Introduction to Abstract Mathematics
Exercise Sheets

by Ian Biringer, last edited Spring 2022.

1 Logic

1.1 Negations

Exercise 1.1. Negate the following statements. Try to phrase your answer in a shortest possible minimally awkward English sentence that doesn't include the phrases 'it is not true that...' or 'it is not the case that', etc...

1. Every horse is red.

2. If it is raining outside then all frogs laugh.

3. In every war there is a hero that does not die.

To formalize what's going on above, it's convenient to adopt some mathematical shorthand. Let's write $\forall$ for 'for all', $\exists$ for 'there exists', and denote the negation of a statement P by *not* P. Then

$$\textit{not}\,(\forall X, P(X)) = \exists X \text{ such that } \textit{not}\, P(X), \tag{1}$$

$$\textit{not}\,(\exists X \text{ such that } P(X)) = \forall X, \textit{not}\, P(X). \tag{2}$$

Here, we write $P(X)$ to indicate that the P is a statement that accepts an input X, and the truth of P depends on what X is. For example, P could be the statement *"X is a politician"*, so then $P(\textit{Obama})$ is true, while $P(\textit{my cat})$ is false.

Similarly, let's write $P \wedge Q$ for P *and* Q, and write $P \vee Q$ for P or Q. So, $P \wedge Q$ is true when *both* P and Q are true, while $P \vee Q$ is true if *at least one* of the two is true. This interpretation of 'or' is typical in math; the statement P *or* Q *but not both* is a different thing, usually referred to as *exclusive or.*

Fact 1.2. $\textit{not}\,(P \wedge Q) = (\textit{not}\, P) \vee (\textit{not}\, Q)$

Proof. To prove such a statement, we check for each pair of truth values for P and Q whether the two sides of the equation have the same truth value. For instance, if both P and Q are true, then both sides of the equation are false. One way to organize this kind of case by case analysis is with a *truth table.* For example,

P	Q	$P \wedge Q$	$(\textit{not}\, P) \vee (\textit{not}\, Q)$
T	T	T	F
T	F	F	T
F	T	F	T
F	F	F	T

indicates the possible truth values (T or F) of the statements $P \wedge Q$ and $(\textit{not}\, P) \vee (\textit{not}\, Q)$, depending on whether P, Q are true or false. Since these values are negations of each other, the Fact follows.

In general, some words of explanation might be necessary in order to convince the reader of the correct value for a given entry. For instance, if P is false and Q is true, then $\textit{not}\, P$ is true and $\textit{not}\, Q$ is false, so at least one of the two is true, i.e. $(\textit{not}\, P) \vee (\textit{not}\, Q)$ is true. The justifications of the other entries above are similar in length. □

Exercise 1.3. $\textit{not}\,(P \vee Q) = \textit{not}\, P \wedge \textit{not}\, Q$.

Exercise 1.4. Negate the following statements, using the rules discussed above.

1. For every horse that jumps higher than the holy rabbit, there exists a lion that runs faster than the ugly goat and wants to eat that horse.

2. If it's raining outside, then either I will bring an umbrella, or if my raincoat is back from the cleaners, I will wear it.

3. There exists a real number x such that for all real numbers y, we have $x \geq y$.

Exercise 1.5. Suppose I am the coach of our dodgeball team and you all are the players. I tell you "If we win tonight, then I will buy you pizza tomorrow." When can you rightly claim to have been lied to?

1.2 Implications

We write $P \implies Q$ when P *implies* Q, i.e. if Q is true whenever P is. For future use, we will also write $P \iff Q$ when $P \implies Q$ and $Q \implies P$, i.e. when the two statements are logically equivalent. These can also be read as follows:

$P \implies Q$	"if P then Q" or "P only if Q"
$P \iff Q$	"P if and only if Q"

These variants do all mean the same thing. For instance, "P only if Q" means that P is only true when Q is, which is the same thing as saying that whenever P is true, Q is true. So, this is the same as $P \implies Q$.

Remark (Vacuous truth)**.** Say there are no X's. Is the statement "$\forall X, P(X)$" true? For instance, if there has never been a war, is it true that in every war, there's a hero that doesn't die?

If you believe (1) above applies even in the case where there are no X's, then the answer is that yes, "$\forall X, P(X)$" is true. Namely, the statement "$\forall X, P(X)$" is either true, or its negation "$\exists X$ such that $P(X)$" is true. If there are no X's, there cannot exist an X such that $P(X)$. So, the statement "$\forall X, P(X)$" is true. This phenomenon is called *vacuous truth*; it's true because there are no X's to even check.

In some sense, this is all just a convention. It's not completely clear just from the English language whether "$\forall X, P(X)$" should really be true in the absence of X's. And it's not completely clear that (1) should hold when there are no X's, but it makes everything much simpler to interpret it this way.

A similar phenomenon arises when you have a false condition P and you ask whether the statement "$P \implies Q$" is true. Really, you can interpret this as a "for all" statement: "$P \implies Q$" is the same as saying "for all possible conditions in which P is true, Q is also true." So, if there are no conditions where P is true, this statement is vacuously true just as above.

Exercise 1.6. $\textit{not}\,(P \implies Q) = P \wedge \textit{not}\,Q$.

The **converse** of an implication $A \implies B$ is $B \implies A$, while the **contrapositive** of $A \implies B$ is $\textit{not}\,B \implies \textit{not}\,A$.

Exercise 1.7. Let A represent "6 is an even number" and B represent "6 is a multiple of 4." Express each of the following in ordinary English sentences and state whether the statement is true or false.

1. $\textit{not}\,A$
2. $A \wedge B$
3. $A \vee B$
4. $(\textit{not}\,A) \vee B$
5. $A \wedge (\textit{not}\,B)$
6. $A \implies B$
7. $B \implies A$
8. The converse of $(\textit{not}\,B) \implies A$
9. The contrapositive of $A \implies B$

Exercise 1.8. Find the contrapositive of the following statements:

1. If n is an even natural number, then $n+1$ is an odd natural number.

2. If it rains today, then I bring my umbrella.

Exercise 1.9. Provide an example of a true statement whose converse is false.

Theorem 1.10. *Assume A and B are statements. Then $A \implies B$ if and only if $\textit{not}\, B \implies \textit{not}\, A$. That is, an implication is equivalent to its contrapositive.*

Proof. Here is the relevant truth table.

A	B	$A \implies B$	$\textit{not}\, B \implies \textit{not}\, A$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

It should also sort of make sense that $A \implies B$ means that 'B is true whenever A is'. So, the only way that B can be false is if A is false. □

The upshot of Theorem 1.10 is that if you want to prove a conditional proposition, you can prove its contrapositive instead. For instance, an integer n is *even* if $n = 2k$ for some $k \in \mathbb{Z}$, and is *odd* otherwise. Prove the following using the contrapositive, being very literal and careful to use the definition above.

Exercise 1.11. Assume x and y are integers. If xy is odd, then both x and y are odd.

Proof. The contrapositive statement is: If x or y is even, then xy is even.

Say x is even. Then $x = 2k$ for some integer k, by the definition of an even number. Then, $xy = 2ky$. This shows xy is equal to 2 multiplied by some integer ky, so xy is even. This proof can be applied similarly when y is even. □

Exercise 1.12. Let $x, y \in \mathbb{R}$. Show that if $\forall \epsilon > 0$, we have $|x - y| < \epsilon$, then $x = y$.

Although we will use the implication symbols $\implies$, $\iff$, $\impliedby$, we mostly won't use the symbols $\textit{not}\,, \wedge, \vee$ anymore. These are only used in logic texts, and we'll just write 'not' into English sentences, and write 'or' and 'and' instead of $\wedge, \vee$.

1.3 The importance of definitions

Exercise 1.13. Pair up with a friend or divide into groups. Try to write down a precise definition of one of the following geometric objects. Then have your friend or another group try to challenge your definition by coming up with either an example of some object that fits your definition literally, but isn't the object you're describing, or an example of the requested object that doesn't fit your definition.

(a) a circle,

(b) a polygon,

(c) a line,

(d) a cube.

2 Sets

Loosely, a *set* is a collection of *elements*. If S is a set, we write $x \in S$ if x is an element of S. Here, $\in$ can be read as 'is in'. A precise definition of sets would take us farther into logic than is appropriate at this time, so we will be omit it here. See Russel's paradox (below) for a hint at why a more formal definition is necessary.

A set is often presented in one of the following forms:

- A complete list of its elements: the set $S = \{1, 2, 3, 4, 5\}$ contains precisely the five smallest positive integers.
- A list of some of its elements, with ellipses to indicate unnamed elements: e.g., the set $S = \{3, 4, 5, \ldots, 100\}$ contains the positive integers from 3 to 100, including 6 through 99, even though these latter are not explicitly named. We also have the familiar examples of the *natural numbers*

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

  and the *integers*

  $$\mathbb{Z} := \{\ldots, -2, -1, 0, 1, 2, \ldots\},$$

  as well as the set of all real numbers $\mathbb{R}$ and the set of rational numbers $\mathbb{Q}$ (i.e. the set of all integer fractions p/q), which we'll assume you have seen before.

  In this course, you'll often see ':=' written instead of '=' when we want to emphasize that something is a definition*, rather than an equality of previously defined objects.*

- By specifying a rule that picks out certain elements of a larger set, and puts them into a new set. The notation we use is:

  { things in the bigger set | conditions they have to satisfy to be in the subset }.

  As an example, we can write the set of even numbers as

  $$\{x \in \mathbb{N} \mid x = 2k \text{ for some } k \in \mathbb{Z}\}.$$

  Similarly, the set of all integers whose squares are less than 3 is written

  $$\{x \in \mathbb{Z} \mid x^2 < 3\}.$$

- An alternative way to describe sets is via a rule (a 'function') that produces certain elements in a set from others. Such a description is written as

  { rule producing something from certain elements | those elements }.

  For example, the even numbers are exactly those number that are doubles of integers, so the set of even numbers can be written as

  $$\{2k \mid k \in \mathbb{Z}\}.$$

We say two sets A and B are equal if they contain precisely the same elements, that is, if $x \in A$ if and only if $x \in B$.

Definition 2.1. The *empty set* is the set with no elements, and it is denoted $\emptyset$.

Exercise 2.2. Is it true that every element of the empty set is a whistling, flying purple cow?

2.1 Subsets of sets

We say that a set A is a *subset* of a set B, written $A \subset B$, if every element of A is also an element of B, that is, if $x \in A$, then $x \in B$. Note that $A = B$ if and only if $A \subset B$ and $B \subset A$.

Exercise 2.3. How many subsets does the empty set have?

Exercise 2.4. Let $A = \{1, \{2\}\}$. Is $1 \in A$? Is $2 \in A$? Is $\{1\} \subset A$? Is $\{2\} \subset A$? Is $1 \subset A$? Is $\{1\} \in A$? Is $\{2\} \in A$? Is $\{\{2\}\} \subset A$? Explain.

Definition 2.5. Let A be a set. The *power set* of A is the sets of all subsets of A and is denoted $\mathcal{P}(A)$. That is, $\mathcal{P}(A) = \{B \mid B \subset A\}$.

Exercise 2.6. Let $A = \{1, 2, 3\}$. Identify $\mathcal{P}(A)$ by explicitly listing its elements.

Exercise 2.7. Suppose that A is a set with n elements. How many elements does $\mathcal{P}(A)$ have? *An informal argument is fine. To make a subset, you have to decide for each element, whether to put it in the set or not to put it in the set.*

For each non-negative integer n, let $\binom{n}{k}$ denote the number of subsets of $\{1, \ldots, n\}$ of size k. If $k < 0$ or $k > n$ then let $\binom{n}{k} = 0$. Here, $\binom{n}{k}$ is pronounced *n choose k*.

Exercise 2.8. Calculate $\binom{4}{2}$ by listing all the 2-element subsets of $\{1, 2, 3, 4\}$.

Exercise 2.9. Show that $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ for $1 \leq k \leq n$. *Hint: take a subset of* $\{1, \ldots, n\}$ *and break into cases depending on whether it contains n or not.*

The preious exercise gives a nice way of calculating $\binom{n}{k}$, via *Pascal's triangle*, pictured below in arabic numerals and in Chinese rod numerals. (It was actually studied centuries before Pascal by various people around the world, but for some reason we still call it Pascal's triangle.)

1

1 1

1 2 1

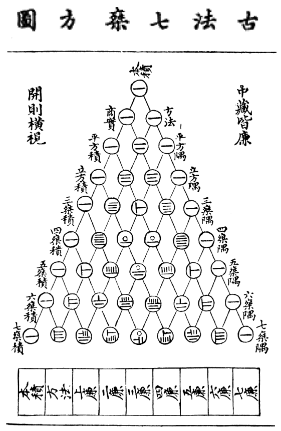
1 3 3 1

1 4 6 4 1

1 5 10 10 5 1

1 6 15 20 15 6 1

1 7 21 35 35 21 7 1



Exercise 2.10. Figure out what the above triangle has to do with the numbers $\binom{n}{k}$, and prove your answer. Then write out the next row.

If n is a natural number, n *factorial* is the number

$$n! = n \cdot (n-1) \cdots 1.$$

For example, $5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$. Note that $n!$ is exactly the number of *permutations* of $1, 2, 3, \ldots, n$, i.e. the. number of ways to list these numbers in some order. For example, $3! = 6$ and there are six permutations of $1, 2, 3$:

$$123, 132, 213, 231, 312, 321.$$

The reason why $n!$ counts permutations is that you have n choices for the first element, $(n-1)$-choices for the second, etc...

Exercise 2.11. Show that $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

Exercise 2.12. What is $\sum_{k=1}^{n} \binom{n}{k}$?

Exercise 2.13. Marcello hosts a party with 10 people, himself included. There is a toast and everyone clinks glasses. How many clinks are heard?

2.2 Unions, Intersections and Products

Definition 2.14. Let A and B be two sets. The *union* of A and B is the set

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

Definition 2.15. Let A and B be two sets. The *intersection* of A and B is the set

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

Theorem 2.16 (Distribution of Union and Intersection)**.** *If A, B, and C are sets,*

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

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

Exercise 2.17. Prove part (a) above.

Definition 2.18. Two sets A and B are *disjoint* if $A \cap B = \emptyset$.

Exercise 2.19. Can a set be disjoint from itself?

Definition 2.20. Let A and B be two sets. The *difference* of A and B is the set

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

When $B \subset A$, the set $A \setminus B$ is also called the *complement* of B in A.

Theorem 2.21. *(DeMorgan's Laws) Let X be a set, and let $A, B \subset X$. Then:*

1. $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$
2. $X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B)$

Exercise 2.22. Prove one of the two parts of DeMorgan's laws.

Exercise 2.23. If $X = \{\text{voters}\}$, $A = \{\text{libertarians}\}$ and $B = \{\text{republicans}\}$, what do DeMorgan's laws say?

Exercise 2.24. If S, T are sets, is it true that $\mathcal{P}(S) \cup \mathcal{P}(T) = \mathcal{P}(S \cup T)$?

Definition 2.25. If A, B are sets, their *(Cartesian) product* is the set

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

of all 'ordered pairs' of elements from A and B, respectively. We can also take a product of any number of sets, e.g.

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

Elements of $A_1 \times \cdots \times A_n$ are called *n-tuples.* Note that $(A \times B) \times C$ is basically the same as $A \times B \times C$, although technically one should write elements of the former set as $((a, b), c)$ instead of (a, b, c), but we'll ignore this from now on. Also, we define

$$A^n = A \overset{n\ times}{\times \cdots \times} A.$$

Note that if $\mathbb{R}$ is the set of real numbers, $\mathbb{R}^2$ is then the plane. If

$$M = \{Subaru, Honda, Ford, Chevrolet, \ldots\}$$

is the set of all car makes, and

$$C = \{red, blue, \ldots\}$$

is the set of all (named) colors, then $M \times C$ is the set of all pairs of car makes with colors, which is useful set if you are buying a car.

Exercise 2.26. How many elements does $\{1, \ldots, m\} \times \{1, \ldots, n\}$ have?

Exercise 2.27. What is $\mathbb{N} \times \emptyset$?

Exercise 2.28. Show that for all sets A, B, C, D, we have

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

2.3 Math is broken

Let $\mathcal{S}$ be the set of all sets, and let $\mathcal{R} := \{A \in \mathcal{S} \mid A \notin A\}$. i.e. $\mathcal{R}$ is the set of all sets that don't contain themselves as elements.

Exercise 2.29. (Russel's Paradox) Find a contradiction in mathematics by studying whether $\mathcal{R}$ is an element of $\mathcal{R}$.

A colloquial restatement of this goes as follows. *In Seville, there is a barber who shaves all those men, and only those men, who do not shave themselves. So, who shaves the barber?*

Is math broken? What the exercise indicates is that it is problematic to assume that there is something like the 'set of all sets', and that we need a stricter definition of a set than 'some collection of elements'. Essentially, the way to resolve this is as follows. Starting out with some basic building blocks like the empty set, and say for simplicity $\mathbb{N}$, we only allow ourselves to look at sets constructed from these by natural set operations like unions, products, taking subsets, power sets, etc.... Writing down the rules precisely is pretty subtle, though, so we'll ignore all that and just naively assume that all reasonable expressions we write down do describe sets.

2.4 The halting problem

The following is sort of similar to Russell's paradox, although it doesn't have anything to do with sets.

A computer program *halts* if it eventually stops running. For example, consider a program **Admirer** that takes an input X and then prints "I love X" on the screen. Compare this with a program **Stalker** that takes in an input X and then repeatedly writes "I love X" on the screen until you recycle your computer in 2025. The first program halts, while the second doesn't. Now each computer program can be encoded as a text file, say, so can be an input to another program. The *halting problem* asks if there's a single computer program that takes as an input a computer program P (say, encoded as a text file) together with another text input X, and prints "Yes" if P halts when fed the input X, and "No" if it doesn't. Here, you should imagine that X is always a string of characters, which P accepts as an input.

Exercise 2.30. Show that there is no such program. *Hint: Hoping for a contradiction, suppose there is a program that solves the halting problem, and call this program* Halt. *Write a program* Paradox *that takes as input a program P and prints "It doesn't halt on itself" if P doesn't halt when fed the input P, and prints "It halts!!!" repeatedly forever if P halts when fed the input P. What's the paradox?*

3 Number Theory

We will start in now with a bit of number theory. As always, $\mathbb{Z}$ will denote the set of integers. You are allowed to assume that all usual properties of addition, subtraction and multiplication of integers work in the usual ways, and interact as expected with the usual order $<$ on $\mathbb{Z}$. For instance, addition is commutative and multiplication distributes over addition, and if $a \leq b$ then $a + c \leq b + c$ for all c.

Theorem 3.1 (Division with remainder)**.** *If $a, b \in \mathbb{Z}$ and $b > 0$, then there exist unique integers q and r such that $a = bq + r$ and $0 \leq r < b$.*

Exercise 3.2. If $a = 7$ and $b = 314$, find q and r. What about if $a = -11$ and $b = 30$?

The following two exercises complete the proof of Theorem 1.

Exercise 3.3. Given a, b as in Theorem 1, let q the largest integer such that $bq \leq a$. Show that $a = bq + r$ where $0 \leq r < b$.

Exercise 3.4. Suppose q_1, r_1 and q_2, r_2 are integers with $0 \leq r_1, r_2 < b$ and

$$a = bq_1 + r_1 = bq_2 + r_2.$$

Show that $q_1 = q_2$ and $r_1 = r_2$.

3.1 Greatest common divisors

Recall that if $a, b \in \mathbb{Z}$, then a *divides* b if there is some integer k with $b = ak$, and we call a a *divisor* of b, while b is a *multiple* of a. We write $a|b$ when this is the case.

Definition 3.5. Let $a, b \in \mathbb{Z}$, not both zero. A *common divisor* of a and b is defined to be any integer c such that $c|a$ and $c|b$. The largest common divisor is usually called the *greatest common divisor* of a and b, and is denoted $gcd(a, b)$.

Exercise 3.6. List all the common divisors of 18 and 24, and find $gcd(18, 24)$.

We say a, b are *relatively prime* or *co-prime* if $gcd(a, b) = 1$.

Exercise 3.7. Let f_n be the Fibonacci sequence. Show that f_n and f_{n+1} are relatively prime for all positive integers n.

Given $a, b \in \mathbb{Z}$, an expression of the form $xa + yb$, where $x, y \in \mathbb{Z}$, is called a *$\mathbb{Z}$-linear combination* of a, b. The numbers x, y are called the *coefficients* of the linear combination. For instance, the following are $\mathbb{Z}$-linear combinations of 3 and 7:

$$-2 \cdot 3 + 5 \cdot 7 = 36, \qquad 0 \cdot 3 - 1 \cdot 7 = -7, \qquad 100 \cdot 3 + 2 \cdot 7 = 314.$$

We define

$$S(a, b) = \{xa + yb \mid x, y \in \mathbb{Z}\}$$

to be the set of all such $\mathbb{Z}$-linear combinations of a and b.

Exercise 3.8. Try to write all elements of $S(18, 24)$ that are between 0 and 50. At some point you'll ask... "How do I know I'm done?" After you ask yourself that, stop writing and move on.

To understand $\mathbb{Z}$-linear combinations (and most other things), consider cake. A delicious birthday cake can be expressed in the form

$$\begin{aligned} \textit{cake} = {} & (1\ \textit{tbsp}) \cdot \textit{vanilla} + (15\ \textit{tbsp}) \cdot \textit{eggs} + (8\ \textit{tbsp}) \cdot \textit{butter} + \\ & (24\ \textit{tbsp}) \cdot flour + (1\ \textit{tbsp}) \cdot \textit{baking powder} + (8\ \textit{tbsp}) \cdot \textit{hot milk}. \end{aligned}$$

This is a real recipe[1]. For students from more civilized countries, tbsp = *tablespoon*, a bizarre unit of measurement that in the US[2] is a little under 15 ml.

Here's another real world example.

Exercise 3.9. Show that any possible amount x of postage that is at least 8 cents can be made using some combination of 3 cent and 5 cent stamps.

In these examples, we are always using nonnegative coefficients. Indeed, it is hard to imagine a cake recipe where first you mix together 24 tbsp of flour and 15 tbsp of eggs, and then somehow remove from that 1 tbsp of vanilla extract. However, in general the coefficients in $\mathbb{Z}$-linear combinations may be negative. For a cake-related interpretation of $S(a, b)$, suppose you have two measuring cups, where one holds a tbsps and one holds b tbsps. Imagine you have an unlimited supply of flour in your pantry, and an (infinitely) big bowl in front of you. You now transfer flour into and out of the bowl using your two measuring cups. For instance, you could use your a-tbsp cup 20 times to fill up the bowl, and then remove 7 scoops using your b-tbsp cup. The possible amounts of flour you can get in the bowl are all the positive elements

[1] http://allrecipes.com/recipe/17481/simple-white-cake/

[2] In Canada and the UK, 1 tbsp is exactly 15 ml, and in Australia, it is 20 ml.

of $S(a,b)$. (It's hard to have a negative amount of flour in a bowl, since a bowl can't carry flour debt.)

Now the set $S(a,b)$ always contains positive integers (e.g. it contains $\pm a$ and $\pm b$, and one of these four is positive) so it contains a *least* positive integer $d(a,b)$.

Exercise 3.10. Show that any common divisor of a, b also divides $d(a,b)$.

Exercise 3.11. Show that $d(a,b)$ is a common divisor of a, b.

Combining Exercises 3.10 and 3.11, we see that $d(a,b) = gcd(a,b)$. So, this proves:

Theorem 3.12. *If $a, b \in \mathbb{Z}$, not both zero, there are $x, y \in \mathbb{Z}$ such that*

$$gcd(a,b) = xa + yb.$$

Exercise 3.13. By hand, find x, y such that $gcd(21,27) = x21 + y27$.

In fact, more is true.

Exercise 3.14. Show that $S(a,b)$ is exactly the set of all multiples of $gcd(a,b)$. *Hint: for one direction, use that $gcd(a,b) \in S(a,b)$, as above.*

At this point, you are probably fed up with computing greatest common denominators and the associated x, y coefficients by hand. Luckily, there is an easier way.

Theorem 3.15 (The Euclidean Algorithm)**.** *Let $a, b \in \mathbb{Z}$ be positive integers, not both zero. Then we can apply division with remainder repeatedly to find q_i, r_i as follows:*

$$\begin{array}{rcll}
a &=& bq_1 + r_1 & \qquad 0 < r_1 < b \\
b &=& r_1q_2 + r_2 & \qquad 0 < r_2 < r_1 \\
r_1 &=& r_2q_3 + r_3 & \qquad 0 < r_3 < r_2 \\
&\vdots&& \\
r_{k-2} &=& r_{k-1}q_k + r_k & \qquad 0 < r_k < r_{k-1} \\
r_{k-1} &=& r_kq_{k+1}, &
\end{array}$$

and where $r_k = gcd(a,b)$.

Exercise 3.16. Use the Euclidean algorithm to find $gcd(18,24)$ and $gcd(75,-21)$.

Let's see how to prove the Euclidean algorithm. Given a, b, we can certainly just keep dividing with remainder, which produces a decreasing sequence of positive integers r_i. This can't go on forever, so at some point we terminate with some r_k where the next remainder is zero. The point is to show that this $r_k = gcd(a,b)$.

Exercise 3.17. Given a, b, use strong induction to show that for each $i = 1, \ldots, k$, the remainder r_i is a $\mathbb{Z}$-linear combination of a, b. In particular, this is true for r_k.

Exercise 3.18. For convenience in notation, set $r_0 = b$, $r_{-1} = a$, and $r_{k+1} = 0$, so that for all $i = -1, \ldots, k-1$ we have

$$r_i = r_{i+1}q_{i+2} + r_{i+2}.$$

Using strong induction 'backwards', show that for each $i = -1, \ldots, k-1$, we have that $r_k | r_i$. In particular, r_k is a common divisor of a, b.

Exercise 3.19. Prove Theorem 3.15.

If you've understood the proof of the Euclidean Algorithm, you should be able to use the same methods now to find the x, y in (3.12) algorithmically!

Exercise 3.20. Use the method of the proof of Exercise 15 to find x, y such that

$$x81 + y173 = 1.$$

3.2 More primes

Recall that a natural number $p \geq 2$ is *prime* if its only positive divisors are 1 and itself. A natural number $n \geq 2$ is *composite* if n is not prime. Previously, we showed:

Theorem 3.21. *Any natural number n can be written as a product*

$$n = p_1 \cdots p_k,$$

where $p_1, \ldots, p_k$ are all prime.

Often, when we write n as such a product, we say that we have *factored* n. The terms in the product are the *factors*.

Exercise 3.22. If p is prime and p does not divide $a \in \mathbb{N}$, show that $gcd(p, a) = 1$.

Exercise 3.23. Let $a, b, n \in \mathbb{N}$ and assume $gcd(a, n) = 1$ and $n|ab$. Show that $n|b$. Then conclude that if p is prime and $p|ab$, then $p|a$ or $p|b$.

Exercise 3.24. Let p be prime and $a_1, \ldots, a_k$ be natural numbers. If $p|a_1 \cdots a_k$, show that $p|a_i$ for some i. *Hint: do induction on k.*

In particular, if the a_i in Exercise 3.24 are all prime, then we have that $p = a_i$ for some i. Using this, you should now prove:

Theorem 3.25 (The Fundamental Theorem of Arithmetic)**.** *Every integer $n \geq 1$ may be factored into a product of primes in a unique way up to the order of the factors. In other words, if $n = p_1 \cdots p_k = q_1 \cdots q_l$ are two prime factorizations of n, then $k = l$ and we can reorder the q_i's so that $p_1 = q_1, p_2 = q_2, \ldots, p_k = q_k$.*

Hint: it may be useful to do induction on n. The base case $n = 1$ is trivial.

Exercise 3.26. Suppose that $n = p_1^{e_1} \cdots p_k^{e_k}$ and $m = p_1^{f_1} \cdots p_k^{f_k}$, where $p_1, \ldots, p_k$ are prime and $e_i, f_i \geq 0$. Show that

$$gcd(m,n) = p_1^{\min\{e_1,f_1\}} \cdots p_k^{\min\{e_k,f_k\}}.$$

Here, $\min\{x,y\}$ is just the minimum of x, y, i.e. whichever one is smaller. Note that in the exercise, we can allow e_i or f_i to be zero. This allows us to apply the exercise to *any* pair of natural numbers n, m. For instance, we can write

$$60 = 2^2 \cdot 3^1 \cdot 5^1 \cdot 7^0, \quad 35 = 2^0 \cdot 3^0 \cdot 5^1 \cdot 7^1,$$

and then $gcd(60, 35) = 2^0 \cdot 3^0 \cdot 5^1 \cdot 7^0 = 5$.

A natural number n is a *perfect square* if there is some $a \in \mathbb{N}$ with $a^2 = n$. Here are some examples of perfect squares and their prime factorizations:

$$9 = 3^2, \quad 64 = 2^6 \quad 36 = 2^2 \cdot 3^2, \quad 400 = 2^4 \cdot 5^2.$$

Exercise 3.27. Show that n is a perfect square if and only if every prime factor occurs an even number of times in the (essentially unique) prime factorization of n.

A real number x is defined to be *rational* if there exist integers p and q such that $x = p/q$ and *irrational* otherwise.

Exercise 3.28. Show that if $n \in \mathbb{N}$ is not a perfect square, then $\sqrt{n}$ is irrational.

So in particular, $\sqrt{2}$ is irrational.

Exercise 3.29. Show that there are infinitely many primes. *Hint: hoping for a contradiction, suppose that the only primes are $p_1, \ldots, p_k$ and consider $n = p_1 \cdots p_k + 1$.*

Exercise 3.30. Show that there are infinitely many primes of the form $4n + 3$.

Finally, try to digest the statement of the following theorem, for inspiration. I don't expect you to prove it, although if you do some sort of medal is in order.

Theorem 3.31 (The prime number theorem)**.** *Given a positive number x, let $\pi(x)$ be the number of primes that are less than or equal to x. Then*

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1.$$

What does this mean? If I randomly give you a number between 1 and 100000000000, is a likely to be prime? How much less likely is it that you get a prime number if I randomly give you a number between 1 and 1000000000000000000000000?

4 Functions

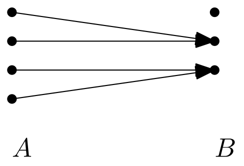
A *function* is a rule that assigns to every element of a set A, an element of another set B. We write functions in the form $f : A \longrightarrow B$. Here, the element of B that the function assigns to an element $a \in A$ is written $f(a)$.

Definition 4.1 (Domain, codomain and range)**.** The *domain* of f is A, and its *codomain* is B. The *image*, or *range*, of f is the set

$$f(A) = \{f(a) \mid a \in A\}$$

Exercise 4.2. What are the domain, codomain and image of the function $f : \mathbb{R} \longrightarrow \mathbb{R}, \quad f(x) = x^2 - 5$?

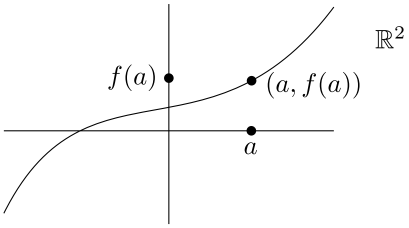
Here are two ways to picture a function. First, you can use dots to represent points in A and in B, and draw an arrow from each $a \in A$ to $f(a) \in B$.



Another way is to look at the function's graph. Namely, if $f : A \longrightarrow B$ is a function, then we define *graph*(f) to be the subset of the product $A \times B$ given by

$$graph(f) := \{(a, f(a)) \mid a \in A\} \subset A \times B.$$

If $f : \mathbb{R} \longrightarrow \mathbb{R}$, then *graph*$(f)$ is the familiar subset of $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ you might remember from calculus.



Definition 4.3 (Surjective, injective and bijective)**.** A function $f : A \to B$ is *surjective*, or *onto*, if $f(A) = B$. It is *injective*, or *one-to-one* if for all $a_1, a_2 \in A$, we have $f(a_1) = f(a_2)$ only if $a_1 = a_2$. It is *bijective* if it is surjective and injective.

For example, the function drawn with arrows and dots above is neither injective nor surjective. The function $f : \mathbb{R} \longrightarrow [-5, \infty)$, $f(x) = x^2 - 5$ is surjective but not injective.

Exercise 4.4. Determine whether the following are injective, surjective or bijective.

1. $f : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z},\ f(n) = (n, n)$
2. $f : \mathbb{Z} \to \mathbb{Z},\ f(n) = \begin{cases} n & n \geq 0 \\ n+5 & n < 0. \end{cases}$
3. $g : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z},\ g(m, n) = m + n$
4. $h : \mathbb{R} \times (\mathbb{R} \setminus \{0\}) \to \mathbb{R},\ h(x, y) = \frac{x}{y}$

Exercise 4.5. (Challenge!) Is there a bijection $f : [0, 1] \longrightarrow (0, 1)$?

Definition 4.6. The *composition* of $f : A \longrightarrow B$ and $g : B \longrightarrow C$ is the function

$$g \circ f : A \longrightarrow C,\ g \circ f(a) = g(f(a)).$$

Exercise 4.7. Write nice-looking formulas for the compositions $f \circ g$ and $g \circ f$, where

$$f : \mathbb{R}^2 \longrightarrow \mathbb{R},\ f(x, y) = \frac{x}{y^2 + 1},\quad g : \mathbb{R} \longrightarrow \mathbb{R}^2,\ g(x) = \left(x^2, x\right).$$

Exercise 4.8.

1. Show that the composition of two injective functions is injective.
2. Show that the composition of two surjective functions is surjective.
3. Show that if $g \circ f$ is surjective, so is g.

4. If $g \circ f$ is surjective, does f have to be surjective? (Either prove it or give a counterexample.)

Definition 4.9 (Image and preimage of subsets)**.** Let $f : A \to B$ be a function. Let $X \subseteq A$. Then the *image of X under f* is

$$f(X) = \{f(x) \mid x \in X\}$$

Let $Y \subseteq B$. Then the *preimage of Y under f* is

$$f^{-1}(Y) = \{a \in A \mid f(a) \in Y\}$$

Exercise 4.10. Identify the following images and preimages.

1. $f([-1, 6])$, where $f : \mathbb{R} \longrightarrow \mathbb{R},\ f(x) = x^2$,

2. $f^{-1}([4, 9])$, where $f : \mathbb{R} \longrightarrow \mathbb{R},\ f(x) = x^2$,

3. $g^{-1}([1, 2] \times [3, 5])$, where $g : \mathbb{R} \longrightarrow \mathbb{R}^2,\ g(x) = (x, x^2)$.

Exercise 4.11. Let $f : A \to B$ be a function. In each of the following, decide if the statement is true. If so, prove it. If not, give an explicit counterexample and then try to prove it under an additional assumption that f is either surjective or injective.

1. $f^{-1}(f(X)) = X$ for all $X \subseteq A$.

2. $f(f^{-1}(Y)) = Y$ for all $Y \subseteq B$.

3. $f(X_1 \cap X_2) = f(X_1) \cap f(X_2)$ for all $X_1, X_2 \subseteq A$.

4. $f^{-1}(Y_1 \cap Y_2) = f^{-1}(Y_1) \cap f^{-1}(Y_2)$ for all $Y_1, Y_2 \subseteq B$.

Definition 4.12. Let $f : A \longrightarrow B$ be a bijection. The *inverse* of f is the function

$$f^{-1} : B \longrightarrow A,$$

where $f^{-1}(b)$ is the unique element $a \in A$ such that $f(a) = b$.

This is a slight abuse of notation, since we previously used the symbol f^{-1} to denote the preimage. However, it should always be clear from context whether we are referring to the preimage or to the inverse function.

Exercise 4.13. Show the following are bijections, and find the inverse.

1. $f : \mathbb{R} \longrightarrow \mathbb{R}$, $f(x) = (5x - 2)/12$.

2. $g : \mathbb{N} \cup \{0\} \longrightarrow \mathbb{Z},\ g(n) = \begin{cases} 0 & n = 0 \\ \frac{n}{2} & n \text{ is even} \\ -\frac{n+1}{2} & n \text{ is odd.} \end{cases}$

3. $h : \mathbb{R} \longrightarrow \{(x, y) \in \mathbb{R}^2 \mid y = 2x\},\ h(x) = (x, 2x)$.

Exercise 4.14. What is a function, really? That is, say that you're comfortable with all the stuff from our set theory sheet. Can you give a definition of a function using only the language of set theory, without saying vague things like 'rule that assigns'?

5 Equivalence Relations

Let A be a set. For every pair $a, b \in A$, let's write either $a \sim b$ or $a \not\sim b$, read as *'a is related to b'* and *'a is not related to b'*, respectively. An arbitrary way to do this for each pair is called a *relation* on A.

Example 5.1. If $a, b \in \mathbb{Z}$, declare $a \sim b$ if $a \leq b$, and $a \not\sim b$ otherwise.

We say that a relation $\sim$ is an *equivalence relation* if the following properties are satisfied.

(1) for all $a \in A$, we have $a \sim a$ (reflexivity),

(2) for all $a, b \in A$, if $a \sim b$ then $b \sim a$ (symmetry),

(3) for all $a, b, c \in A$, if $a \sim b$ and $b \sim c$ then $a \sim c$ (transitivity).

If $\sim$ is an equivalence relation, we often read $a \sim b$ as 'a is equivalent to b', rather than using the word 'related', but either works. Note that the relation $a \sim b$ if $a \leq b$ is not an equivalence relation on $\mathbb{Z}$: we have $2 \leq 3$ but $3 \not\leq 2$, so the relation isn't symmetric.

Example 5.2. If A is any set, define $a \sim b$ if $a = b$. This is an equivalence relation on A. Namely, $a = a$ for all $a \in A$, so it's reflexive. If $a = b$, then $b = a$, so it's symmetric. If $a = b$ and $b = c$, then $a = c$, so it's transitive.

Really, the whole point of equivalence relations is to have some notion of 'similarity' between elements of A that behaves kind of like equality.

Exercise 5.3. Are the following equivalence relations?

1. Let L be the set of lines on the plane. For $a, b \in L$ let $a \sim b$ if a and b are parallel. *Here, lines are parallel if they are disjoint or identical.*

2. Let $\mathcal{P}$ be the set of polygons in the plane, where $P \sim Q$ if P is congruent to Q.

3. For $a, b \in \mathbb{Z}$, let $a \sim b$ if $a - b$ is odd.

4. Fix $n \in \mathbb{Z}$, and for $a, b \in \mathbb{Z}$ let $a \sim_n b$ if $a - b$ is a multiple of n.

5. Let X be a set, and consider the relation $\sim$ on the power set $\mathcal{P}(X)$, where $A \sim B$ if $A \cap B \neq \emptyset$.

6. Let $\mathcal{F}$ be the set of all functions $f : \mathbb{R} \longrightarrow \mathbb{R}$, and define $f \sim g$ if there is some finite subset $S \subset \mathbb{R}$ such that $f(x) = g(x)$ for all $x \notin S$.

Here is an especially important example. Suppose that $f : A \longrightarrow X$ is a function. Let's define a relation $\sim_f$ on A by declaring $a \sim_f b$ when $f(a) = f(b)$.

Exercise 5.4. Show that $\sim_f$ is an equivalence relation.

For example, if we take $f : \mathbb{R}^2 \longrightarrow \mathbb{R}$, $f(x, y) = \sqrt{x^2 + y^2}$ then $a, b \in \mathbb{R}^2$ are related exactly when they have the same length. In general, this exercise says that whenever we define a relation by saying '*$a \sim b$ if a and b have the same blarhgh*', it will automatically be an equivalence relation, since we can take

$$blarhgh : A \longrightarrow \{ \text{ possible values of blarhgh } \}.$$

as our function in Exercise 5.4. Do any of the examples in Exercise 5.3 arise like this?

Exercise 5.5. Is the following theorem correct?

Theorem 5.6. *Suppose $\sim$ is a relation on a set A that's symmetric and transitive. Then $\sim$ is reflexive.*

Exercise 5.7. Suppose that $\sim_1, \sim_2$ are two equivalence relations on A. Define a new relation $\sim$ by setting $a \sim b$ when $a \sim_1 b$ and $a \sim_2 b$. Show that $\sim$ is an equivalence relation. What happens if you use 'or' instead of 'and' in the construction?

Exercise 5.8. Can you give a rigorous interpretation of an equivalence relation in terms of set theory? $\sim$ should be defined to be a certain subset of something.

5.1 Equivalence classes

Let A be a set and let $\sim$ be an equivalence relation on A. Then for $a \in A$, the *$\sim$-equivalence class of* a is defined as

$$[a]_\sim = \{x \in A \mid a \sim x\}$$

When the equivalence relation is understood, we will sometimes just write $[a]$ instead of $[a]_\sim$. For example, if ℓ is a line in $\mathbb{R}^2$ and $\sim$ is as in Exercise 5.3 (a), then $[\ell]$ is the set of lines parallel to a.

Exercise 5.9. Determine the following equivalence classes, by writing out a set theoretic description of all the elements in them.

1. The $\sim_2$-equivalence class of 5 in Exercise 5.3 (c).
2. The $\sim_f$-equivalence class of the point $(1, 0) \in \mathbb{R}^2$, where f is the function defined just after Exercise 5.4.

Exercise 5.10. Suppose that $\sim$ is an equivalence relation on X. Show that

1. if $a \sim b$ then $[a] = [b]$,
2. if $a \not\sim b$ then $[a] \cap [b] = \emptyset$.

Example 5.11. Suppose that $\sim_n$ is the equivalence relation on $\mathbb{Z}$ defined as in Exercise 5.3 (c), i.e. where $a \sim_n b$ if $a - b$ is a multiple of n. By division with remainder, every $m \in \mathbb{Z}$ has the form

$$m = qn + r, \quad q \in \mathbb{Z}, r \in \{0, \ldots, n-1\},$$

in which case $m \sim r$, so $[m] = [r]$. Moreover, if $r, s \in \{0, \ldots, n-1\}$ and $r \neq s$, then $s - r$ cannot be divisible by n, so $r \not\sim s$, implying $[r] \neq [s]$. In other words, the equivalence relation $\sim_n$ has exactly n equivalence classes, which are

$$[0], [1], [2], \ldots, [n-1].$$

5.2 Quotient sets

Suppose $\sim$ is an equivalence relation on X. The corresponding *quotient set* is

$$X/\sim := \{[a] \mid a \in X\},$$

the set of all $\sim$-equivalence classes.

Exercise 5.12. Define a map $\pi : X \longrightarrow X/\sim$, where $\pi(x) = [x]$. Show that the equivalence relation $\sim_\pi$ of Exercise 5.4 is just the original $\sim$. This shows that in fact, every equivalence relation comes from the construction in Exercise 5.4.

Many natural mathematical objects are constructed as quotient sets of equivalence relations. For instance, let's assume that we are children that know about integers and set theory. How do we define the set of rational numbers $\mathbb{Q}$? We say that a rational number is just an integer fraction, but there are coincidences like

$$\frac{a}{b} = \frac{-a}{-b} = \frac{2a}{2b}$$

and if you only know about integer arithmetic it's not clear what that horizontal line between the a and the b is supposed to mean, as $2/3$ has no intrinsic meaning. However, you can at least express what the coincidences are that you want to deal with just using integer arithmetic, since

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

Exercise 5.13. Let $S = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid b \neq 0\}$ and define $(a, b) \sim (c, d)$ if $ad = bc$. Show that $\sim$ is an equivalence relation.

We now just define $\mathbb{Q} := S/\sim$. This as a very nice, but currently it is just a set that we for some reason are calling by a suggestive name. In order for the set to really behave like rational numbers, we need to say what it means to add and multiply elements of the set. For instance, suppose we have $x, y \in \mathbb{Q}$ and want to define $x + y$. Well, by definition we have $x = [(a, b)]$ and $y = [(c, d)]$ for some $a, b, c, d \in \mathbb{Z}$, where $b, d \neq 0$. We'd like to make our definition so that it satisfies the usual law

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

so the way to do it using our current notation is to write:

$$\text{if } x = [(a, b)] \text{ and } y = [(c, d)], \text{ then } x + y := [(ad + bc, bd)]. \tag{3}$$

There's a subtlety here. Suppose for a moment that we try to define a similar operation called $\oplus$ on $\mathbb{Q}$, where $x \oplus y := [(a + c, b + d)]$. (This is the naive way that children without our sophistication might try to add fractions.) Now of course, you probably will object and say 'that's not a good way to do it', but can you say concretely why it's not a good definition? Let's get a feeling for how this new sort of addition works. Here are two examples:

$$\begin{aligned}&\text{If } x = [(0,1)] \text{ and } y = [(1,2)], \text{ then } x \oplus y := [(1,3)].\\&\text{If } x = [(0,2)] \text{ and } y = [(3,6)], \text{ then } x \oplus y := [(3,8)].\end{aligned}$$

This all seems very nice until you notice that the x's in the two examples are actually the same, as are the two y's. Namely, $(0,1) \sim (0,2)$ and $(1,2) \sim (3,6)$, so the associated equivalence classes are the same. However, $(1,3) \not\sim (3,8)$, so you get different definitions of $x \oplus y$ depending on which elements you are using to represent the equivalence classes! That's ridiculous. In the situation, we say that the problem is that $\oplus$ is not *well-defined.*

Exercise 5.14. Is the function $f : \mathbb{Q} \longrightarrow \mathbb{Z}$, $f([(a,b)]) = b$ well defined?

Exercise 5.15. Consider the equivalence relation $\sim$ on the set $\mathcal{F}$ of all functions $f : \mathbb{R} \longrightarrow \mathbb{R}$ from Exercise 5.3 (f). Is the following function well defined?

$$Z : \mathcal{F}/\sim \longrightarrow \mathbb{R}, \quad Z([f]) = f(0)$$

Exercise 5.16. Show that $+$ is *well-defined* by (3), meaning that the equivalence class $x + y$ doesn't depend on the particular choices of $(a,b) \in x$ and $(c,d) \in y$.

Exercise 5.17. Define multiplication on $\mathbb{Q}$ and show it is well-defined. Then prove that $x(y + z) = xy + xz$ for all $x, y, z \in \mathbb{Q}$.

Exercise 5.18. Let $\mathbb{Z}/n\mathbb{Z} := \mathbb{Z}/\sim_n$ be the set of $\sim_n$-equivalence classes on $\mathbb{Z}$, where $a \sim_n b$ if $a - b$ is divisible by n. Show that

$$\begin{aligned}&\text{“If } x = [a] \text{ and } y = [b], \text{ then } x + y := [a+b].''\\&\text{“If } x = [a] \text{ and } y = [b], \text{ then } x \cdot y := [ab].''\end{aligned}$$

give well-defined notions of addition and multiplication on $\mathbb{Z}/n\mathbb{Z}$.

Here, you can imagine an element of $\mathbb{Z}/12\mathbb{Z}$ as an ‘hour’ on the clock. 14 hours is the same as 2 hours, so you can say that if it is currently 5 o'clock and you party for 9 hours, it will be 2 o'clock.

5.3 Partitions

Let X be a set. A *partition* of X is a set $\mathcal{A} \subset \mathcal{P}(X)$ of subsets such that

1. $\cup_{A \in \mathcal{A}} A = X$
2. if $A, B \in \mathcal{A}$, then either $A = B$ or $A \cap B \neq \emptyset$.

Intuitively, this is just a way to break up X into a bunch of different pieces. As an example, here are some partitions of the set $\{1, 2, 3, 4\}$:

$$\mathcal{A} = \{\{1,2\},\{3\},\{4\}\},\ \mathcal{B} = \{\{1,2,3,4\}\},\ \mathcal{C} = \{\{1\},\{2\},\{3\},\{4\}\}.$$

Partitions of a set X are essentially the same as equivalence relations on X.

Exercise 5.19. If $\sim$ is an equivalence relation on X, show $X/\sim$ is a partition of X.

Exercise 5.20. Conversely, let $\mathcal{A}$ be a partition of X and for $a, b \in X$ define $a \sim b$ if there is some element $A \in \mathcal{A}$ such that $a, b \in A$. Show that $\sim$ is an equivalence relation, and that $X/\sim\, = \mathcal{A}$.

5.4 Bell numbers

The total number of partitions of an n-element set is called the n^{th} *Bell number*, written B_n, after the mathematician Eric Bell.

Exercise 5.21. Calculate B_1, B_2, B_3 by writing out all possible partitions, and then just say what B_4 is without writing them all out.

Exercise 5.22. By induction, show that $B_n \leq n!$.

Exercise 5.23. Show that $B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k$ for $n = 1, 2, \ldots$.

Computing the B_n by writing out all the partitions is a bit of a pain. You can also compute them using Exercise (5.23), but here's an even cooler way. Start by writing the number 1 in the upper left corner of a triangle. We now define the other rows of the triangle recursively. The first entry of a row is the last entry of the previous row. To calculate the i^{th} entry of a row, just add the $(i-1)^{th}$ entries of that row and the previous row. The Bell numbers will appear along the diagonal, and also in the first column as long as you discard the initial 1 in the top left corner.

$$\begin{array}{cccc}
1 & & & \\
1 & 2 & & \\
2 & 3 & 5 & \\
5 & 7 & 10 & 15
\end{array}$$

Exercise 5.24. Continue making the triangle to find B_5.

The following comes from a 2011(!) paper of Sun and Wu.

Exercise 5.25. Given $1 \leq k \leq n$, let $A_{n,k}$ be the the number of partitions of $\{1, \ldots, n+1\}$ that include the one-element (*singleton*) set $\{k+1\}$, and where there are no other singleton sets consisting of elements bigger than $k+1$.

1. Show that $A_{n,k} = A_{n,k-1} + A_{n-1,k-1}$. *Hint: take a partition P of $\{1, \ldots, n+1\}$ as in the definition of $A_{n,k}$ and break into cases depending on whether the singletons set $\{k\}$ is an element of P.*

2. Show that $A_{n+1,1} = A_{n,n} = B_n$. *Hint: to show $A_{n+1,1} = B_n$, start with a partition of $\{1, \ldots, n+2\}$ where $\{2\}$ is a singleton. Take the set containing* 1 *and break it into singletons, then discard* 1 *and* 2 *and subtract* 2 *from all other numbers.*

3. Prove that the triangle method of calculating Bell numbers B_n works.

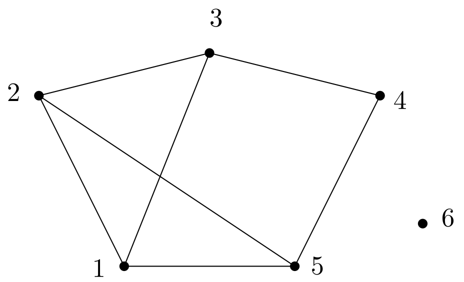
6 Graphs

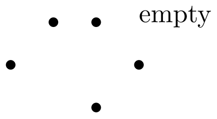
A *graph* is a pair $G = (V, E)$ where V is a set and E is a set of 2-element subsets of V. Elements of V are called *vertices* and subsets $\{x, y\} \in E$ are called *edges*, and we say $x \in V$ is *incident to* $e \in E$ if $v \in e$. Alternatively, x is *an endpoint* of e. To understand this terminology, visualize a graph as a set of points (the vertices) connected by line segments (the edges). For instance, we have

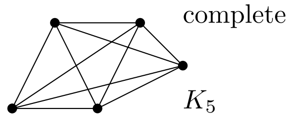
$$V = \{1, 2, 3, 4, 5, 6\}, \quad E = \{\{1, 2\}, \{2, 3\}, \{3, 4\}, \{4, 5\}, \{2, 5\}\}$$

Note that each set of two vertices that is an element of E is connected by an edge. The vertex 6 is not incident to any edges, since you don't see a 6 in E.

Remark 6.1. Sometimes we'll denote a graph just by G and write $V(G)$ and $E(G)$ when we want to refer to vertex set and edge set of G.







There are two very simple graph on every set V: the *empty graph*, where $E = \emptyset$, and the *complete graph*, where $E = \{\{x, y\} \mid x, y \in V, x \neq y\}$. Here are pictures of the empty and complete graphs on a vertex set with 5 elements. The complete graph on n vertices is denoted by K_n.

Exercise 6.2. How many different graphs are there with vertex set $V = \{1, \ldots, n\}$?

The *degree* of a vertex $v \in V$, written $\deg(v)$, is the number of edges incident to v. We write $|V|$ and $|E|$ for the numbers of vertices and edges in G, respectively.

Exercise 6.3.

1. If $G = (V, E)$ is a graph, show that $\sum_{v \in V} \deg(v) = 2|E|$.
2. Show that every graph has an even number of vertices of odd degree.
3. There is a party at Marcello's with 5 people attending, including Marcello. Is it possible that everyone knows exactly 3 other people?

6.1 Isomorphism of graphs

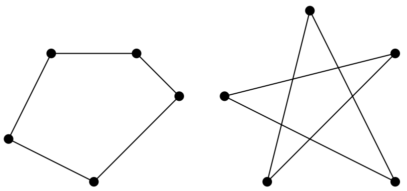
Let G, H be graphs. A bijection $f : V(G) \longrightarrow V(H)$ is an *isomorphism* if

$$\{v, w\} \in E(G) \iff \{f(v), f(w)\} \in E(H), \quad \forall v, w \in V(G).$$

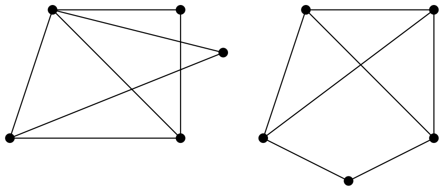
Usually, we will write graph isomorphisms as $f : G \longrightarrow H$. If there is such an isomorphism, we say that G and H are *isomorphic*, written $G \cong H$.

Exercise 6.4. In each part below, are the two graphs pictured isomorphic? If so, exhibit an isomorphism by labeling the vertices of the two graphs with numbers (here, 1,2,3,4,5) in a way that defines a graph isomorphism. If not, you have to prove that there is *no* isomorphism!

(a)



(b)



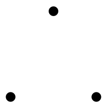
Exercise 6.5. Let $\mathcal{G}$ be the set[3] of all graphs. Show that $\cong$ defines an equivalence relation on $\mathcal{G}$.

We call a $\cong$-equivalence class an *isomorphism class* of graphs. As an example, while there are lots of different graphs with two vertices, e.g.

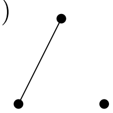
a) $V = \{1, 2\},\ E = \{\{1, 2\}\}$ *b)* $V = \{\heartsuit, \clubsuit\},\ E = \{\{\heartsuit, \clubsuit\}\}$
c) $V = \{8, \Box\},\ E = \emptyset$ *d)* $V = \{404.5, \hookrightarrow\},\ E = \emptyset$,

etc..., there are only two isomorphism classes, depending on whether the two vertices are connected by an edge or not. Here, examples a) and b) are isomorphic (why?), as are examples c) and d), but the first two lie in a different isomorphism class than the last two. Similarly, there are four isomorphism classes of graphs on three vertices, represented by the following:

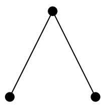
(a)



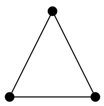
(b)



(c)



(d)



Here, 'represented' means that each of the four isomorphism classes contains exactly one of the graphs pictured above.

Exercise 6.6. Show that none of the graphs above are isomorphic, and that every graph on 3 vertices is isomorphic to one of those above.

Exercise 6.7. How many isomorphism classes of graphs with 4 vertices do you think there are? Draw an element from each class, with no repeats. No proofs required, although think through it if you want.

[3] The careful and informed reader may protest that this is not a set (see Russell's paradox), and that would be a great point. One can fix this by considering only graphs whose vertex sets are subsets of some fixed set like $\mathbb{R}$, if desired, but let's ignore this here.

6.2 Connected graphs

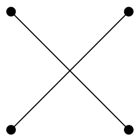
A *walk* from v to w of *length* n in a graph $G = (V, E)$ is a sequence of vertices

$$v = v_0, v_1, \ldots, v_n = w$$

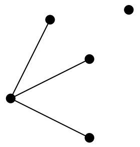
such that $\{v_i, v_{i+1}\} \in E$ for $i = 0, \ldots, n-1$. Here, the length of the walk is intuitively the number of edges it traverses. We say G is *connected* if for every pair of vertices $v, w \in V$, there is a walk from v to w.

Exercise 6.8. Which of the following graphs are connected?

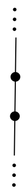
(a)



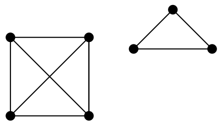
(b)



(c)



(d)



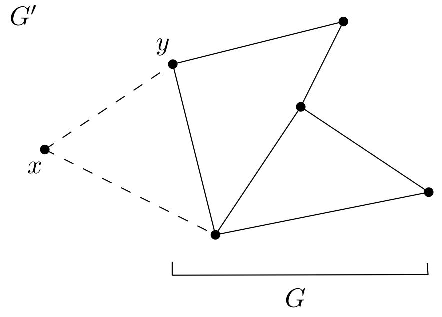
For clarity, the picture in (c) is supposed to indicate that there are infinitely many vertices arranged like the integer points on a vertical real line.

Exercise 6.9. Show by counterexample that the following theorem is false. Then explain why the proof is false.

'Theorem'. *If every vertex in a finite graph G is incident to an edge, then the graph G is connected. (Here, 'finite' just means $|V| < \infty$.)*

'Proof'. We use by induction on $n = |V(G)|$. The theorem doesn't have any content when $n = 1$, since the only graph on 1 vertex has no edges. So for the base case, we can start with a graph G with two vertices v, w. Since v is incident to an edge e, this edge must also be incident to w, and hence G is connected. For the inductive step, let G be a graph on n vertices with such that all vertices of G are incident to an edge. So G is connected, by the induction hypothesis. Construct a new graph G' with by adding a new vertex x to G. Since we are only dealing with graphs where all vertices are incident to an edge, we can assume that the vertex x is adjacent to some vertex y of G.

But then G' is obviously connected, since any two vertices of G can be connected via a walk in G, and x can be connected to any vertex z in G by first walking to y and then walking within G to z. $\square$



6.3 Connected components

Let G be a graph. For $v, w \in V(G)$, let $v \sim w$ if there is a walk from v to w.

Exercise 6.10. Show that $\sim$ is an equivalence relation.

The equivalence classes of $\sim$ are called the *connected components* of G. Draw some examples to illustrate why they're called this. Note that G is connected if and only if all vertices are related, i.e. there's a single connected component containing all vertices of G.

Exercise 6.11. If a graph G has n vertices and m edges, where $0 \leq m \leq n-1$, show that G has at least $n-m$ connected components. In particular, a connected graph on n vertices has at least $n-1$ edges. *Hint: fix n and use induction on m.*

Let $G = (V, E)$ be a graph. A walk $v = v_0, v_1, \ldots, v_n = w$ on G is a *path* if $v_i \neq v_j$ when $i \neq j$.

Exercise 6.12. Suppose that $v = v_0, \ldots, v_n = w$ is a walk from v to w that has *minimal length*, i.e. its length is less than or equal to the length of any other walk from v to w. Show that $v_0, \ldots, v_n$ is a path.

Note that the well ordering principle implies that whenever there's a walk from v to w, there's a walk with minimal length, and hence a path from v to w.

We say a walk $v_0, \ldots, v_n$, where $n \geq 3$, is a *cycle* if the following hold:

1. $v_0 = v_n$,

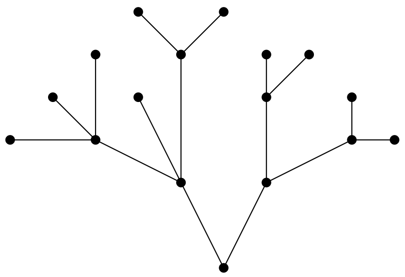
2. it does not repeat vertices, except that the first/last vertices are the same: we have $v_i \neq v_j$ except when $i = j$ or $\{i, j\} = \{0, n\}$.

Informally, a cycle is just a loop in a graph that doesn't repeat vertices. We require that $n \geq 3$ in order to rule out things like a single vertex v_0, or a sequence v_0, v_1, v_0, neither of which should be called a cycle.

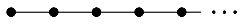
A graph G is a *tree* if it is connected and has no cycles.

Exercise 6.13. Which of the following are trees?

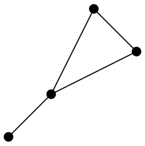
(a)



(b)



(c)



Exercise 6.14. Show that G is a tree if and only if for every two vertices v, w in G, there is a unique path in G from v to w. *Hint: the hardest part here is to prove that if G is a tree, there is a *unique* path between any two vertices v, w. To do this, you need to take two distinct paths from v to w and try to produce from them a cycle. The problem is, the two paths may partially agree, so you can't always form a cycle by doing one path and then the other backwards. To deal with this, do a proof by contradiction, taking a pair of distinct paths in G that have the same endpoints, and* where the sum of the lengths of the two paths is minimal. *Show that the walk obtained by following one of these, then the other backwards, is in this case a cycle.*

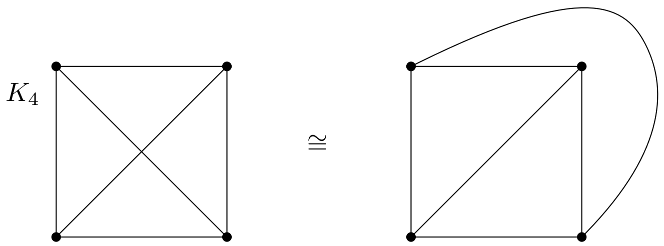
A vertex of a tree T is called a *leaf* if it has degree one. (Why?)

Exercise 6.15. Show that every finite tree T with at least two vertices has at least two leaves. *Hint: as T is finite, there is a path of maximal length.*

Exercise 6.16. Show that a connected graph on n vertices is a tree if and only if it has exactly $n - 1$ edges. *Hint: to prove that trees have $n - 1$ edges, use induction and the previous exercise.*

6.4 Planar graphs

A *planar embedding* of a graph G is a way to draw it in the plane in such a way that no edges cross. A graph is *planar* if it admits a planar embedding. Note that the complete graph K_4 doesn't look like it's planar when you draw its edges as straight lines, but it does admit a planar embedding, draw on the right in the figure below. This indicates that it can be hard to actually prove that a graph is non-planar, since you have to say somehow that there's NO possible way to find a planar embedding, no matter what you draw.



Given a graph G with a planar embedding, the edges of G divide the plane into a number of different regions, called *faces*. Above, the planar embedding of K_4 has 4 faces. For a given planar embedding of a graph, we let F be the set of all faces.

Exercise 6.17 (Euler's Formula)**.** If $G = (V, E)$ is a connected planar graph with a given planar embedding, then $|V| - |E| + |F| = 2$. *Hint: do induction on* $|E|$*, the number of edges of* G*.*

In particular, this implies that $|F| = 2 - |V| + |E|$ and hence the number of faces only depends on the graph G, and not on the planar embedding chosen.

Exercise 6.18. If G is a planar graph with n vertices, then G has at most $3n - 6$ edges. *Hint: Try adding edges to* G *to make a new graph* G' *with a planar embedding, where* G' *is connected and all faces of* G' *are bounded by* 3 *edges.*

Exercise 6.19. Give an example of a non-planar graph.

7 Cardinality

Definition 7.1. Given two sets A, B we say that A, B have the *same size*, or alternatively *same cardinality*, written $A \approx B$, if there is a bijection $f : A \longrightarrow B$.

This $\approx$ satisfies the following three properties.

1. For any set A, we have $A \approx A$, via the identity bijection $i : A \longrightarrow A$, $i(a) = a$.

2. If $A \approx B$ then $B \approx A$, since any bijection $f : A \longrightarrow B$ has an inverse $f^{-1} : B \longrightarrow A$, which is also a bijection.

3. If $A \approx B$ and $B \approx C$, then $A \approx C$. Indeed, bijections $A \longrightarrow B$ and $B \longrightarrow C$ compose to give a bijection $A \longrightarrow C$.

So if the 'set of all sets' were a set, which it is not, $\approx$ would define an equivalence relation on it. When A, B are finite, we have $A \approx B$ exactly when A, B have the same number of elements, since then those elements can be matched up to give the desired bijection.

You may be used to thinking that all infinite sets have cardinality ∞, so should all be equivalent under $\approx$, but we'll see in this worksheet that there are many different 'sizes' of infinity.

Exercise 7.2. Show that $\mathbb{N} \approx \mathbb{N} \cup \{0\}$.

Exercise 7.3. Is $\mathbb{Z} \approx \mathbb{N}$?

7.1 Countability

Definition 7.4. If $A \approx \mathbb{N}$, we say that A is *countably infinite*. We say A is *countable* if it is finite or countably infinite.

For example, $\mathbb{N} \cup \{0\}$ is countably infinite, and $\{1, 8, \heartsuit\}$ is countable. Note that a set A is countably infinite exactly when its elements can be arranged into an infinite list, i.e. when A can be written in the form

$$A = \{a_1, a_2, \ldots \ldots\}.$$

Indeed, if A is countable, then there's a bijection $f : \mathbb{N} \longrightarrow A$, and if we set $a_i := f(i)$, then $A = \{a_1, a_2, \ldots \ldots\}$ as above. Conversely, if $A = \{a_1, a_2, \ldots \ldots\}$, then we can define a bijection $f : \mathbb{N} \longrightarrow A$ by setting $f(i) = a_i$.

Here's a first example of an uncountable set.

Theorem 7.5. *There's no surjection $f : \mathbb{N} \longrightarrow (0, 1)$. In particular, there's no bijection, so $(0, 1)$ is uncountable.*

The proof is Cantor's famous diagonal argument.

Proof. Let $f : \mathbb{N} \longrightarrow (0,1)$ be a function. We'll show there's some $x \in (0,1)$ such that $x \neq f(i)$ for all $i \in \mathbb{N}$. This will show f isn't surjective.

Let's write out decimal expansions of all the numbers $f(i) \in (0,1)$ as follows.

$$\begin{aligned} f(1) &= .a_{11}\, a_{12}\, a_{13}\, a_{14} \ldots \\ f(2) &= .a_{21}\, a_{22}\, a_{23}\, a_{24} \ldots \\ f(3) &= .a_{31}\, a_{32}\, a_{33}\, a_{34} \ldots \\ f(4) &= .a_{41}\, a_{42}\, a_{43}\, a_{44} \ldots \\ &\vdots \end{aligned}$$

We want to construct some $x \in (0,1)$ that's not equal to any of these. So, set

$$x = .x_1\, x_2\, x_3 \ldots, \quad x_i = \begin{cases} 3 & a_{ii} = 4 \\ 4 & a_{ii} \neq 4. \end{cases}$$

For example, suppose we have

$$\begin{aligned} f(1) &= .3869\ldots \\ f(2) &= .0482\ldots \\ f(3) &= .4490\ldots \\ f(4) &= .2224\ldots \\ &\vdots \end{aligned}$$

Then $x = .4343\ldots$. By construction $x_i \neq a_{ii}$, so x and $f(i)$ differ in the i^{th} decimal place, and hence aren't equal. (Note that since x doesn't have 0's and 9's in its decimal expansion, it has a *unique* decimal example, so to check it's not equal to any of the $f(i)$, it suffices to check that the decimal expansions above are different. Contrast this with the two decimal expansions for $.10000\ldots = .099999\ldots$.) □

Exercise 7.6. Draw the graph of a bijection $f : (0,1) \longrightarrow \mathbb{R}$, and conclude that $\mathbb{R}$ is also uncountable.

Exercise 7.7. (a) If $B \subset \mathbb{N}$, show that B is countable. *Hint: suppose that B is infinite. Given $b \in B$, let $g(b)$ be the number of elements of B that are less than or equal to b. Show that $g : B \longrightarrow \mathbb{N}$ is a bijection.*

(b) Using part (a), show very quickly that if A is countable and $f : B \longrightarrow A$ is injective, then B is countable. In particular, a subset of a countable set is countable.

Exercise 7.8. (a) If $f : \mathbb{N} \longrightarrow B$ is surjective, show that B is countable. *Hint: if $b \in B$, let $g(b) = \min\{x \in A \mid f(x) = b\}$.*

(b) Using part (a), show that if A is countable and $f : A \longrightarrow B$ is surjective, then B is countable.

Exercise 7.9. Show that if A, B are both countably infinite, so is $A \cup B$.

Exercise 7.10. Show that if A, B are both countably infinite, so is $A \times B$. *Hint: think about snakes! Make an $\mathbb{N} \times \mathbb{N}$ grid, and starting at $(1, 1)$, try to wind through it. Alternatively, let p_i be the i^{th} prime and consider p_i^j.*

Exercise 7.11. Using the previous exercise and our definition of $\mathbb{Q}$ as a quotient set, show that $\mathbb{Q}$ is countably infinite.

Exercise 7.12. Show that the set $\mathbb{R} \setminus \mathbb{Q}$ of all irrational numbers is uncountable.

7.2 Ordering sizes of infinity

If there is an injection $f : A \longrightarrow B$, we write $A \preceq B$. If $A \preceq B$ but $A \not\approx B$, i.e. there's an injection $A \longrightarrow B$ but there is no such bijection, we write $A \prec B$. For example, $\mathbb{N} \prec \mathbb{R}$ because the inclusion $i : \mathbb{N} \longrightarrow \mathbb{R}$, $i(n) = n$ is an injection, but we proved in Exercise 7.6 that there's no bijection $\mathbb{N} \longrightarrow \mathbb{R}$.

Note that to prove that $A \prec B$, it does *not* suffice to produce an injection that is not a bijection. For example, $f : \mathbb{N} \longrightarrow \mathbb{N}$, $f(x) = x + 1$ is an injection that is not a bijection, but $\mathbb{N} \approx \mathbb{N}$. The point is to construct an injection, and then show separately there is no possible (unrelated) bijection.

Exercise 7.13. If A is a set, show that $A \prec \mathcal{P}(A)$.

Exercise 7.14. (The Schroeder–Bernstein theorem) Prove that if $A \preceq B$ and $B \preceq A$, then $A \approx B$. *Hint: we can take A, B to be disjoint, and take injections*

$$f : A \longrightarrow B, \ g : B \longrightarrow A.$$

Form a graph $G = (V, E)$ with $V = A \cup B$ and draw red edges from each a to $f(a)$, and blue edges from each b to $g(b)$. What do the connected components of this graph look like? Try to define a bijection between A and B piecewise, individually on each connected component.

Exercise 7.15. Show that $\mathcal{P}(\mathbb{N}) \approx \mathbb{R}$. *Hint: for convenience, produce injections in both directions. You will probably find using binary or decimal expansions useful.*

Exercise 7.16. If $A \preceq B$ and $B \prec C$, show that $A \prec C$. *Hint: Amazingly, this isn't obvious. Use the Schroeder-Bernstein theorem.*

Exercise 7.17. Let $\mathcal{A}$ be a set whose elements are sets. Show that there is some set B such that $A \prec B$ for all $A \in \mathcal{A}$.

This exercise suggests an unimaginable number of different infinite cardinalities. Namely, given a set A, let $\mathcal{P}^n(A)$ be the n^{th} *iterated power set* of a set A, defined by

$$\mathcal{P}^n(A) := \mathcal{P}(\cdots \mathcal{P}(\mathcal{P}(A)) \cdots).$$

Starting with $\mathbb{N}$, we can construct a sequence of sets as follows:

$$\mathbb{N} \prec \mathcal{P}(\mathbb{N}) \prec \mathcal{P}^2(\mathbb{N}) \prec \ \cdots \prec B \prec \mathcal{P}(B) \prec \mathcal{P}^2(B) \prec \cdots \prec C \prec \mathcal{P}(C) \prec \cdots ,$$

where here, B is some set that is bigger in size than all $\mathcal{P}^n(\mathbb{N})$, and then C is defined similarly with B instead of $\mathbb{N}$. Of course, this goes on forever, even after we run out of letters in the alphabet, and the exercise above shows that even after you repeat this procedure forever, there's STILL a bigger set than everything so far constructed. Then you can repeat the process with that bigger set, and continue...