}a^{k+1-j}b^j + b^{k+1} \\
&= a^{k+1} + \sum_{i=1}^{k}\binom{k}{i}a^{k+1-i}b^i + \sum_{i=1}^{k}\binom{k}{i-1}a^{k+1-i}b^i + b^{k+1} \\
&= a^{k+1} + \sum_{i=1}^{k}\left(\binom{k}{i} + \binom{k}{i-1}\right)a^{k+1-i}b^i + b^{k+1} \\
&= a^{k+1} + \sum_{i=1}^{k}\binom{k+1}{i}a^{k+1-i}b^i + b^{k+1} \\
&= \sum_{i=0}^{k+1}\binom{k+1}{i}a^{k+1-i}b^i,
\end{aligned}$$

as desired. □

Example 3.11. This theorem is very helpful in figuring out coefficients of any binomial expansion. For example

$$(a+2b)^4 = a^4 + 4a^3\cdot(2b) + 6a^2\cdot(2b)^2 + 4a\cdot(2b)^3 + (2b)^4 = a^4 + 8a^3b + 24a^2b^2 + 32ab^3 + 16b^4.$$

4 Number systems

Different sets of numbers have their origins in counting. The set of natural numbers $\mathbb{N}$ is a direct abstraction of counting. The set of nonnegative integers $\mathbb{Z}_{\geq 0}$ simply comes from adding 0 to the set $\mathbb{N}$. The arithmetic operations $+, \times$ always make sense for any pair of numbers in $\mathbb{Z}_{\geq 0}$, but not subtraction $-$. To rectify this, we can introduce negative integers and form the set of integers $\mathbb{Z}$. Now $+, \times, -$ always make sense, but not division $\div$, even when the divisor is nonzero. To rectify this, we introduce the fractions and the set of rational numbers $\mathbb{Q}$. Now all arithmetic operations make sense, but for example the equation $x^2 = 2$ has no solution in $\mathbb{Q}$. We can move to a larger set of numbers, say $\mathbb{R}$ to solve this. In this class, $\mathbb{R}$ is usually the largest set of numbers we use. On the other hand, in $\mathbb{R}$, the equation $x^2 = -1$ still has no solution, so sometimes we can move to the set of complex numbers $\mathbb{C}$ to solve this.

This somewhat lengthy discussion aims to illustrate a(n) (extremely simplified) history of development of these number systems. Each extension to a larger set of numbers came from the need to make sure certain arithmetic operations always make sense, or certain equations to always have solutions. We now move to develop these number systems (somewhat) rigorously.

4.1 Natural numbers and Peano axioms

The first axiomatic treatment of the set of natural numbers was proposed independently by German mathematician Richard Dedekind (in his book *Was sind und was sollen die Zahlen?*) and Italian mathematician Giuseppe Peano (in his book *Arithmetices principia, nova methodo exposita*). As remarked by Dedekind, the "essence" of natural numbers is the existence of a successor function (which corresponds to $+1$ in our naïve treatment of natural numbers).

Axiom 4.1. *The set of natural numbers $\mathbb{N}$ is a set with a function $s : \mathbb{N} \to \mathbb{N}$ and an element $1 \in \mathbb{N}$ such that*

(1) *s is an injection;*

(2) *1 is not in the image of s; and*

(3) *For a subset $A \subseteq \mathbb{N}$, if $1 \in A$ and $(n \in A \Rightarrow s(n) \in A)$, then $A = \mathbb{N}$.*

Note that by (2), $s(1) \neq 1$. Similarly $s(s(1)) \neq 1$. Since s is an injection by (1), $s(s(1)) \neq s(1)$. By the same argument $s(s(s(1)))$ is different from $1, s(1), s(s(1))$. So we have the following elements belong to $\mathbb{N}$: $1, s(1), s(s(1)), s(s(s(1))), \ldots$. Moreover, by (3), which is a version of the induction principle, this list exhausts all elements of $\mathbb{N}$. We can define $2 = s(1)$, $3 = s(2)$, and so on. In this way, we have recovered the familiar form of $\mathbb{N}$ using these axioms.

Note that the arithmetic operations $+, \times$ can be defined using these axioms:

Definition 4.2. We can define the sum $m + n$ of two elements $m, n \in \mathbb{N}$ inductively as follows:

- $m + 1 = s(m)$ for any $m \in \mathbb{N}$; and
- $m + s(n) = s(m + n)$ for any $m, n \in \mathbb{N}$.

Similarly, we can define the product $m \times n$ of two elements $m, n \in \mathbb{N}$ inductively as follows:

- $m \times 1 = m$ for any $m \in \mathbb{N}$; and
- $m \times s(n) = m \times n + m$ for any $m, n \in \mathbb{N}$.

We can then define the ordering $<$ on $\mathbb{N}$ as follows

Definition 4.3. Given $m, n \in \mathbb{N}$, $m < n$ if and only if $m + c = n$ for some $c \in \mathbb{N}$.

In particular $n < n + 1 < n + 2 < \cdots$ for any $n \in \mathbb{N}$. The basic properties of these operators and ordering can then be proved using the axioms and definitions above.

We now briefly discuss how to construct $\mathbb{Z}_{\geq 0}$ and $\mathbb{Z}$ based on $\mathbb{N}$. Details are omitted, but the key ideas are presented.

$\mathbb{Z}_{\geq 0}$ from $\mathbb{N}$. To define the set of nonnegative integers from natural numbers, we only need to add 0. Indeed, we can define $\mathbb{Z}_{\geq 0} = \mathbb{N} \cup \{0\}$, and extend the successor function s by setting $s(0) = 1$. The operations $+, \times$ and the ordering $<$ can be defined in similar ways.

$\mathbb{Z}$ from $\mathbb{Z}_{\geq 0}$. To define the set of integers, we need to add negative integers. Indeed, define $\mathbb{Z} = \mathbb{Z}_{\geq 0} \cup \{-k | k \in \mathbb{N}\}$, where $-k$ by definition is the unique solution to $x + k = 0$. Notice that this implies that $-(-k) = k$ for any natural number k, as well as $-0 = 0$. We can extend the successor function as follows: $s(-1) = 0$, and $s(-k) = -s^{-1}(k)$ when $k \in \mathbb{N}$. Note that s is now a bijection. The operations $+, \times$ and the ordering $<$ can again be defined similarly via s and its inverse s^{-1}. We can also define subtraction $-$ for any pair of integers: $m - n$ by definition is $m + (-n)$.

4.2 Fractions and rational numbers

For $\mathbb{Z}$, the operations $+, -, \times$ always make sense, but not $\div$. That is, the following equation $bx = a$ does not always have a solution in $\mathbb{Z}$. To rectify this, we introduce a *fraction* $\frac{a}{b}$ to represent the unique solution to the equation. On the other hand, if we want to extend $\times$ to all fractions, it is natural to have $d \times b \times \frac{a}{b} = d \times a$, which means $\frac{a}{b} = \frac{da}{db}$. We can solve this issue by thinking of fractions as equivalence classes, as follows.

Let $\mathcal{S} = \mathbb{Z} \times (\mathbb{Z} - \{0\})$. We define a relation $\sim$ on $\mathcal{S}$ as follows: $(a_1, b_1) \sim (c_1, d_1) \Leftrightarrow a_1 b_2 = a_2 b_1$. Then $\sim$ is called an "equivalence relation". Let $\mathbb{Q} = \mathcal{S}/\sim$ be the set of "equivalence classes", i.e. we view two pairs as the same if they are related by $\sim$. Instead of writing $[(a, b)]$ as the equivalent class of $(a, b) \in \mathbb{S}$, we simply write $\frac{a}{b} = [(a, b)]$. We call $\mathbb{Q}$ the set of rational numbers (so any element in $\mathbb{Q}$ is a rational number), and sometimes field of fractions.

Note that since $(a, b) \sim (da, db)$ for any integer $d \neq 0$, we have $\frac{a}{b} = \frac{da}{db}$, as expected.

If a, b has a common divisor d, that is $a = da_1, b = db_1$ for some integers a_1, b_1, then clearly $\frac{a}{b} = \frac{a_1}{b_1}$. Moreover, we have $\frac{a}{b} = \frac{-a}{-b}$. This implies that for any element in $\mathbb{Q}$, we can choose a representative $\frac{a}{b}$ so that a, b are coprime, and $b > 0$. This will be our preferred choice of fractional representation of a rational number, and a fraction written in this form is called *in lowest terms*.

We note that the set of integers are mapped injectively into $\mathbb{Q}$ via the map $n \mapsto \frac{n}{1}$.

We can define arithmetic operations and ordering as follows:

Definition 4.4. Given $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$, their sum is defined as follows:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$

Their product is defined as follows:

$$\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}.$$

The opposite (or negative) of $\frac{a}{b}$ is defined to be

$$-\frac{a}{b} = \frac{-a}{b}.$$

Consequently, the difference of two rational numbers $r_1, r_2 \in \mathbb{Q}$ is defined to be $r_1 - r_2 = r_1 + (-r_2)$.

The inverse of $\frac{a}{b}$ when $a \neq 0$, is defined to be

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

Consequently, the quotient of two rational numbers $r_1, r_2 \in \mathbb{Q}$ is defined to be $r_1 \div r_2 = r_1 \times r_2^{-1}$.

Definition 4.5. Suppose $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$ are in lowest terms, so in particular $b, d > 0$. Then

$$\frac{a}{b} < \frac{c}{d} \Leftrightarrow ad < bc.$$

One need to check that the arithmetic operations are well-defined, in the sense that if we choose different fractional representatives of rational numbers, the end result of the operation is the same. For example, we have

Proposition 4.6. *The arithmetic operation $+$ is well defined. That is, if $\frac{a_1}{b_1}$ and $\frac{a_2}{b_2}$ represent the same rational number, and $\frac{c_1}{d_1}$ and $\frac{c_2}{d_2}$ represent the same rational number, then $\frac{a_1d_1+b_1c_1}{b_1d_1}$ and $\frac{a_2d_2+b_2c_2}{b_2d_2}$ represent the same rational number.*

Proof. To show that $\frac{a_1d_1+b_1c_1}{b_1d_1}$ and $\frac{a_2d_2+b_2c_2}{b_2d_2}$ represent the same rational number, we need to show that

$$(a_1d_1+b_1c_1)(b_2d_2)=(a_2d_2+b_2c_2)(b_1d_1),$$

which is equivalent to

$$a_1d_1b_2d_2+b_1c_1b_2d_2=a_2d_2b_1d_1+b_2c_2b_1d_1.$$

Since $\frac{a_1}{b_1}$ and $\frac{a_2}{b_2}$ represent the same rational number, we have $a_1b_2=a_2b_1$. So $a_1b_2d_1d_2=a_2b_1d_1d_2$. Similarly $c_1d_2b_1b_2=c_2d_1b_1b_2$. Adding these two equations, we get the desired equality. □

Well-defined-ness of other operations and ordering is omitted. We also remark that other familiar properties of the rational number can also be proved from these axioms and definitions.

4.3 Decimal representations of rational numbers

The most common way to represent an integer is to use *decimals*: $123=1\times100+2\times10+3=1\times10^2+2\times10^1+3\times10^0$. We remark that in the same way, integers can be represented with powers of *any* fixed integer >1. In computer science, it is very common to use binary representation: $10011=1\times2^4+0\times2^3+0\times2^2+1\times2^1+1\times2^0$ for just one example.

Such a decimal representation can be extended to some rational numbers as well. Instead of just nonnegative powers of 10, we can also include negative powers, separated by a *decimal point*: $12.34=1\times10^1+2\times10^0+3\times10^{-1}+4\times10^{-2}$. In general,

$$0.a_1a_2\cdots a_n=a_1\times10^{-1}+a_2\times10^{-2}+\cdots+a_n\times10^{-n}.$$

where $a_i\in\{0,1,2,3,4,5,6,7,8,9\}$ for $i=1,\ldots,n$. Note that

$$a_1\times10^{-1}+a_2\times10^{-2}+\cdots+a_n\times10^{-n}=\frac{a_1\times10^{n-1}+a_2\times10^{n-2}+\cdots+a_n}{10^n},$$

so $0.a_1a_2\cdots a_n$ represents a rational number with a fractional representation as above.

We remark that for simplicity, we focus on decimals with only 0 before the decimal point. This can be easily generalized by adding integers.

One can also define *infinite decimals* as follows:

Definition 4.7. An infinite decimal $0.a_1a_2a_3\cdots$, where $a_i\in\{0,1,\ldots,9\}$ represents a rational number q if

$$0.a_1a_2\cdots a_n\le q\le0.a_1a_2\cdots a_n+\frac{1}{10^n}.$$

In this case, we simply write $q=0.a_1a_2a_3\cdots$.

Note that this implies $|q - 0.a_1a_2\cdots a_n| \leq 10^{-n}$, which gets arbitrarily close to 0 as n gets larger. In the language of limits from calculus, this means

$$q = \lim_{n\to\infty} 0.a_1a_2\cdots a_n.$$

Note that a finite decimal $0.a_1a_2\cdots a_n$ can be treated as an infinite one by setting $a_i = 0$ for all $i \geq n+1$.

We also remark that it is easy to multiply a decimal by 10, which amounts to shift the decimal point by one position to the right:

$$10 \times 0.a_1a_2a_3\cdots = a_1.a_2a_3\cdots .$$

Example 4.8. We have

$$\frac{1}{3} = 0.333333\cdots .$$

Indeed, assume $\frac{1}{3} = 0.a_1a_2a_3\cdots$. To find a_1 so that $0.a_1 \leq \frac{1}{3} \leq 0.a_1 + 0.1$, we need to find a_1 so that $a_1 \leq \frac{10}{3} \leq a_1 + 1$. Since $\frac{10}{3} = 3 + \frac{1}{3}$, we conclude that $a_1 = 3$. Now

$$\frac{1}{3} = \frac{10}{3} - 3 = 10 \times 0.3a_2a_3\cdots - 3 = 3.a_2a_3\cdots - 3 = 0.a_2a_3\cdots$$

So we immediately conclude $a_2 = a_1 = 3$ and as a matter of fact, $a_{i+1} = a_i$. So inductively $a_i = 3$ for all natural number i.

Example 4.9. We have

$$0.99999\cdots = 1.$$

Indeed, with n 9's, we have $0.999\ldots9 \leq 0.99999\cdots \leq 0.999\cdots9 + 10^{-n} = 1$, and so

$$|1 - 0.9999\cdots| \leq 10^{-n}$$

for any positive integer n, which means they are equal.

This example suggests that decimal representations are not unique. In fact, we have

$$0.a_1a_2\cdots a_n99999\cdots = 0.a_1a_2\cdots a_n + 10^{-n}.$$

Example 4.10. Using similar arguments, we can show

$$\frac{5}{7} = 0.714285714285714285\cdots$$

where 714285 are repeated.

A pattern already emerges: for the few examples we have tried, the decimal representation of a rational number eventually repeats a certain string *ad infinitum*. This is in fact the case in general.

Definition 4.11. A *recurring infinite decimal* is an infinite decimal that after certain digit, repeats a string of digits. We write

$$0.a_1a_2\cdots a_n\overline{a_{n+1}\cdots a_{n+m}} \text{ or } 0.a_1a_2\cdots a_n\dot{a}_{n+1}\cdots\dot{a}_{n+m}$$

to represent an infinite decimal which repeats the string of digits $a_{n+1}\cdots a_{n+m}$ after a_n.

For example, $0.3333\cdots 0.\overline{3}$, and $\frac{5}{7} = 0.\overline{714285}$. Note that a finite decimal is recurring by viewing $\overline{0}$ as the repeated part: $0.5 = 0.5\overline{0}$. We can also use the fact that $0.0\overline{9} = 0.1$ to write $0.5 = 0.4\overline{9}$.

We claim

Theorem 4.12. *A recurring infinite decimal represents a rational number, and any rational number can be represented by a recurring infinite decimal.*

The proper proof of this theorem needs materials not entirely covered at this point, so we skip it. We give an example of how to find a fraction from a recurring infinite decimal. A general proof in this direction is not hard to construct analogously.

Example 4.13. To find a fractional representation of

$$x = 12.79\overline{317},$$

we start by multiplying some power of 10 to move the decimal point to just before the repeated part:

$$100x = 1279.\overline{317}.$$

Next, we move the decimal point across one iteration of the repeated part:

$$1000 \times 100x = 1279317\overline{317}.$$

The difference of the two equation gives

$$99900x = 1279317 - 1279 = 1278038$$

which implies

$$x = \frac{1278038}{99900}.$$

4.4 Real numbers

Note that we can easily write down an infinite decimal that is not recurring:

$$0.12112111211112\cdots$$

Here, between two 2's there are increasing number of 1. If we look at the first n part of the number

$$0.1, 0.12, 0.121, 0.1211, 0.12112, \ldots$$

we notice that these numbers are getting closer to each other, and start to cluster. This observation gives rise to the definition of the set of real numbers $\mathbb{R}$ as *metric completion* of $\mathbb{Q}$. Intuitively, $\mathbb{R}$ contains $\mathbb{Q}$ and also numbers that can be approximated to arbitrary precision by rational numbers.

A proper, rigorous definition of real numbers using *Cauchy sequences* or *Dedekind cuts*, named after two important mathematicians Augustin-Louis Cauchy and Richard Dedekind, is beyond the scope of this course, and will be likely treated in a higher level real analysis course. For this course, we can simply view $\mathbb{R}$ as the set of numbers that can be represented by an infinite decimal, among which the recurring ones are rational.

Here is another way of finding numbers that are not rational. Note that for any positive real number $x \in \mathbb{R}_+$, there exists a positive real number y such that $y^2 = x$, which we denote by $y = \sqrt{x}$. To properly prove this fact, we need a rigorous definition of $\mathbb{R}$, so we skip it. We show:

Theorem 4.14. *There does not exist a rational number r such that $r^2 = 2$. In particular $\sqrt{2}$ is not rational.*

Proof. Suppose by contradiction that there exist a rational number r such that $r^2 = 2$, where the fraction is written in lowest terms. Write $r = \frac{p}{q}$ in lowest terms. That is, we have $q > 0$ and $\gcd(p, q) = 1$. Then $r^2 = \frac{p^2}{q^2} = 2$, and thus $p^2 = 2q^2$. This means that p^2 is even. By a result we proved in Part I, p is also even. Write $p = 2k$ for some integer k. Then $p^2 = 4k^2 = 2q^2$. Thus $q^2 = 2k^2$. By a similar argument, q is also even. But then 2 is a common divisor of p, q, and p, q are not coprime, a contradiction! □

5 Counting infinite sets

In this section, we briefly introduce cardinalities of infinite sets. Recall that on the theoretic side of finite counting, we define a set has cardinality n if there is a bijection from $\mathbb{N}_n$ to this set. In some sense, we choose $\mathbb{N}_n$ as a reference, and compare it via bijections to other sets. One important goal of defining different number systems is to construct some reference sets that we can compare other sets to in the infinite setting. For example, $\mathbb{N}$, $\mathbb{Q}$ and $\mathbb{R}$ are all infinite. Do they have the "same" cardinality? What are some other sets that share the cardinality with these sets? We will attempt to answer these questions in this section.

We start with the following definition:

Definition 5.1. Two sets X and Y (not necessarily finite!) are said to be *equipotent* (or have the same cardinality) if there exists a bijection $f : X \to Y$. In this case, we write $|X| = |Y|$.

We want to remark (very strongly!) that at this point $|X|$ by itself is not a well-defined "number" yet. The equality "$|X| = |Y|$" does not mean we are comparing two numbers, but rather a "shorthand" for the existence of a bijection between the two sets. It is easy to show

Proposition 5.2. *If $|X| = |Y|$ and $|Y| = |Z|$, then $|X| = |Z|$.*

More generally, we have the following definition:

Definition 5.3. If there exists an injection $f : X \to Y$, we write $|X| \leq |Y|$. If there exists a surjection $f : X \to Y$, we write $|X| \geq |Y|$.

Again, $|X|$ by itself is not a well-defined "number", we use $|X| \leq |Y|$ as a shorthand for existence of an injective function between the two sets. We remark that these definitions are clearly made with Theorem 1.17 in mind; they agree with the usual comparison of cardinalities of finite sets (when cardinalities are actual numbers). It is not immediately clear that $|X| \leq |Y|$ if and only if $|Y| \geq |X|$. But it is true:

Proposition 5.4. *Let X, Y be sets. Then $|X| \leq |Y|$ iff $|Y| \geq |X|$.*

Proof. Suppose that $|X| \leq |Y|$. Then there exists an injection $f\colon X \to Y$. To prove that $|Y| \geq |X|$ we need to find a surjective function $g\colon Y \to X$. For $y \in f(X)$, define $g(y)$ as the unique $x \in X$ so that $f(x) = y$. For $y \in Y \setminus f(X)$, set $g(y) = x_0$, where x_0 is any fixed element of X. Then g is clearly surjective, as $g(f(X)) = X$.

Suppose that $|Y| \geq |X|$. Then there exists a surjective function $g\colon Y \to X$. Now, by Lemma 1.16, there exists an injective function $f\colon X \to Y$ so that $g \circ f = \mathrm{id}_X$. Thus $|X| \leq |Y|$. □

5.1 Denumerable sets

We start with sets that have the same size as $\mathbb{N}$:

Definition 5.5. A set X is said to be *denumerable* if it is equipotent to $\mathbb{N}$. In other words, if there exists a bijection $f : \mathbb{N} \to X$. If X is denumerable, we sometimes write $|X| = \aleph_0$.

A set is said to be *countable* if it is either finite or denumerable.

Here we can view $\aleph_0$ as a "number" we assign to the cardinality of $\mathbb{N}$. The symbol is usually read as "aleph-null", and was first used by German mathematician Georg Cantor. $\aleph$ Is the first letter in the Hebrew alphabet.

If X is denumerable, we can "list" or *enumerate* elements of X as an infinite sequence via the bijection $f : \mathbb{N} \to X$:

$$X = \{f(1), f(2), f(3), \ldots\}$$

giving some rationale behind the name.

Example 5.6. The set of natural numbers $\mathbb{N}$ is denumerable, since the identity function $\mathrm{id} : \mathbb{N} \to \mathbb{N}$ is a bijection.

Example 5.7. Any finite set is not denumerable. Indeed if X is finite, then any function $f : \mathbb{N} \to X$ is not injective. You will prove this as part of your homework.

Example 5.8. The set of nonnegative integers $\mathbb{Z}^{\geq 0} = \{0, 1, 2, 3, \ldots\}$ is denumerable. Indeed we can construct a bijection $f : \mathbb{N} \to \mathbb{Z}^{\geq 0}$ by $f(n) = n - 1$.

Example 5.9. The set of integers $\mathbb{Z}$ is denumerable. We can a bijection $f : \mathbb{N} \to \mathbb{Z}$ by

$$f(n) = \begin{cases} -\frac{n-1}{2} & \text{if } n \text{ is odd,} \\ \frac{n}{2} & \text{if } n \text{ is even.} \end{cases}$$

In other words we can list elements in $\mathbb{Z}$ as follows:

$$\{0, 1, -1, 2, -2, 3, -3, \ldots\}.$$

Example 5.10. The set of even integers $\mathcal{E}$ is denumerable. Indeed, it is straightforward to write down a bijection $g : \mathbb{Z} \to \mathcal{E}$ by $g(n) = 2n$. Composed with the function f in the previous example, we get a bijection from $\mathbb{N}$ to $\mathcal{E}$.

This example suggests the following basic property of denumerable sets:

Proposition 5.11. *Let X be a denumerable set. Then Y is equipotent to X if and only if Y is also denumerable.*

Proof. Since X is denumerable, there exists a bijection $f : \mathbb{N} \to X$. If Y is equipotent to X, we have a bijection $g : X \to Y$. Thus $g \circ f : \mathbb{N} \to Y$ is a bijection. So Y is denumerable. On the other hand, if Y is denumerable, then we have a bijection $h : \mathbb{N} \to Y$. Then $h \circ f^{-1} : X \to Y$ is a bijection. So X and Y are equipotent. □

In other words, to show a set is denumerable, we do not need to always compare it to $\mathbb{N}$. Any other set known to be denumerable can serve as reference.

Examples 5.8, 5.9, and 5.10 illustrate the so-called paradox of infinity: a *proper* subset can have the same cardinality as the set itself. In fact this property *characterizes* infinite sets. To show this, let us prove some statements in preparation.

Proposition 5.12. *If X is denumerable, then $X \cup \{a\}$ is denumerable for any singleton $\{a\}$.*

Proof. If $a \in X$, then $X \cup \{a\} = X$ is denumerable. Otherwise, let $f : \mathbb{N} \to X$ be a bijection. Then

$$g(n) = \begin{cases} a & \text{if } n = 1 \\ f(n-1) & \text{if } n \geq 2 \end{cases}$$

is a bijection from $\mathbb{N}$ to $X \cup \{a\}$. □

This result is best summarized in the story of Hilbert Hotel. Hilbert Hotel has denumerably many rooms, with room numbers going through all natural numbers. On this particular day, it is fully occupied. A new guest arrives and ask if there are any vacancies. The manager simply asks the guest in Room k moves to Room $k+1$, and now Room 1 is vacant, which our new guest gladly takes.

Using induction on $|Y|$, we can show

Corollary 5.13. *If X is denumerable and Y is finite, then $X \cup Y$ is denumerable.*

Similarly we can show

Theorem 5.14. *If X is denumerable and Y is finite, then $X - Y$ is denumerable.*

This is left as an excercise.

The following result states that in some sense, denumerable sets are the smallest infinite sets:

Proposition 5.15. *Any infinite set contains a denumerable subset.*

Proof. Let X be an infinite set. We construct a denumerable subset A, and a function $f : \mathbb{N} \to X$ inductively as follows.

For the base step, choose any $a_1 \in X$. Define $f(1) = a_1$, and set $A_1 = \{a_1\}$.

Suppose now that $f(1) = a_1, f(2) = a_2, \ldots, f(k) = a_k$ have all been chosen, and we have $A_k = \{a_1, \ldots, a_k\}$. Note that $X - A_k$ is nonempty, since otherwise $X = A_k$ is finite. Thus we can chose a_{k+1} that is different from $a_1, \ldots, a_k$. Set $f(k+1) = a_{k+1}$ and $A_{k+1} = A_k \cup \{a_{k+1}\}$.

In this way we constructed a function $f : \mathbb{N} \to X$, and by construction it is injective. Take $A = \mathrm{Im}(f) = \{a_1, a_2, a_3, \ldots\}$. Then A is a denumerable subset of X. □

Now we are ready to showcase the "paradox" of infinity in general:

Theorem 5.16 (Dedekind)**.** *A set X is infinite if and only if it is equipotent to a proper subset of itself.*

Proof. For the "if" direction, we prove its contrapositive: if a set X is finite, then it is not equipotent to any proper subset of X. This follows from our result Corollary 1.19 on finite sets.

For the "only if" direction. Suppose X is infinite. By Proposition 5.15, X contains a denumerable subset $A = \{a_1, a_2, a_3, \ldots\}$. We can do a Hilbert Hotel trick on A while leaving the other parts of X unchanged. Define a function

$$f(x) = \begin{cases} a_{n+1} & \text{if } x = a_n \in A \\ x & \text{if } x \notin A \end{cases}$$

Then f gives a bijection from X to $X - \{a_1\}$. In particular, X is equipotent to a proper subset $X - \{a_1\}$, as desired. □

In fact, the proof above gives

Proposition 5.17. *Let X be an infinite set. Then $|X - \{a\}| = |X| = |X \cup \{a\}|$ for any singleton $\{a\}$.*

Using induction, this implies

Corollary 5.18. *Let X be an infinite set, and Y a finite set. Then $|X - Y| = |X| = |X \cup Y|$.*

Here are some more properties of denumerable sets:

Proposition 5.19. *If X is denumerable, then any subset of X is countable.*

Proof. We may assume $X = \mathbb{N}$. In the general case, there exists a bijection $f : \mathbb{N} \to X$. Note that a subset B of X is equipotent to $f^{-1}(B) \subseteq \mathbb{N}$, if we can show that any subset of $\mathbb{N}$ is countable, then so is B.

If a subset A of $\mathbb{N}$ is finite, then it is automatically countable. Suppose A is infinite. Construct a function $f : \mathbb{N} \to A$ inductively as follows: for the base step, set $f(1) = \min A$. Note that $\min A$ exists by the so-called *well-ordering principle*, which can be proved using induction. Now suppose that $f(1), f(2), \ldots, f(k)$ has been defined. Let $A_{k+1} = A - \{f(1), \ldots, f(k)\}$. Then A_{k+1} is nonempty, and so $\min A_{k+1}$ exists. We can then define

$$f(k+1) = \min A_{k+1}.$$

It is easy to check from construction that this is a bijection, as $f(1) < f(2) < f(3) < \cdots$, and every number in A is covered. □

This proposition is very helpful for checking if an infinite set is denumerable, since we only need to show it is equipotent to the subset of a known denumerable set, or equivalently, we only need to construct an injection to a denumerable set instead of a bijection.

The next three propositions hold similarly for general infinite sets as well, but are harder to prove. So we stick to denumerable sets.

Proposition 5.20. *If A and B are denumerable, then so is $A \cup B$.*

Proof. Let $C = B - A$. Then $A \cup B = A \cup C$, and $A \cap C = \emptyset$. If C is finite, then by Corollary 5.13, $A \cup B = A \cup C$ is denumerable.

Suppose now C is infinite. Since $C \subseteq B$, it is denumerable. Let $f : \mathbb{N} \to A$ and $g : \mathbb{N} \to C$ be bijections. Consider the function $h : \mathbb{N} \to A \cup C$ defined as follows

$$h(n) = \begin{cases} f(\frac{n-1}{2}) & \text{if } n \text{ is odd,} \\ g(\frac{n}{2}) & \text{if } n \text{ is even.} \end{cases}$$

It is easy to check that h is a bijection. So $A \cup B = A \cup C$ is denumerable. □

Proposition 5.21. *If A and B are denumerable, then so is $A \times B$.*

Proof. Write $A = \{a_1, a_2, \ldots, a_m, \ldots\}$ and $B = \{b_1, b_2, \ldots, b_n, \ldots\}$. We list $A \times B$ in a infinite table as follows:

$$\begin{array}{cccccc}
(a_1,b_1) & (a_2,b_1) & (a_3,b_1) & (a_4,b_1) & \cdots \\
(a_1,b_2) & (a_2,b_2) & (a_3,b_2) & (a_4,b_2) & \cdots \\
(a_1,b_3) & (a_2,b_3) & (a_3,b_3) & (a_4,b_3) & \cdots \\
(a_1,b_4) & (a_2,b_4) & (a_3,b_4) & (a_4,b_4) & \cdots \\
\vdots & \vdots & \vdots & \vdots & \ddots
\end{array}$$

We can then list these elements in one long sequence by going through each (top-right to bottom-left) diagonal: first the diagonal (a_1, b_1), and then the diagonal (a_2, b_1)–(a_1, b_2), and then the diagonal (a_3, b_1)–(a_2, b_2)–(a_1, b_3), and so on. While it is possible to explicitly write down a bijection between $A \times B$ and $\mathbb{N}$, the formula itself is not too illuminating, so we leave the arguments as they are here. □

Using induction on n, we can then show

Corollary 5.22. *If $A_1, A_2, \ldots, A_n$ is denumerable, then $A_1 \times A_2 \times \cdots \times A_n$ is denumerable. In particular, if $A_1 = A_2 = \cdots = A$, then A^n is denumerable.*

We are now ready to show:

Theorem 5.23 (Cantor)**.** *The set of rational numbers $\mathbb{Q}$ is denumerable.*

Proof. For each rational number $r \in \mathbb{Q}$, write $r = \dfrac{p}{q}$ as a fraction in lowest terms (i.e. p, q coprime and $q > 0$). Consider the following map $f : \mathbb{Q} \to \mathbb{Z} \times \mathbb{N}$ defined by

$$f\left(\frac{p}{q}\right) = (p, q).$$

Since fractional representation in lowest terms is unique for each rational number, the function f is well-defined. Moreover, it is easy to see that f is injective. Thus $|\mathbb{Q}| = |\operatorname{Im}(f)|$, as $f : \mathbb{Q} \to \operatorname{Im}(f)$ is an bijection. On the other hand, $\operatorname{Im}(f)$ is an infinite subset of $\mathbb{Z} \times \mathbb{N}$, which is denumerable by Proposition 5.21. So $\operatorname{Im}(f)$ is denumerable, and hence $\mathbb{Q}$ is denumerable. □

5.2 Uncountable sets

Definition 5.24. A set X is said to be *uncountable* if it is not countable.

Up to this point, we have no concrete example of an uncountable set. For our number systems, $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ are all countable, so it makes to ask if $\mathbb{R}$ is denumerable or not. The answer is no, according to Cantor:

Theorem 5.25 (Cantor)**.** *The set of real numbers $\mathbb{R}$ is uncountable.*

Proof. The argument used in this proof also bears Cantor's name, called Cantor's diagonal argument. Let $f : \mathbb{N} \to \mathbb{R}$ be any function. For any natural number n, write

$$f(n) = a_{n0}.a_{n1}a_{n2}a_{n3}\cdots$$

in its decimal representation (For finite decimals, we always choose repeating 0's at the end instead of repeating 9's to avoid ambiguity), where $a_{n0} \in \mathbb{Z}$, and $a_{n1}, a_{n2}, \ldots \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

Consider the real number with decimal representation

$$b = 0.b_1b_2b_3\cdots$$

where $b_n = 0$ if $a_{nn} \neq 0$ and $b_n = 1$ if $a_{nn} = 0$. Note that $f(n) \neq b$ for any natural number n, since a_{nn}, the n-th digit after the decimal point of $f(n)$, is different from b_n, the n-th digit after the decimal point of b. Thus $b \notin \mathrm{Im}(f)$, so f is not surjective, and in particular not bijective. □

We write $|X| < |Y|$ if $|X| \leq |Y|$ and $|X| \neq |Y|$ (in other words, if there exist an injection from X to Y but there does not exist any bijection between X and Y). So Cantor's theorem above can be simply stated as $|\mathbb{N}| < |\mathbb{R}|$.

One might be curious if there any sets X such that $|\mathbb{N}| < |X| < |\mathbb{R}|$. The proposition that no such sets exist is called the Continuum Hypothesis:

Continuum Hypothesis. If $|X| > \aleph_0$ and $|X| \leq |\mathbb{R}|$, then $|X| = |\mathbb{R}|$.

It was proved by American mathematician Paul Cohen that the Continuum Hypothesis is independent from the usual axioms of set theory (e.g. ZFC). That is, using axioms of set theory, we cannot prove or disprove the Continuum Hypothesis. We can assume either and develop a different mathematical universe, and both are mathematically consistent.

The next theorem implies that there are many different "levels" of infinity:

Theorem 5.26. *For any set X, $|X| < |\mathcal{P}(X)|$.*

Proof. If X is finite of cardinality n, this is equivalent to $n < 2^n$ for any natural number n. This can be proved using induction.

In general, let $f : X \to \mathcal{P}(X)$ be any function. Consider the set

$$A = \{x \in X | x \notin f(x)\}.$$

Suppose for some $x_0 \in X$, we have $f(x_0) = A$. If $x_0 \in A$, then by definition of A, $x_0 \notin f(x_0) = A$, a contradiction. If $x_0 \notin A$, the again by definition $x_0 \in f(x_0) = A$, again a contradiction. So $A \notin \mathrm{Im}(f)$, so f is not surjective and in particular, not bijective. □

Starting with $\aleph_0 = |\mathbb{N}|$, we have

$$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| < |\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))| < \cdots$$

So there are ever "larger" infinities.

The following statement is a generalization of the pigeonhole principle to infinite sets:

Theorem 5.27 (Cantor-Schröder-Bernstein)**.** *Let X, Y be nonempty sets. Suppose $|Y| < |X|$, then any function $f : X \to Y$ is not an injection.*

The proof of this theorem is omitted. This result was stated without proof by Cantor, and proved by German mathematicians Ernst Schröder and Felix Bernstein.

We have mentioned that constructing injections are much easier than bijections. The following follows easily from Cantor-Schröder-Bernstein above (in fact, equivalent to it!), and tells us it is often enough to construct injections to show two sets are equipotent:

Corollary 5.28 (Cantor-Schröder-Bernstein)**.** *If $|X| \leq |Y|$ and $|Y| \leq |X|$, then $|X| = |Y|$. In other words, if there exist injections $f : X \to Y$ and $g : Y \to X$, then there exists a bijections $h : X \to Y$.*

We now give some applications of this powerful result.

Proposition 5.29. *Show that* $|\mathbb{R}| = |(0, +\infty)|$.

Proof. This is a rare case where we can write down an explicit bijection: $f(x) = e^x$ is a bijection from $\mathbb{R}$ to $(0, +\infty)$, with inverse $\ln(x)$. □

Proposition 5.30. *Show that* $|\mathbb{R}| = |(0, +\infty) \cup (-5, -4)|$.

Proof. Now it is harder to write down a bijection. However, since $(0, +\infty) \cup (-5, -4) \subseteq \mathbb{R}$, we have $|(0, +\infty) \cup (-5, -4)| \leq |\mathbb{R}|$. On the other hand $f(x) = e^x$ gives an injection from $\mathbb{R}$ to $(0, +\infty) \cup (-5, -4)$, so $|\mathbb{R}| \leq |(0, +\infty) \cup (-5, -4)|$. By Cantor-Schröder-Bernstein, $|\mathbb{R}| = |(0, +\infty) \cup (-5, -4)|$. □

Proposition 5.31. *Show that* $|\mathbb{R}| = |(-\pi/2, \pi/2)|$.

Proof. This is another case where writing down a bijection is possible: $f(x) = \tan(x)$ is a bijection from $(-\pi/2, \pi/2)$ to $\mathbb{R}$. □

Proposition 5.32. *Show that* $|\mathbb{R}| = |[0, 1)|$.

Proof. By the previous proposition, we only need to show $|[0, 1)| = |(-\pi/2, \pi/2)|$. On the one hand $[0, 1) \subseteq (-\pi/2, \pi/2)$ and hence $|[0, 1)| \leq |(-\pi/2, \pi/2)|$. On the other hand, we can write down an injection $f(x) = \dfrac{1}{\pi}(x + \pi/2)$ from $(-\pi/2, \pi/2)$ to $[0, 1)$. Thus $|(-\pi/2, \pi/2)| \leq |[0, 1)|$. By Cantor-Schröder-Bernstein, we have $|[0, 1)| = |(-\pi/2, \pi/2)|$. □