MAT102 Lecture Notes

Tyler Holden, ©2016-

Contents

1 Motivating Problems

The kinds of questions we will be considering in this course are not those amenable to rote memorization or procedural algorithms, like those of which secondary school is replete. We will instead be looking at questions that require you to think critically, to use knowledge you have already acquired, and you apply it to solve a problem you have never seen before.

Critical thinking is hard! Do not be discouraged if you cannot do it at first. Like playing a musical instrument or learning a sport, it is something that can be learned with practice and dedication.

To this effect, let's look at some famous mathematical problems.

Example 1.1

Suppose that a standard 8×8 chessboard has two diagonally opposite corners removed. Is it possible to tile the chessboard with dominoes? More precisely, given 31 dominoes of size 2×1, is it possible to cover the chessboard in dominoes such that no two overlap?

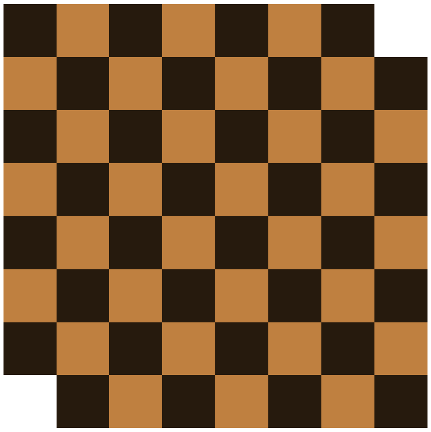


Figure 1: A chessboard with two diagonal pieces removed. Notice that by necessity, those two pieces are of the same color.

Another topic of great appeal to the layman is the notion of infinity. Did you know that there are many different kinds of infinity? In fact, there are infinitely many different kinds of infinity, with no infinity being the largest infinity. However, the infinity which enumerates the infinities is larger than any infinity which it enumerates. That's confusing eh?

Let's start with a more reasonable example:

Example 1.2

There are as many whole numbers (like $1, 2, 3, 4, \ldots$) as rational numbers (like $1/2, 17/4, -22/883$), but there are strictly more real numbers than these two.

Or how about this famous anecdote:

Example 1.3

One day Gauss' teacher asked his class to add together all the numbers from 1 to 100, assuming that this task would occupy them for quite a while. He was shocked when young Gauss, after a few seconds thought, wrote down the answer 5050.
More generally, what is the sum

$$1 + 2 + 3 + 4 + \cdots + (n-1) + n$$

for any natural number n? What if we change it to

$$1^2 + 2^2 + 3^2 + 4^2 + \cdots + (n-1)^2 + n^2?$$

We will be able to answer all of these questions and more by the end of this course.

2 Mathematical Infrastructure

In order to discuss proofs, we will need raw materials, things like numbers, functions, and sets. You should already be familiar with some of the basics, but here we will introduce these items in a little more depth.

2.1 Quadratic Formula

The quadratic formula represents an interesting starting point. Consider the equation

$$ax^2 + bx + c = 0$$

for constants a, b, c. The student is familiar with the famous *quadratic formula*, which tells us that the solutions to this equation are given by

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

But as far as most of you are concerned, this is some mysterious quantity that your high school teachers materialized out of thin air. So where does it come from?

The answer is really quite simple, although there is some tricky algebra to be done. We are taught when we are younger how to "complete the square," which is to convert

$$ax^2 + bx + c \quad \text{into something of the form } \alpha(x-\beta)^2 + \gamma.$$

This is useful for graphing the quadratic, or maybe determining the apex of the corresponding parabola. It is also very useful for finding the roots, since

$$\begin{aligned}\alpha(x-\beta)^2+\gamma=0 \quad &\Leftrightarrow \quad \alpha(x-\beta)^2=-\gamma \\ &\Leftrightarrow \quad (x-\beta)^2=-\frac{\gamma}{\alpha} \\ &\Leftrightarrow \quad (x-\beta)=\pm\sqrt{-\frac{\gamma}{\alpha}} \\ &\Leftrightarrow \quad x=\beta\pm\sqrt{-\frac{\gamma}{\alpha}}. \qquad (2.1)\end{aligned}$$

Well now, that looks pretty darn similar to the quadratic formula, except that we need to write α, β, γ in terms of a, b, c. So let's complete the square on ax^2+bx+c, where we find that

$$\begin{aligned} ax^2+bx+c &= a\left(x^2+\frac{b}{a}x\right)+c && \text{factor out the } a \\ &= a\left(x^2+\frac{b}{a}x+\frac{b^2}{4a^2}-\frac{b^2}{4a^2}\right)+c && \text{squaring half the coefficient of } x \\ &= a\left(x^2+\frac{b}{a}x+\frac{b^2}{4a^2}\right)-\frac{b^2}{4a}+c && \text{pulling the } b^2/(4a^2) \text{ term out} \\ &= \underbrace{a}_{\alpha}\left(x+\underbrace{\frac{b}{2a}}_{\beta}\right)^2+\underbrace{\frac{4ac-b^2}{4a}}_{\gamma}. \end{aligned}$$

Substituting these values of α, β, γ into (2.1) gives us the quadratic formula.

The *discriminant* of the quadratic is the term $D := b^2-4ac$ located under the square root sign in the quadratic formula. The sign of the this term can tell us precisely how many roots a quadratic formula has. For example, if $D>0$ then there are precisely two distinct roots, if $D=0$ then there is a single repeated root, and if $D<0$ then there are no roots.

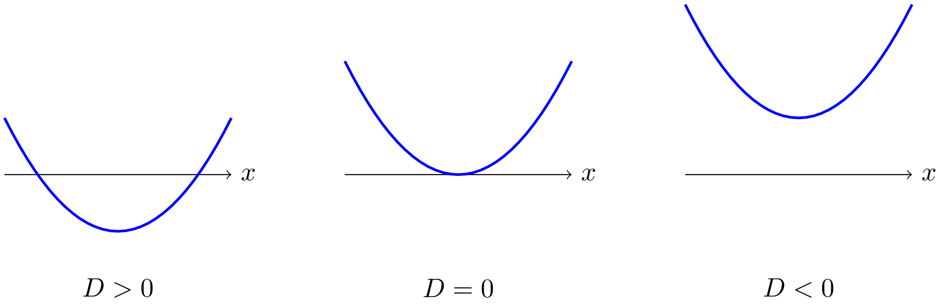


Figure 2: The various graphs of the parabola ax^2+bx+c depending on the value of the discriminant D. There are $1+\operatorname{sgn}(D)$ roots of the parabola.

2.2 Bounding Arguments

To discuss the notion of length, we need to be able to compare relative sizes. This leads us to the notion of inequalities. For example, we know that $2<4$ or that $-5\le 0$, or even that $e<\pi$. This is known as the total ordering of the real numbers, which we will discuss in more detail later.[1]

2.2.1 Inequalities

This becomes significantly more complicated when we are determining more general rules; that is, rules that hold when we are unable to use specific numbers. You may take the following as axioms (though in reality they need to be proven):

Proposition 2.1

If a, b, c are real numbers then the following hold:

1. If $a < b$ and $c > 0$ then $ca < cb$,
2. $a^2 \geq 0$
3. If $a \geq 0$ there is a unique non-negative number d such that $d^2 = a$. We often write $d = \sqrt{a}$ to explicitly denote the relationship between d and a.
4. If $a < b$ and $b < c$ then $a < c$.

Proposition 2.1 (3) in particular is difficult to prove, and requires something called the *Completeness Axiom.*

Exercise: How does Proposition 2.1 change if the less-than-or-equal signs are changed to less-than signs?

We can use these basic tools to build more sophisticated results.

Proposition 2.2

For any real numbers a, b we have $a^2 + b^2 \geq 2ab$.

Proof. Note that $(a - b)^2 \geq 0$ by property (2). Expanding the square gives

$$\begin{aligned}(a-b)^2 \geq 0 \quad &\Leftrightarrow \quad a^2 - 2ab + b^2 \geq 0 \\ &\Leftrightarrow \quad a^2 + b^2 \geq 2ab,\end{aligned}$$

which is what we wanted to show. □

Example 2.3

Suppose that $a, b, c \geq 0$ and $b + c \geq 2$. Show that $(a + b + c)^2 \geq 4a + 4bc$.

[1] The proper definition of the inequality is as follows: We say that $a > b$ if $a - b$ is a positive number. Using this, try to prove the facts about inequalities. For example, Proposition 2.1 (1) and (4)

Solution. Starting with the left hand side, we expand to get

$$(a+b+c)^2 = a^2+b^2+c^2+2ab+2bc+2ac.$$

We need to find some way of using the fact that $b+c \geq 2$. Notice that by clever factoring, we can write

$$2ab+2ac+2bc = 2a(b+c)+2bc \geq 4a+2bc$$

so that our inequality becomes

$$(a+b+c)^2 \geq a^2+b^2+c^2+4a+2bc.$$

We must somehow convert the $a^2+b^2+c^2+2bc$ into something that looks like $4bc$. By Proposition 2.2, we know that $b^2+c^2 \geq 2bc$ so

$$a^2+(b^2+c^2)+2bc \geq a^2+4bc \geq 4bc$$

where in the last inequality we have used the fact that $a^2 \geq 0$. Putting this all together,

$$(a+b+c)^2 \geq 4a+4bc$$

exactly as required. ■

Proposition 2.4

If a, b are real numbers such that $0 < a < b$, then $a^2 < ab < b^2$ and $0 < \sqrt{a} < \sqrt{b}$.

Proof. Let's start by showing that $a^2 < ab < b^2$. We know that $0 < a < b$ and since $a > 0$ we can multiply through by a, preserving the inequality, to get

$$0 < a^2 < ab.$$

Similarly, since $b > 0$ we can multiply into $0 < a < b$ and preserve the inequality, to get

$$0 < ab < b^2.$$

Combining both inequalities together gives $a^2 < ab < b^2$ as required.

To show that $0 < \sqrt{a} < \sqrt{b}$, note that that assumption $a < b$ can be written as $b - a > 0$. Thinking of this as a difference of squares allows us to write

$$b - a = (\sqrt{b}-\sqrt{a})(\sqrt{b}+\sqrt{a}) > 0$$

As both $\sqrt{a}, \sqrt{b} > 0$, so too is there sum, showing that $\sqrt{a}+\sqrt{b} > 0$. Thus $\sqrt{b}-\sqrt{a} > 0$ as well, or equivalently $\sqrt{a} < \sqrt{b}$. □

2.2.2 The Arithmetic-Geometric Mean Inequality

One of the more famous inequalities in mathematics is the *Arithmetic-Geometric Mean Inequality*. In order to discuss it, we must remind ourselves of the arithmetic mean and the geometric mean.

Definition 2.5

If a, b are two real numbers, then the

$$\text{Arithmetic Mean is} \quad \frac{a+b}{2}, \qquad \text{Geometric Mean is} \quad \sqrt{ab}.$$

The arithmetic mean is usually what is meant when we talk about an average. However, there are cases in which the geometric mean can also be interpreted as an average. For example, say that you have an investment of \$100 which grows at a rate of 5% the first year and 8% in the second year. After two years the value of your investment is

$$\$100 \times (1.05) \times (1.08) = \$100 \times (1.134) = \$113.40$$

It is often more convenient to discuss such a investment in terms of its effective annual rate, which is the hypothetical *fixed* rate at which your bond would have accrued the same final value. If that value is r, then we need to solve

$$r \times r = 1.1134, \qquad \Rightarrow \qquad r = \sqrt{1.05 \times 1.08} \approx 1.065.$$

The number 1.065 is precisely the geometric mean.

Given a collection of n numbers $a_1, \ldots, a_n$, we know their arithmetic mean is given by

$$\frac{a_1 + a_2 + \cdots + a_n}{n},$$

the geometric mean of that same group of number is given by

$$\sqrt[n]{a_1 a_2 \cdots a_n}.$$

Theorem 2.6: Arithmetic-Geometric Mean Inequality (AM-GM)

For any real numbers a, b we have

$$ab \leq \left(\frac{a+b}{2} \right)^2$$

with equality if and only if $a = b$. If in addition $ab > 0$ then

$$\sqrt{ab} \leq \frac{a+b}{2}.$$

Note that this theorem generalizes to

$$\sqrt[n]{a_1 \cdots a_n} \leq \frac{a_1 + \cdots + a_n}{2}$$

but we will focus on the proof when $n = 2$.

Proof. To present the proof directly would likely lead to confusion, since at some point it will appear as though we arbitrarily add a term. Instead, let's work backwards to see if we can reduce our inequality to a similar statement. If our inequality holds then

$$\begin{aligned} ab \leq \left(\frac{a+b}{2}\right)^2 \quad &\Leftrightarrow \quad 4ab \leq a^2 + b^2 + 2ab \\ &\Leftrightarrow \quad 2ab \leq a^2 + b^2 \end{aligned}$$

and we know that this last identity is correct by Proposition 2.2. A proper proof would now consist of tracing back through this system of equivalences to arrive at the desired result. □

Warning!

What I did in the proof above was create a chain of logically equivalent statements, eventually arriving at a result which I knew to be true, thus implying that every statement in the chain is true. I *did not* assume that the first inequality was true!

Students are often tempted to prove inequalities in a similar fashion, but fail to ensure that every statement is logically *equivalent*, or *beg the question* by assuming that the end result is true. For example, if you complete a proof by concluding $0 = 0$, then your proof is almost certainly wrong.

Here's an interesting alternate proof. Fix two positive real numbers a, b and construct a semicircle whose radius is $a + b$, as shown in Figure 3. Let h be the perpendicular line emanating from the meeting point of line segments of length a and b along the radius.

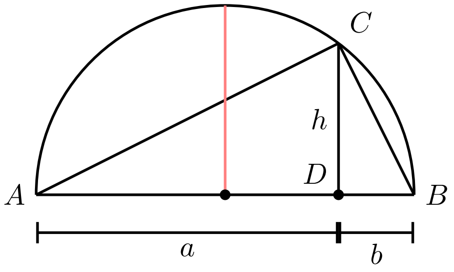


Figure 3: An alternate proof of the AM-GM.

As an inscribed angle, $\angle ACB$ is a right angle. This in turn implies that triangle $\triangle ADC$ is similar to triangle $\triangle CDB$. As these are similar, the ratios of their side-lengths are equal; namely,

$$\frac{a}{h} = \frac{h}{b} \quad \Rightarrow \quad h^2 = ab \quad \Rightarrow \quad h = \sqrt{ab}.$$

Thus the height h is precisely the geometric mean. Compare this to the red line, whose length is the radius $(a+b)/2$. Note that by construction, h will always be shorter than the radius, and they will be equal precisely when $a = b$.

Example 2.7

A farmer is given 120 metres of fencing and wishes to make a rectangular pasture which encloses the maximum amount of area. Show that the largest such pasture is obtained with a square.

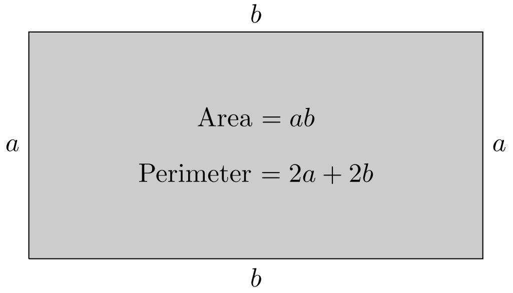


Figure 4: The farmer is making a rectangular pasture, but has a fixed amount of fencing.

Solution. Consider a rectangle with side length a, b as shown in Figure 4. The perimeter of this rectangle is the fence, of which the farmer has 120 metres, so $120 = 2a + 2b$. The area is ab, which seems to work well with the AM-GM, so were we to plug this in directly we would get

$$ab \leq \left(\frac{a+b}{2}\right)^2.$$

But we know $120 = 2a + 2b$, so dividing everything by 4 gives $(a + b)/2 = 30$, and so

$$ab \leq \left(\frac{a+b}{2}\right)^2 = 30^2 = 900.$$

At this point, we only know that 900 is an upper bound for the area: It could be the case that the true upper bound is some smaller number. One of the powerful aspects of the AM-GM is that it gives a condition on the inequality to be saturated; namely, when $a = b$. Setting $a = b$ gives us a square, and if we want to solve for the precise values of a and b, we have $120 = 2a + 2b = 4a$ showing that $a = b = 30$. ■

Example 2.8

Find the minimum of the function $f(x) = x^3 + \dfrac{4}{x^3}$.

Solution. If you know calculus, this problem can be done using optimization techniques. However, it requires a great deal of time and energy to develop that infrastructure, whereas this problem can be solved with the AM-GM. How would we realize this? To find the minimum, we need a bound of the form $f(x) \geq m$, where m is some constant. Note that if we multiply the two components of

f, we would indeed get a constant. To see if this goes anywhere, let $a = x^3$ and $b = 4/x^3$, so that $ab = 4$, and

$$\left(\frac{a+b}{2}\right)^2 = \left(\frac{x^3 + 4/x^3}{2}\right)^2 = \frac{(x^3+4/x^3)^2}{4}.$$

The AM-GM then says that

$$4 \leq \frac{(x^3+4/x^3)^2}{4} \quad \Rightarrow \quad 16 \leq (x^3+4/x^3)^2 \quad \Rightarrow \quad 4 \leq x^3 + \frac{4}{x^3}.$$

So $f(x) \geq 4$. As with all inequalities though, this might not be a good lower bound, maybe we can do better. We need to check that this value of the lower bound is actually achieved. By the AM-GM, we know that equality occurs when $a = b$, which in this case gives us

$$x^3 = \frac{4}{x^3} \quad \Rightarrow \quad (x^3)^2 = 4$$

so $x = \sqrt[6]{4} = \sqrt[3]{2}$, or more conveniently $x^3 = 2$. From here it's easy to see that when $x = \sqrt[3]{2}$, $f(\sqrt[3]{2}) = 4$ as required. ■

2.2.3 Absolute Values

Absolute values are used to measure distances.

Definition 2.9

If x is a real number, then the *absolute value of* x is

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

Note that $|x| \geq 0$, for if x is positive the absolute value does nothing, while if x is negative, the absolute value adds on yet another negative sign, making it positive.

One can think of the absolute value as measure the distance of a number from zero. For example, the numbers 4 and -4 should both be a distance of 4 from 0. We can also use absolute values to measure the distance between two numbers. If x, y are real numbers, the distance from x to y is $|x - y|$.

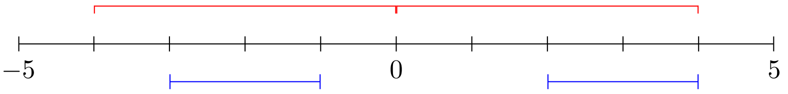


Figure 5: The real line from -5 to positive 5. We would like to define a system of measurement such that the red bars have the same length and the blue bars have the same length.

We can use absolute values to describe intervals of real numbers. For example, the collection of x which satisfy $|x| < 2$ are those such that $-2 \leq x \leq 2$, or the interval $(-2, 2)$. In a similar vein, the collection of x such that $|x - 1| < 3$ are those that are "within a distance of 3 from the number 1. You can probably guess that this amounts to the interval $(-2, 4)$, but to see it more precisely note that

$$|x - 1| < 3 \quad \Leftrightarrow \quad -3 < x - 1 < 3 \quad \Leftrightarrow \quad -2 < x < 4.$$

Proposition 2.10

If x, y are real numbers, then

1. $x \leq |x|$,
2. $|xy| = |x||y|$,
3. $\sqrt{x^2} = |x|$,
4. $|x+y| \leq |x| + |y|$ (Triangle Inequality).

Proof. We will prove (4) and leave the others as an exercise. Since $x^2 = |x|^2$, $y^2 = |y|^2$, and $2xy \leq 2|x||y|$ we have

$$x^2 + 2xy + y^2 \leq |x|^2 + 2|x||y| + |y|^2 \qquad \Leftrightarrow \qquad (x+y)^2 \leq (|x| + |y|)^2 .$$

Taking the square root of both sides gives $|x+y| \leq |x| + |y|$ as required. □

Exercise: When is the triangle inequality actually an equality?

Example 2.11

If $|x-1| < 1$, find an M such that $|x^2 + x - 2| < M$.

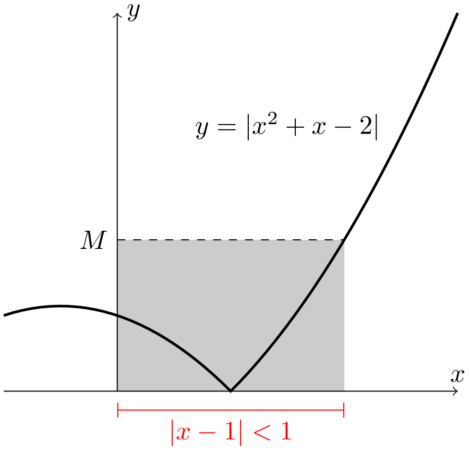


Figure 6: Determining some number larger than $|x^2 + x - 2|$ when $|x-1| < 1$.

Solution. Graphically, this question may be interpreted as in Figure 6. Note that we can write

$$|x^2 + x - 2| = |x+2||x-1| < |x+2| \qquad \text{since } |x-1| < 1.$$

When $|x-1| < 1$ we have $0 < x < 2$, so to make this look like something involving $x+2$ we add 2 to everything, giving $2 < x + 2 < 4$, which implies that $|x+2| < 4$. Hence $|x^2 + x - 2| < 4$ when $|x-1| < 1$. ■

Example 2.12

Find an $M > 0$ such that
$$\left| \frac{x^3 - x - 3}{x^4 + 1} \right| \leq M$$
whenever $|x| < 2$.

Solution. Looking at the numerator, we can use the triangle inequality to write
$$|x^3 - x - 3| \leq |x|^3 + |x| + |3| < 2^3 + 2 + 3 = 13.$$
For the denominator, we have to be more careful. Recall that if when we take reciprocals, an inequality changes direction, so we want to bound $|x^4 + 1|$ from below. Indeed,
$$|x^4 + 1| = x^4 + 1 \geq x^4 > 2^4 = 16.$$
Combining everything together gives
$$\left| \frac{x^3 - x - 3}{x^4 + 1} \right| \leq \frac{13}{16}.$$
Of course, any M larger than $13/16$ will also work, like $M = 1$. ■

2.3 Sets and Set Building

A *set* is any collection of distinct objects.[2] Some examples of sets might include
$$\text{the alphabet} = \{a, b, c, \ldots, x, y, z\}, \qquad \begin{matrix}\text{Universities in}\\ \text{Toronto}\end{matrix} = \{\text{UofT}, \text{Ryerson}, \text{York}\},$$
$$\text{The Kardashian Sisters} = \{\text{Kim}, \text{Khloe}, \text{Kourtney}\}.$$
We use the symbol '$\in$' (read as 'in') to talk about when an element is in a set; for example, $1 \in \{1, 2, 3\}$ but ☹ $\notin \{\text{dog}, \text{cat}\}$.

Each of the previous examples were *finite* sets, as they consisted of only a finite number of elements. A set can also have infinitely many elements. In such instances, it is inconvenient to write out every element of the set so we use *set builder notation*. Herein, if P is a proposition on the set S, such that for each $x \in S$, $P(x)$ is either true or false, then one can define the set
$$\{x \in S : P(x)\}$$
which consists of all the elements in S which make P true. For example, if M is the set of months in the year, then
$$\{m \in M : m \text{ has 31 days}\} = \{\text{January}, \text{March}, \text{May}, \text{July}, \text{August}, \text{October}, \text{December}\}.$$
This was an example where the resulting set was still finite, but it still demonstrates the compactness of setbuilder notation.

The following are some important infinite sets that we will see throughout the course:

[2] This is not true, since it is possible to define objects called *classes*, but we will not worry about this too much in this context

- The **naturals**[3] $\mathbb{N} = \{1, 2, 3, \ldots\}$,
- The **integers** $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$,
- The **rationals** $\mathbb{Q} = \{p/q : p, q \in \mathbb{Z}, q \neq 0, \gcd(p, q) = 1\}$,
- The **reals** $\mathbb{R}$ (the set of all infinite decimal expansion).

Special subsets of the real numbers are the intervals. The mathematical definition of the interval is somewhat complicated, but you're likely familiar with them. Notationally, we write

$$\begin{aligned} (a,b) &= \{x \in \mathbb{R} : a < x < b\} & (-\infty, b) &= \{x : x \leq b\} \\ (a,b] &= \{x \in \mathbb{R} : a < x \leq b\} & (-\infty, b] &= \{x \in \mathbb{R} : x \leq b\} \\ (a,b] &= \{x \in \mathbb{R} : a \leq x < b\} & (a, \infty) &= \{x \in \mathbb{R} : x > a\} \\ [a,b] &= \{x \in \mathbb{R} : a \leq x \leq b\} & [a, \infty) &= \{x \in \mathbb{R} : x \geq a\} \end{aligned}$$

Definition 2.13

If $a, b \in \mathbb{Z}$, we say that $a|b$ (read a *divides* b), if there exists some integer k such that $b = ak$.

Divisibility is something we'll explore in great detail later in the course, and forms the foundation of a field of mathematics called *number theory*. Number theory is really interested in the primes, with which you should be familiar. Just in case you need a refresher, let's recall the definition below:

Definition 2.14

Let a be an integer. We say that a is *prime number* if the only numbers which divide a are a and 1. We say that a is even if $2|a$, and *odd* otherwise.

2.3.1 Relations on Sets

We can also talk about *subsets*, which are collections of items in a set and indicated with a '$\subseteq$' sign. For example, if P is the set of prime numbers, then $P \subseteq \mathbb{Z}$, since every element on the left (a prime number) is also an element of the right (an integer). Similarly, one has $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$. Note that if A is a set, $A \subseteq A$.

There is a particular distinguished set, known as the *empty set* and denoted by $\emptyset$, which contains no elements. Recalling the definition of a vacuous truth, it is not too hard to convince oneself that the empty set is a subset of every set!

Exercise: Determine the subset relations for the following sets:

1. $S = \{x \in \mathbb{R} : x = 2n, n \in \mathbb{Z}\}$,
2. $T = \left\{x \in \mathbb{R} : x = a - \frac{1}{2}, \forall a \in \mathbb{N}\right\}$,
3. $U = \left\{x \in \mathbb{Q} : x = \frac{p}{2^n}, \gcd(p, k) = 1\right\}$,
4. $V = \{x \in \mathbb{Z} : x = 3^n, n \in \mathbb{N}\}$.

[3] Some mathematicians believe that 0 is a natural number. I am personally undecided, and always just choose which version is more convenient.

Two sets are equal when they contain precisely the same elements. In practice, showing that two sets are equal is usually done by mutual subset inclusion: if A, B are sets then

$$A = B \qquad \Leftrightarrow \qquad A \subseteq B \text{ and } B \subseteq A$$

Example 2.15

Consider the sets

$$A = \{n \in \mathbb{N} : n = 4k + 1 \text{ for some } k \in \mathbb{N}\},$$

$$B = \{n \in \mathbb{N} : n = 4k - 3 \text{ for some } k \in \mathbb{N}\}$$

Show that $A = B$.

Solution. Let's begin by showing that $A \subseteq B$. Let $n \in A$, so that there exists a k such that $n = 4k + 1$. Notice that we can equivalently write $n = 4(k + 1) - 3$, showing that $n \in B$. Since n was arbitrary, we conclude that every element in A is also in B, so $A \subseteq B$.

Conversely, if $n \in B$ then $n = 4k - 3$ for some k. We can write this as $n = 4k - 3 = 4(k - 1) + 1$, showing that $n \in A$. Since n was arbitrary, every element of B is also an element of A, so $B \subseteq A$.

Both inclusions imply that $A = B$, as required. ■

Example 2.16

Let $A = \left\{x \in \mathbb{R} : x^2 - 1 < 0\right\}$ and $B = (-1, 1)$. Show that $A = B$.

Solution. Let $x \in A$ so that $x^2 - 1 < 0$. This means that $x^2 < 1$, which we can solve to get $x \in (-1, 1)$. Hence $x \in B$, and $A \subseteq B$.

Conversely, if $x \in (-1, 1)$ then we know $x^2 < 1$, so $x^2 - 1 < 0$, showing that $x \in B$ and $B \subseteq A$. Both inclusions show that $A = B$. ■

2.3.2 Operations on Sets

Union and Intersection Let S be a set and choose two sets $A, B \subseteq S$. We define the *union* of A and B to be

$$A \cup B = \{x \in S : x \in A \text{ or } x \in B\}$$

and the *intersection* of A and B to be

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

Example 2.17

Determine the union and intersection of the following two sets:

$$A = \{x \in \mathbb{R} : x > 1\}, \qquad B = \{x \in \mathbb{R} : -1 < x < 2\}.$$

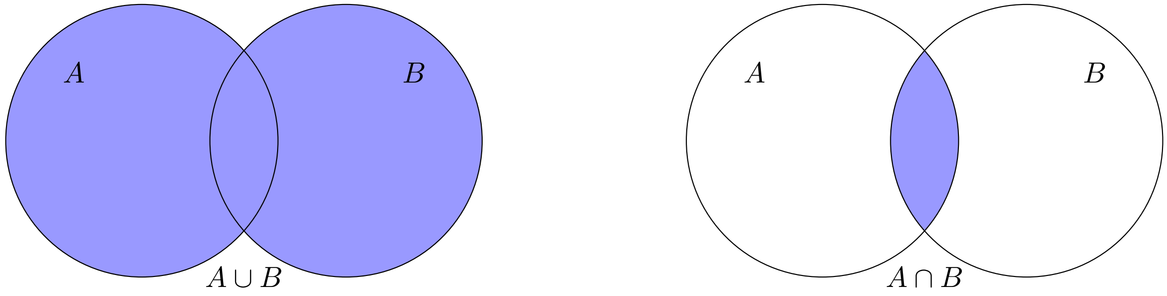


Figure 7: Left: The union of two sets is the collection of all elements which are in both (though remember that elements of sets are distinct, so we do not permit duplicates). Right: The intersection of two sets consists of all elements which are common to both sets.

Solution. By definition, one has

$$\begin{aligned} A \cup B &= \{x \in \mathbb{R} : x \in A \text{ or } x \in B\} = \{x \in \mathbb{R} : x > 1 \text{ or } -1 < x < 2\} \\ &= \{x \in \mathbb{R} : x > -1\}, \\ A \cap B &= \{x \in \mathbb{R} : x \in A \text{ and } x \in B\} = \{x \in \mathbb{R} : x > 1 \text{ and } -1 < x < 2\} \\ &= \{x \in \mathbb{R} : 1 < x < 2\}. \end{aligned}$$ ■

Let $I \subseteq \mathbb{N}$ be an indexing set: Given a collection of sets $\{A_i\}_{i \in I}$ in S, one can take the intersection or union over the entire collection, and this is often written as

$$\bigcup_{i \in I} A_i = \{x \in S : \text{there is an } i \in I, x \in A_i\}, \qquad \bigcap_{i \in I} A_i = \{x \in S : \text{ for every } i \in I, x \in A_i\}.$$

Example 2.18

Consider the set $\{x \in \mathbb{R} : \sin(x) > 0\}$. Write this set as as an infinite union of intervals.

Solution. We are well familiar with the fact that $\sin(x) > 0$ on $(0, \pi)$, $(2\pi, 3\pi)$, $(4\pi, 5\pi)$, etc. If we let the interval $I_n = (2n\pi, (2n+1)\pi)$ then the aforementioned intervals are I_0, I_1, and I_2. We can convince ourselves that that $\sin(x) > 0$ on any of the I_n, and hence

$$\{x \in \mathbb{R} : \sin(x) > 0\} = \bigcup_{n \in \mathbb{Z}} I_n = \bigcup_{n \in \mathbb{Z}} (2n\pi, (2n+1)\pi).$$ ■

Example 2.19

Define $I_n = \left(0, \frac{1}{n}\right) \subseteq \mathbb{R}$. Determine $I = \bigcap_{n \in \mathbb{N}} I_n$.

Solution. By definition, I consists of the elements which are in I_n for every $n \in \mathbb{N}$. We claim that I cannot consist of any positive real number. Indeed, if $p > 0$ then there exists $n \in \mathbb{N}$ such that $\frac{1}{n} < p$, which means that $p \notin I_k$ for all $k \geq n$, and hence cannot be in I. Since I has no positive real numbers, and certainly cannot contain any non-positive real numbers, we conclude that $I = \emptyset$. ■

Exercise: Let $I_n = (-n, n) \subseteq \mathbb{R}$ for $n \in \mathbb{N}$. Determine both $\bigcup_n I_n$ and $\bigcap_n I_n$.

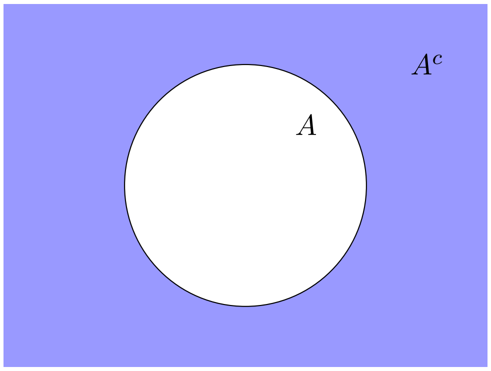


Figure 8: The complement of a set A with respect to S is the set of all elements which are in S but not in A.

Complement If $A \subseteq S$ then the *complement* of A with respect to S is all elements which are not in A; that is,

$$A^c = \{x \in S : x \notin A\}.$$

Example 2.20

Determine the complement of $I = \bigcup_{n\in\mathbb{Z}} (2n\pi, (2n+1)\pi)$ from Example 2.18, with respect to $\mathbb{R}$.

Solution. Since I contains all the open intervals of the form $(2n\pi, (2n+1)\pi)$ we expect its complement to contain everything else. Namely,

$$I^c = \bigcup_{n\in\mathbb{Z}} [(2n-1)\pi, 2n\pi]. \qquad \blacksquare$$

Example 2.21

For any sets A and B, let $A \setminus B = \{x \in A : x \notin B\}$. Show that $A \setminus B = A \cap B^c$.

Solution. We begin by showing that $A \setminus B \subseteq A \cap B^c$. Let $x \in A \setminus B$, so that we know $x \in A$ but $x \notin B$. Since $x \notin B$ we know that $x \in B^c$, and since $x \in A$ and $x \in B^c$ we know $x \in A \cap B^c$. This shows that $A \setminus B \subseteq A \cap B^c$.

The reverse direction is almost identical. Let $x \in A \cap B^c$ so that $x \in A$ and $x \in B^c$. The statement $x \in B^c$ is equivalent to saying that $x \notin B$, so $x \in A$ and $x \notin B^c$ implies that $x \in A \setminus B$.

Both inclusion give the equality $A \setminus B = A \cap B^c$, as required. $\blacksquare$

Exercise:

1. Show that $(A \cup B)^c = A^c \cap B^c$,
2. Show that $(A \cap B)^c = A^c \cup B^c$,
3. Verify that $I^c = \bigcap_{n \in \mathbb{Z}} (2n\pi, (2n+1)\pi)^c$ is an equivalent solution for Example 2.20.

Example 2.22

Let A, B, C be sets. Show that $(B \setminus A) \cup (C \setminus A) = (B \cup C) \setminus A$.

Solution. We must show two inclusions, so let's start with $(\subseteq)$. Let $x \in (B \setminus A) \cup (C \setminus A)$, so that $x \in (B \setminus A)$ or $x \in (C \setminus A)$. For our first case, suppose $x \in B \setminus A$, in which case $x \in B$ and $x \notin A$. But as $x \in B$, we know $x \in B \cup C$, so $x \in B \cup C$ and $x \notin A$ implies $x \in (B \cup C) \setminus A$. Precisely the same reasoning holds if we take $x \in C \setminus A$, so $(B \setminus A) \cup (C \setminus A) \subseteq (B \cup C) \setminus A$.

Conversely, suppose $x \in (B \cup C) \setminus A$, so that $x \in B \cup C$ and $x \notin A$. Since $x \in B \cup C$, we know either $x \in B$ or $x \in C$. Suppose for now that $x \in B$. Since $x \in B$ and $x \notin A$, we know $x \in (B \setminus A)$, so $x \in (B \setminus A) \cup (C \setminus A)$. Exactly the same reasoning holds if we assume $x \in C$, so $(B \setminus A) \cup (C \setminus A) \subseteq (B \cup C) \setminus A$.

Both inclusions give equality, as required. ■

Cartesian Product The Cartesian product of two sets A and B is the collection of ordered pairs, one from A and one from B; namely,

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

A geometric way (which does not generalize well) is to visualize the Cartesian product as sticking a copy of B onto each element of A, or vice-versa. For our purposes, the main example of the product will be to define higher dimensional spaces. For example, we know that we can represent the plane $\mathbb{R}^2$ as an ordered pair of points $\mathbb{R}^2 = \{(x, y) : x, y \in \mathbb{R}\}$, while three dimensional space is an ordered triple $\mathbb{R}^3 = \{(x, y, z) : x, y, z \in \mathbb{R}\}$. In this sense, we see that $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$, $\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$, and motivates the more general definition of $\mathbb{R}^n$ as an ordered n-tuple

$$\mathbb{R}^n = \underbrace{\mathbb{R} \times \cdots \times \mathbb{R}}_{n\text{-times}}.$$

Exercise: We have swept some things under the rug in defining $\mathbb{R}^n$, largely because the true nature is technical and boring. There is no immediate reason to suspect that $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$ should be well defined: we first need to check that the Cartesian product is associative; that is, $(\mathbb{R} \times \mathbb{R}) \times \mathbb{R} = \mathbb{R} \times (\mathbb{R} \times \mathbb{R})$. By definition, the left-hand-side is

$$(\mathbb{R} \times \mathbb{R}) \times \mathbb{R} = \{((a,b),c) : (a,b) \in \mathbb{R} \times \mathbb{R}, c \in \mathbb{R}\}$$

while the right-hand-side is

$$\mathbb{R} \times (\mathbb{R} \times \mathbb{R}) = \{(a,(b,c)) : a \in \mathbb{R}, (b,c) \in \mathbb{R} \times \mathbb{R}\}.$$

Syntactically, neither of these looks the same as $\mathbb{R}^3 = \{(a,b,c) : a,b,c \in \mathbb{R}\}$, but nonetheless they all define the same data.

Exercise: Let $S^1 = \left\{(x,y) : x^2 + y^2 = 1\right\} \subseteq \mathbb{R}^2$ be the unit circle. What familiar shape is $S^1 \times S^1$?

2.3.3 Functions Between Sets

Given two sets A, B, a function $f : A \to B$ is a map which assigns to every point in A a *unique* point of B. If $a \in A$, we usually denote the corresponding element of B by $f(a)$. When specifying the function, one may write $a \mapsto f(a)$. The set A is termed the *domain*, while B is termed the *codomain*.

Some examples of functions are as follows:

1. Define $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, (m,n) \mapsto 3^m 2^n$. For example, $f(2,2) = 3^2 2^2 = 36$.
2. If $\text{Poly}_{\mathbb{Q}}$ is the set of all polynomials with rational coefficients, $\pi : \text{Poly}_{\mathbb{Q}} \to \mathbb{Q}$ given by $\pi(p) = p(0)$ is a function. For example, if $p(x) = \frac{1}{2}x^2 - x + \frac{17}{18}$ then $\pi(p) = \frac{17}{18}$.
3. Consider the function
$$f : \mathbb{R} \to \mathbb{Q}, \qquad x \mapsto \begin{cases} \frac{1}{q} & \text{if } x \in \mathbb{Q}, x = \frac{p}{q}, \gcd(p,q) = 1 \\ 0 & \text{otherwise} \end{cases}.$$
If you have taken calculus before, this is an example of a function which is continuous on $\mathbb{R} \setminus \mathbb{Q}$ and discontinuous on $\mathbb{Q}$.

The *graph* of a function $f : A \to B$ is the set

$$\Gamma(f) = \{(x, f(x)) \in A \times B\}.$$

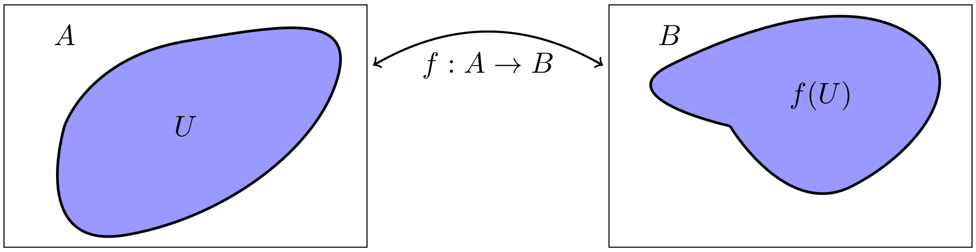
When $f : \mathbb{R} \to \mathbb{R}$, this coincides with the notion of a graph with which you are familiar.

It is important to note that not every element of B needs to be hit by f; that is, B is not necessarily the range of f. Rather, B represents the ambient space to which f maps. Also, if either of the domain or codomain changes the function itself changes. This is because the data of the domain and codomain are intrinsic to the definition of a function. For example, $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$ is a different function than $g : \mathbb{R} \to [0, \infty)$, $g(x) = x^2$.

Definition 2.23

Let $f : A \to B$ be a function.

1. If $U \subseteq A$, then we define the *image* of U to be
$$f(U) = \{y \in B : \exists x \in U, f(x) = y\} = \{f(x) : x \in U\}.$$
2. If $V \subseteq B$, we define the *pre-image* of V to be
$$f^{-1}(V) = \{x \in A : f(x) \in V\}.$$



Note that despite being written as $f^{-1}(V)$, the preimage of a set does not say anything about the existence of an inverse function.

Example 2.24

Let $f : \mathbb{R} \to \mathbb{R}$ be specified by $f(x) = x^2$. Determine $f([0, 1])$ and $f^{-1}(f([0, 1])$.

Solution. By definition, one has
$$f([0, 1]) = \{f(x) : x \in [0, 1]\} = [0, 1].$$
On the other hand, since $f([0, 1]) = [0, 1]$ we know that $f^{-1}(f([0, 1])) = f^{-1}([0, 1])$ for which
$$f^{-1}([0, 1]) = \{x \in \mathbb{R} : f(x) \in [0, 1]\} = [-1, 1]. \blacksquare$$

Example 2.25

Let $f(x) = x^2/(1 + x^2)$. Show that $f(\mathbb{R}) = [0, 1)$.

Solution. First we notice that for any $x \in \mathbb{R}$, $f(x) \geq 0$. Indeed, since $x^2 \geq 0$ then $1 + x^2 \geq 0$, giving
$$\frac{x^2}{1 + x^2} \geq 0.$$

When $x = 0$ we do in fact have $f(x) = 0$ so this inequality is saturated. Now we also have $f(x) < 1$, since

$$1 + x^2 > x^2, \qquad \text{and so} \quad \frac{x^2}{1+x^2} < 1.$$

These two facts together imply that $f(\mathbb{R}) \subseteq [0, 1)$. To show the other direct, we must show that every element of $[0, 1)$ is equal to $f(x)$ for some $x \in \mathbb{R}$. Let $y \in [0, 1)$ and notice that

$$\begin{aligned} f(x) = y \quad &\Leftrightarrow \quad \frac{x^2}{1+x^2} = y \\ &\Leftrightarrow \quad x^2 = y + x^2 y \\ &\Leftrightarrow \quad x^2(1-y) = y \\ &\Leftrightarrow \quad x = \sqrt{\frac{y}{1-y}}. \end{aligned}$$

Notice that it was necessary for $0 \leq y < 1$ to ensure that the term $y/(1-y)$ under the square root is positive. Since this value of x maps to y, we have $[0, 1) \subseteq f(\mathbb{R})$, and equality then follows from the double inclusion. ■

Example 2.26

If $f : \mathbb{R} \to \mathbb{R}$ is given by $f(x) = \dfrac{2|x+1|}{3|x|+2}$, show that $f(\mathbb{R}) = [0, 1]$.

Solution. We need to show a double subset inclusion, for which we start with ($\subseteq$). Suppose $y \in f(\mathbb{R})$, so that $y = f(x)$ for some $x \in \mathbb{R}$; namely,

$$y = \frac{2|x+1|}{3|x|+2}.$$

Both the numerator and denominator of y are positive, so $y \geq 0$. Applying the triangle inequality gives us

$$y = \frac{2|x+1|}{3|x|+2} \leq \frac{2|x|+2}{3|x|+2} \leq \frac{3|x|+2}{3|x|+2} = 1,$$

so that $y \leq 1$. Both inequalities show that $y \in [0, 1]$, so $f(\mathbb{R}) \subseteq [0, 1]$.

For the other direction, there are a few arguments that could be made. First of all, note that $f(-1) = 0$ and $f(0) = 1$, showing that the endpoints of $[0, 1]$ are actually achieved.

1. Since f is continuous on $[-1, 0]$, the Intermediate Value Theorem implies that every value between $[0, 1]$ is acheived, and so $[0, 1] \subseteq f(\mathbb{R})$.

2. On $[-1, 0]$ we know both $|x| \leq 0$ and $|x + 1| \leq 0$. Let $y \in [0, 1]$, so that

$$y = \frac{-2x-2}{-3x+2} \quad \Leftrightarrow \quad x = \frac{2y+2}{3y-2} \in \mathbb{R}.$$

Hence $[0, 1] \subseteq f(\mathbb{R})$.

In either case, both inclusions give the desired equality. ■

Example 2.27

Let $f : \mathbb{R}^3 \to \mathbb{R}^2$ be given by $f(x, y, z) = (x, y)$. If

$$S^2 = \left\{(x, y, z) \in \mathbb{R}^3 : x^2 + y^2 + z^2 = 1\right\},$$

determine $f(S^2)$.

Solution. Let $(a, b, c) \in S^2$ so that $a^2 + b^2 + c^2 = 1$. The image of this point under f is $f(a, b, c) = (a, b)$. It must be the case that $a^2 + b^2 \leq 1$, and so $f(S^2) \subseteq D^2 = \left\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 \leq 1\right\}$. We claim that this is actually an equality; that is, $f(S^2) = D^2$. In general, to show that two sets A and B are equal, we need to show $A \subseteq B$ and $B \subseteq A$. As we have already shown that $f(S^2) \subseteq D^2$, we must now show that $D^2 \subseteq f(S^2)$.

Let $(a, b) \in D^2$ so that $a^2 + b^2 \leq 1$. Let $c = \sqrt{1 - a^2 - b^2}$, which is well-defined by hypothesis. Then $a^2 + b^2 + c^2 = 1$ so that $(a, b, c) \in S^2$, and $f(a, b, c) = (a, b)$. Thus $f(S^2) = D^2$. ■

Exercise: Let $f : \mathbb{R}^3 \to \mathbb{R}^2$ be the function given in Example 2.27. Determine $f^{-1}(D^2)$.

Example 2.28

Let $f : X \to Y$ be a function, with $A, B \subseteq X$. Show that $f(A \cap B) \subseteq f(A) \cap f(B)$.

Solution. Let $y \in f(A \cap B)$ so that $y = f(x)$ for some $x \in A \cap B$. Since $x \in A \cap B$ we know that $x \in A$ and $x \in B$. This in turn implies that $f(x) \in f(A)$ and $f(x) \in f(B)$, so that $y = f(x) \in f(A) \cap f(B)$. ■

Exercise: Does the converse to Example 2.28 hold? More precisely, is it the case that $f(A) \cap f(B) \subseteq f(A \cap B)$, and therefore the two sets are actually equal?

2.3.4 Properties of Functions

Definition 2.29

A function $f : [a, b] \to \mathbb{R}$ is said to be

1. *increasing on* $[a, b]$ if whenever $x_1, x_2 \in [a, b]$ satisfy $x_1 < x_2$, then $f(x_1) \leq f(x_2)$. We say that f is *strictly increasing on* $[a, b]$ if $x_1 < x_2$ implies that $f(x_1) < f(x_2)$.

2. *decreasing on* $[a, b]$ if whenever $x_1, x_2 \in [a, b]$ satisfy $x_1 < x_2$, then $f(x_1) \geq f(x_2)$. We say that f is *strictly decreasing on* $[a, b]$ if $x_1 < x_2$ implies that $f(x_1) > f(x_2)$.

Definition 2.30

A function $f : \mathbb{R} \to \mathbb{R}$ is said to be *bounded* if there exists an $M > 0$ such that $|f(x)| \leq M$ for all $x \in \mathbb{R}$.

Furthermore, note that if $f, g : A \to B$ are functions, then anything that can be done to points in B can be done to f and g, by defining the operations in a pointwise fashion. For example, if $f, g : \mathbb{R} \to \mathbb{R}$, then since we can add/multiply in the codomain $\mathbb{R}$, we can similarly perform these actions on f, g as

$$(f+g)(x) = f(x) + g(x), \qquad (fg)(x) = f(x)g(x).$$

Example 2.31

Show that if $f, g : \mathbb{R} \to \mathbb{R}$ are bounded, then $f + g$ is bounded as well.

Solution. Since both functions are bounded, there exists an $M_1 > 0$ and $M_2 > 0$ such that $|f(x)| < M_1$ and $|g(x)| < M_2$ for all $x \in \mathbb{R}$. Define $M = M_1 + M_2$, which we claim will work for the sum $f + g$. Indeed, for any $x \in \mathbb{R}$ we have

$$|f(x) + g(x)| \leq |f(x)| + |g(x)| < M_1 + M_2 = M$$

which is what we wanted to show. ■

2.4 Ordered Fields

Chances are you have seen the real numbers $\mathbb{R}$ before. In fact, you might even think that you have a good understanding of the real number. The reality is, the real numbers are actually an incredibly subtle and difficult object with which to play. In this section, I will show you examples of other objects, called *fields* which have similar properties to the real numbers.

2.4.1 The Field Axioms

Fields are actually very complicated mathematical objects that have a lot of underlying structure. This means that in order to tell you what a field does, I must enumerate a great deal of axioms.

Definition 2.32

Given a set S, a *(closed) binary operator* is a function $b : S \times S \to S$.

The definition of a binary operator is somewhat self-explanatory. Binary describes the number 2, so a binary operator is something which operates on two elements of S and produces another element of S. The additional adjective *closed* is used to describe the fact that the output of elements in S remains in S.

For example, multiplication and addition of integers are both closed binary operators. We abuse notation somewhat, and write

$$\begin{aligned} + : \mathbb{Z} \times \mathbb{Z} &\to \mathbb{Z}, \\ (a, b) &\mapsto a + b, \end{aligned} \qquad\qquad \begin{aligned} \times : \mathbb{Z} \times \mathbb{Z} &\to \mathbb{Z}, \\ (a, b) &\mapsto a \times b \end{aligned}$$

However, notice that division is *not* a closed binary operator, since dividing two integers need not give back an integer. For example, $1, 2 \in \mathbb{Z}$, but $\div(1, 2) = 1/2$ is not an integer.

Definition 2.33

A field is any set F equipped with two closed binary operators $\oplus, \otimes$, called addition and multiplication respectively, such that for any $x, y, z \in F$ we have

1. [Associativity] $x \oplus (y \oplus z) = (x \oplus y) \oplus z$ and $x \otimes (y \otimes z) = (x \otimes y) \otimes z$,
2. [Commutativity] $x \oplus y = y \oplus x$ and $x \otimes y = y \otimes x$
3. [Identity] There exist distinct numbers 0_F and 1_F such that for any $x \in F$, $x \oplus 0_F = x$ and $x \otimes 1_F = x$.
4. [Additive Inverses] For any $x \in F$ there exists $n \in F$ such that $x \oplus n = 0_F$. We usually write $n = -x$.
5. [Multiplicative Inverses] For any *non-zero* number $x \in F$, there exists $r \in F$ such that $x \otimes r = 1_F$. We usually write $r = x^{-1}$.
6. [Distributivity] $x \oplus (y \times z) = (x \oplus y) \oplus (x \otimes z)$

The distributivity property is essential, since it says that addition and multiplication play together nicely; that is, they are compatible. Out of laziness, we will write $\cdot$ for $\otimes$, $+$ for $\oplus$, and simply 0 and 1 for the identities from now on.

1. The real numbers $\mathbb{R}$ and the rational numbers $\mathbb{Q}$ are both fields (check this as best you can). However, $\mathbb{Z}$ and $\mathbb{N}$ are not fields. In the case of $\mathbb{N}$, elements do not have additive inverses. In the case of $\mathbb{Z}$, elements do not have multiplicative inverses.

2. Define a binary operator on $\mathbb{N}$ called the *modulo operation*, where $a \bmod b$ is the remainder when a is divided by b. For example,

   $$5 \bmod 2 = 1, \quad 8 \bmod 3 = 2, \quad 19 \bmod 5 = 4, \quad 72 \bmod 10 = 2$$

   Consider the set $F_2 = \{0, 1\}$ where addition and multiplication are done modulo 2; that is,

   $$a + b = (a + b) \bmod 2, \qquad a \cdot b = (a \cdot b) \bmod 2.$$

   This is a field, with multiplication and addition tables given by

$+$	0	1
0	0	1
1	1	0

,

$\cdot$	0	1
0	0	0
1	0	1

.

Similarly, $F_3 = \{0,1,2\}$ with addition and multiplication done modulo 3 is a field, with addition and multiplication tables

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

,

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

However, $F_4 = \{0,1,2,3\}$ with addition and multiplication given modulo 4 is *not* a field, as we will show in Example 2.37.

3. [Advanced Example] Let $P_1(F_2)$ be the degree one polynomials with coefficients in F_2 satisfying the identity $x^2+x+1=0$:

$$P_1(\mathbb{R}) = \left\{ax+b : a,b \in F_2, x^2+x+1=0\right\}.$$

This is a field with precisely four elements, $\{0,1,x,x+1\}$. Addition and multiplication tables are given by

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

,

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Example 2.34

If F is a field, show that for any $x \in F$, $x \cdot 0 = 0$.

Solution. Notice that

$$\begin{aligned} x \cdot 0 &= x \cdot (0+0) && \text{by (3)} \\ &= (x\cdot 0) + (x \cdot 0) && \text{by (6)} \end{aligned}$$

Let $-(x\cdot 0)$ be the additive inverse of $x \cdot 0$, guaranteed to exist by (4), so

$$\begin{aligned} 0 &= (x\cdot 0) + [-(x\cdot 0)] \\ &= [(x\cdot 0)+(x\cdot 0)] + [-(x\cdot 0)] && \text{from above} \\ &= (x\cdot 0) + \underbrace{[(x\cdot 0)+[-(x\cdot 0)]]}_{=0} && \text{by (6)} \\ &= x \cdot 0 \end{aligned}$$

as required. ■

Example 2.35

If F is a field then the identity elements are unique

Solution. Let z be any additive identity element, so that $z + x = x$ for all $x \in F$. In addition, we have that $z + x = x = x + 0$. Let $-x$ be the additive identity for x, so that

$$0 = x + (-x) = (z + x) + (-x) = z + (x + (-x)) = z$$

showing that necessarily, $z = 0$. A similar argument holds for the multiplicative identity. ■

Example 2.36

If F is a field then inverse elements are unique.

Solution. Let $x \in F$, and take n, m to be additive inverses so that $x + n = 0 = x + m$. Notice that

$$n = (x + m) + n = (x + n) + m = m$$

showing that $n = m$ and demonstrating uniqueness of inverses. A similar argument holds for multiplicative inverses. ■

Example 2.37

If F is a field and $x, y \in F$ satisfy $xy = 0$, then either $x = 0$ or $y = 0$.

Solution. Suppose that $xy = 0$. If both x and y are zero then the result certainly holds, so assume without loss of generality that x is non-zero. Since x is non-zero, it has a multiplicative inverse x^{-1}, which implies

$$y = (x^{-1} \cdot x)y = x^{-1} \cdot (x \cdot y) = x^{-1} \cdot 0 = 0$$

showing that $y = 0$. ■

Example 2.37 shows that F_4 cannot be a field. Indeed, in F_4 we have that $2 \cdot 2 = 0$ but neither of these is zero. If F_4 were a field, then Example 2.37 says that one of these must be zero, and that is not the case.

Example 2.38

Let $\mathbb{F}_3 = \{0, 1, x\}$ be a field with three elements. Determine $1 + x^{-1}$.

Solution. We claim that $1 + x^{-1} = 0$ (look at the chart in the examples above). To show this, let's assume that it's not the case and show that something weird happens.

If $1 + x^{-1} \neq 0$, then it must have a multiplicative inverse, and its is either 1 or x. If its inverse is 1, then

$$1 \cdot (1 + x^{-1}) = 1 \quad \Rightarrow \quad 1 + x^{-1} = 1 \quad \Rightarrow \quad x^{-1} = 0.$$

But this would imply that $x \cdot x^{-1} = 1 = 0$, which cannot happen.

If the inverse is x, then

$$x \cdot (1 + x^{-1}) = 1 \quad \Rightarrow \quad x + 1 = x \quad \Rightarrow \quad 1 = 0$$

which is also not possible. We conclude that $1 + x^{-1}$ cannot be inverted, so it must be 0. ■

2.4.2 Ordered Fields

We have already looked at an ordering on the real numbers, where by definition we say that $a < b$ if $b - a > 0$. We generalize this notion as follows:

Definition 2.39

If F is a field, a subset $P \subseteq F$ is a *positive set* if

1. [Closure] For any $x, y \in P$, $x + y \in P$ and $xy \in P$,
2. [Trichotomy] For any non-zero $x \in F$, either $x \in P$ or $-x \in P$.

Notice that the set of positive real numbers is a positive set in $\mathbb{R}$. If F admits a positive set P, we can define an ordering on F by saying that $x < y$ if $y - x \in P$. By $y - x$ we of course mean $y + (-x)$, but we shall be sloppy with that notation henceforth. Any field endowed with an ordering is said to be an *ordered field*.

Proposition 2.40

Let F be an ordered field.

1. If $x < y$ and $y < z$ then $x < z$.
2. If $c > 0$ and $x < y$ then $cx < cy$.
3. If $x < y$ and $u < v$ then $x + u < y + v$

Proof. The proofs effectively imitate what we do in $\mathbb{R}$.

1. By definition, we have that $y - x \in P$ and $z - y \in P$. Hence
$$z - x = z + (y - y) + x = \underbrace{(z - y)}_{\in P} + \underbrace{(y - x)}_{\in P} \in P$$
using the closure of P under addition. Since $z - x \in P$ we conclude $x < z$.

2. Note that $c > 0$ is equivalent to $c - 0 = c \in P$, so we know that $c \in P$. Furthermore, we know that $y - x \in P$. Hence
$$cy - cx = c(y - x) \in P$$
using the closure of P under multiplication.

3. We know that $y - x \in P$ and $v - u \in P$, so
$$(y + v) - (x + u) = \underbrace{(y - x)}_{\in P} + \underbrace{(v - u)}_{\in P} \in P$$
by closure of additivity. □

Ordered fields must have infinitely many elements. Assume that $1 \in P$. Since P is closed under addition, by repeatedly using Proposition 2.40(3), we must have

$$0 < 1 < 1+1 < 1+1+1 < 1+1+1+1 < \cdots$$

and this must go on for ever. If our field only has finitely many elements, then at some point this process must begin to cycle back on old numbers, allowing us to show something along the lines of $x < x$, which is not possible.

2.4.3 Complete Fields

Definition 2.41

If F is an ordered field, we say that a subset $S \subseteq F$ is *bounded from above* if there exists an element $M \in F$ such that for all $x \in S$, $x < M$. In this case, we say that M is an *upper bound* of S.

A bounded set has many possible upper bounds. For example, the set $S = \{1/n : n \in \mathbb{N}\} \subseteq \mathbb{Q}$ is bounded, with an upper bound of 2. But 3, or 4, or in fact any rational number larger than 2 is also an upper bound for S.

This pattern is typical. If M is an upper bound for S and $M < N$, then for every $x \in S$ we have

$$x < M < N$$

showing that N is also an upper bound for S. An interesting question which naturally arises is then "Is there a least upper bound?"

Definition 2.42: The Completeness Axiom

An ordered field F is *complete* if whenever $S \subseteq F$ is bounded from above, there exists a *least upper bound* of S.

For example, the set $S = \left\{x \in \mathbb{Q} : x^2 < 2\right\}$ is certainly bounded above, since $x < 2$ for all $x \in S$. However, this set does not have a least upper bound in the rational numbers. Therefore, $\mathbb{Q}$ is not complete. However, notice that $\mathbb{R}$ is a complete ordered field, and in fact is constructed in such a manner as to guarantee that it is complete.

It is possible to show that $\mathbb{R}$ is in essence the *only* complete ordered field, in the sense that any other field which is complete and ordered is essentially just $\mathbb{R}$ in disguise.

3 Mathematical Logic

3.1 Mathematical Predicates

A *logical predicate* is a statement about objects in S which evaluate to either true or false. We will denote predicates by a capital letter, such as P, in which case $P(x)$ is read as "x satisfies property P" or some other equivalent sentence.

Simple examples of predicates include

$P(x)$	“x is a dog,”
$P(x)$	“x has a birthday today,”
$P(x,y)$	“x and y have the same calculus lecture,”
$P(x,y,z)$	“The sum of x and y is greater than z,”

where we have left the choice of universe to context.

As demonstrated above, there is no limit on the number of objects discussed in a predicate and, given an explicit description of x (or y and z as appropriate), one can assign a value of true or false to each predicate. In the first instance where $P(x)$ reads “x is a dog,” it is hopefully clear that $P(\text{Dalmation})$ is true, while $P(\text{Beluga})$ is false.

Not everything is a mathematical statement. For example, ‘15^2’ is not a statement: there is no way to assign a value of true or false to ‘15^2’.

Example 3.1

If $x, y \in \mathbb{N}$ we say that x is divisible by y if there is no remainder when we divide x by y. Consider the predicate $P(x,y)$ representing “x is divisible by y.” Evaluate the truth of $P(x,y)$ on the following pairs (x,y):

$$(5,2), \quad (35,5), \quad (0,1), \quad (1,0).$$

Solution. The statement $P(5,2)$ is that “5 is divisible by 2.” This is false for the division yields $5 = 2 \cdot 2 + 1$, leaving a remainder of 1. On the other hand, $P(35,5)$ is true, since $35 = 5 \cdot 7$ with no remainder. $P(0,1)$ is also true as $0 = 0 \cdot 1$ and in fact, this would be true regardless of which number we had chosen for y. The only contentious example occurs when trying to evaluate $P(1,0)$, since we cannot divide by zero. In this case, we adhere to the convention that no number is divisible by zero, so that $P(1,0)$ is false. As in previous case, $P(1,0)$ would be false regardless of our choice of x. ■

Remark 3.2 You might be disturbed at the idea of writing false mathematical statements, such as “5 is divisible by 2.” Morality aside, it is important to realize that we can write false statements in English is well. For example, the statement “Pigs can fly” is obviously false, but this does not prevent me from writing it down. While we will eventually endeavour to only write true statements, for the moment it is important to consider false statement as well.

3.2 Universal and Existential Quantifiers

Quantifiers allow us to discuss the number of objects which satisfy a predicate. If we wish to discuss *every* element of a set, we use the *universal quantifier* $\forall$, read as “for all.” To state that an element in a set *exists*, we use the *existential quantifier* $\exists$, read as ”there exists.”

When combined with a predicate P, we can assign truth values to quantified statements. For example, let S be a universe of discourse. The statement $\forall x \in S, P(x)$ will be true precisely when $P(x)$ is true for every element in S. On the other hand, $\exists x \in S, P(x)$ will be true as long as a single element of S makes $P(x)$ true.[4]

The addition of quantifiers allows us to make statements such as the following:

- Every cow has a favourite radio station.
- There is a black horse.
- In every sport, there exists someone who breaks the rules.
- There is one textbook that every class uses.

These last two examples have multiple quantifiers. Can you spot them?

Example 3.3

Determine whether each of the quantified statements is true or false.

1. $\forall x \in \mathbb{N}, x^2 \geq 0$
2. $\exists x \in \mathbb{R}, x = \sqrt{-1}$,
3. $\forall x \in \mathbb{Q}, \forall y \in \mathbb{Q}, x + y \in \mathbb{Q}$,
4. $\exists x \in \mathbb{N}, \exists y \in \mathbb{N}, x/y \in \mathbb{N}$.

Solution.

1. This statement is true, since squaring any non-zero real number results in a positive number.
2. This statement is false. If such an x existed, it would also satisfy $x^2 = -1$. By our comment in part 1, the square of a non-zero number is always positive, leading us to a contradiction.
3. This statement is true. Write $x = a/b$ and $y = c/d$ so that
$$x + y = \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$
Since $ad + bc \in \mathbb{Z}$ and $bd \in \mathbb{N}$, this is also a rational number.
4. This statement is true. For example, by setting $x = 4$ and $y = 2$ we have $x/y = 4/2 = 2$, which is also a natural number. ■

Notice how the above solutions demonstrated the truth of quantifier statements. To show that $\exists x \in S, P(x)$, we find a single example of an $x \in S$ which makes $P(x)$ true. To show that

[4] A simple mnemonic for remembering which symbol corresponds to which quantifier is that "for all" looks like an upside down A which stands for ALL, and "there exists" looks like a backwards E which stands for EXISTS.

$\forall x \in S, P(x)$ is more subtle. Rather than try to demonstrate $P(x)$ for every x, we choose an *arbitrary* $x \in S$. If $P(x)$ is true for an arbitrary x, then it must be true for every x.

Doubly quantified statements must be treated with caution. One may freely interchange two adjacent quantifiers of the *same* type, but not of different type. For example, the statements

$$\forall x \in \mathbb{Q}, \forall y \in \mathbb{Q}, x + y \in \mathbb{Q} \quad \text{is logically equivalent to} \quad \forall y \in \mathbb{Q}, \forall x \in \mathbb{Q}, x + y \in \mathbb{Q},$$

and

$$\exists x \in \mathbb{N}, \exists y \in \mathbb{N}, x/y \in \mathbb{N} \quad \text{is logically equivalent to} \quad \exists y \in \mathbb{N}, \exists x \in \mathbb{N}, x/y \in \mathbb{N}.$$

However, interchanging existential and universal quantifiers can lead to serious trouble.

Example 3.4

Consider the statements

$$\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, \ x + y = 0 \tag{3.1}$$

and

$$\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, \ x + y = 0. \tag{3.2}$$

Compare these expressions by translating them as follows:

1. Convert the mathematical notation into English.
2. Turn the sentence derived above into a simple sentence, which does not involve any variables.
3. Evaluate whether each statement is true or false.

Solution. We start with equation (3.1) for which a direct translation of the notation into English gives us

"For all x in the real numbers, there exists y in the real numbers, (such that) $x + y = 0$."

This is fine but not very enlightening. By recognizing that $x + y = 0$ is equivalent to $x = -y$, we could also re-interpret this sentence as saying "For every real number there is another real number which is its negative." Dropping the superfluous words we arrive at the intuitive statement

"Every real number has a negative."

This statement is certainly true: Given an integer a, we can construct its negative to be $-a$.

Looking at (3.2) we have

$$\exists y \in \mathbb{Z}, \forall x \in \mathbb{Z}, \ x + y = 0. \tag{3.3}$$

Using the same translation process as above, the corresponding simple sentence is given by

"There is an element which is the negative of every integer."

This says there is a number to which we can add any other number and always get zero. Certainly this is not true! If it were, then there would be a number n such that $n + a = 0$ and $n + b = 0$ for any integers a and b. Equating these expressions, we would find that $n + a = n + b$ which in turn implies that $a = b$. This would force all integers to be equal, which is nonsense. ■

Example 3.4 teaches us that changing the order of the quantifiers significantly changes the logical statement, and hence the truth of that statement. To borrow a term from the computer scientists, universal quantifiers admit a 'scope' to the existential quantifiers they precede. For example, the statement $\forall x, \exists y, P(x, y)$ means that the choice of y is allowed to depend upon x. The statement $\exists y, \forall x, P(x, y)$ does not confer this dependence: the choice of y must work for every x.

Example 3.5

Let S be the set of all students in a classroom, and $B(a, b)$ be the statement "student a has the same birthday as student b." Write the mathematical statements

$$\forall a \in S, \forall b \in S, B(a, b), \qquad \forall a \in S, \exists b \in S, B(a, b)$$

$$\exists a \in S, \forall b \in S, B(a, b), \qquad \exists a \in S, \exists b \in S, B(a, b)$$

in plain language.

Solution. We may interpret each of the statements as follows:

$\forall a \in S, \forall b \in S, B(a, b)$ Every student (a) in the classroom has the same birthday as every other student (b) in the classroom

$\forall a \in S, \exists b \in S, B(a, b)$ For each student (a) in the classroom, there exists some other student (b) in the classroom with the same birthday.

$\exists a \in S, \forall b \in S, B(a, b)$ There exists a student (a) who has the same birthday as every other student (b) in the classroom.

$\exists a \in S, \exists b \in S, B(a, b)$ There exists a student (a) in the classroom who has the same birthday as another student (b) in the classroom.

■

3.3 And, Or, Not

Three operations allow us to form new predicates from old: The *AND* operation, also known as *conjunction*; the *OR* operation, also known as *disjunction*; and the *NOT* operation, also as *negation*.

- **AND:** When we link two predicates using an *AND* statement, **both** predicates must evaluate to true for the new predicate to be true. Notationally, the statement $P(x)$ AND $Q(x)$ is written $P(x) \wedge Q(x)$.

  For example, if our universe is $\mathbb{N}$, let $E(x)$ represent "x is even" and $P(y)$ represents "y is positive." The statement $E(x) \wedge P(y)$ is then "x is even and y is positive,"

$$E(2) \wedge P(2) \text{ is true}, \qquad E(4) \wedge P(-1) \text{ is false},$$

$$E(3) \wedge P(1) \text{ is false}, \qquad E(1) \wedge P(-1) \text{ is false}.$$

As demonstrated, if either $E(x)$ or $P(y)$ is false, then $E(x) \wedge P(y)$ will also be false.

- **OR:** An *OR* statement will evaluate to true when **at least one** of the component predicates is true. The statement $P(x)$ OR $Q(x)$ is written $P(x) \vee Q(x)$.

$$E(2) \vee P(2) \text{ is true}, \qquad E(4) \vee P(-1) \text{ is true},$$
$$E(3) \vee P(1) \text{ is true}, \qquad E(1) \vee P(-1) \text{ is false}.$$

The only way that $E(x) \vee P(y)$ is false is if both $E(x)$ and $P(y)$ is false.

- **NOT:** Finally, negation does not link predicates but rather acts on a single predicate and negates it's truth value. The statement NOT $P(x)$ is written $\neg P(x)$. For example, if $E(x)$ is "x is even," then $\neg E(x)$ is "x is not even." Similarly, $\neg P(x)$ is "x is not positive, and we have

$$\neg E(2) \text{ is false}, \qquad \neg E(3) \text{ is true}, \qquad P(4) \text{ is false}, \qquad P(-1) \text{ is true}.$$

All of these rules can be tricky to remember when trying to absorb the information from the written word. By organizing the truth data of each operation into a *truth table*, we have a quick and easy way of seeing the structure of each logical statement. To facilitate writing out these tables, let T denote TRUE and F denote FALSE. The truth tables for all three operations are given in Table 1.

AND

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

OR

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

NOT

P	$\neg P$
T	F
F	T

Table 1: The truth tables for the AND, OR, and NOT operations.

Example 3.6

Let $O(x)$ represent "x is odd" and $E(x)$ represent "x is even." Compute $O(x) \wedge E(x), O(x) \vee E(x), \neg E(x)$ and $\neg O(x)$ when $x = 1$ and $x = 2$.

Solution. We begin with the case $x = 1$:

$O(1) \wedge E(1)$ "1 is both odd and even." This statement is FALSE, as 1 is certainly not even. This is the second row of the AND truth table.

$O(1) \vee E(1)$ "1 is either odd or even." This statement is TRUE, since 1 is odd. This is the second row of the OR truth table

$\neg E(1)$ "1 is not even." This statement is TRUE as the number 1 is not even.

$\neg O(1)$ "1 is not odd." This statement is FALSE as the number 1 is certainly odd.

Now on to the case for $x = 2$, which is very similar to the $x = 1$ case.

$O(2) \wedge E(2)$ "2 is both odd and even." This statement is FALSE as 2 is not odd. This is the third row of the AND truth table.

$O(2) \vee E(2)$ "2 is either odd or even." This statement is TRUE since 2 is even. This is the third row of the OR truth table.

$\neg E(2)$ "2 is not even." This is FALSE, since 2 is certainly even.

$\neg O(2)$ "2 is not odd." This is TRUE, since 2 is not odd.

■

Example 3.7

Create the truth table corresponding to the statement $\neg(P \wedge Q) \vee R$.

Solution. While it is possible to create the truth table immediately, this is prone to mistakes. By breaking down the truth table into several smaller tables, we obtain a clearer picture and our solution is more robust to error. We start by examining the $\neg(P \wedge Q)$ predicate.

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

Now we add in the disjunction with R into an expanded truth table, which gives

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

We conclude that the statement $\neg(P \wedge Q) \vee R$ is always true except in the case where (P, Q, R) is (T, T, F). ■

Showing that two logical statements are equivalent can be done by showing that they have the same truth table, as the following Proposition demonstrates.

Proposition 3.8

Let P, Q be propositions. The negation of the AND and OR statements are as follows:

$$\neg (P \wedge Q) = (\neg P) \vee (\neg Q), \qquad \neg (P \vee Q) = (\neg P) \wedge (\neg Q).$$

Proof. It suffices to show that the expressions have equivalent truth tables. We will give the result for the first identity, and leave the second as an exercise. The truth tables for the negation of the AND statement are 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

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

The resulting values of the truth table are identical, showing that these statements are in fact equivalent. □

3.3.1 Negating Quantifiers

To develop intuition for negating quantifiers, let's think about how we would disprove a statement involving a quantifier. For example, the universally quantified statement "every horse is black" may be disproved by showing that there exists a non-black horse. Mathematically, if $P(x)$ is "x is a black horse,

$$\text{the negation of} \quad \forall x, P(x) \quad \text{is} \quad \exists x, \neg P(x).$$

The existentially quantified statement "there exists a pink horse" is disproved by showing that "every horse is not pink." Mathematically, if $P(x)$ is the statement "x is a pink horse," then

$$\text{the negation of} \quad \exists x, P(x) \quad \text{is} \quad \forall x, \neg P(x).$$

By thinking about the case of a general predicate P, the negation rules above still apply.

Example 3.9

Consider the mathematical statement $\forall x \in \mathbb{R}, x < x^2$. Determine whether this sentence is true or false, and write the negation of this sentence.

Solution. This sentence is false. For example, if $x = 1/2$ then $x^2 = 1/4$, showing that $x > x^2$. The negation of this sentence is

$$\exists x \in \mathbb{R} : x \geq x^2.$$

Notice that our counter-example satisfies the negation of our sentence, as we would expect. ■

Example 3.10

Negate the sentence ”Every real number has a negative.”

Solution. From Example 3.4 we know that the given sentence can be stated mathematically as

$$\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x + y = 0.$$

Applying our rules for negation, the negative of this sentence becomes

$$\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, x + y \neq 0.$$

Translating this back into an English sentence, we have “There is a real number which has no negative.” ■

3.4 Implications

At the core of mathematical statements are implications, which consist of ‘if-then’ statements. A typical theorem contains a *hypothesis* and a *conclusion*, such that IF the hypothesis is TRUE, THEN the conclusion is TRUE. This is a conditional statement that requires us to first check the truth of the hypothesis before we can ascertain the truth of the conclusion, and is called an implication because the veracity of the first statement implies the veracity of the second.

To frame this mathematically, let P and Q be predicates. The statement “If P then Q,” or alternatively “P implies Q,” is written $P \Rightarrow Q$ and has truth table given by Table 2.

IMPLICATION

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

Table 2: The truth table for the implication $P \Rightarrow Q$.

Carefully consider the bottom two rows of Table 2, which are known as *vacuous truths*. The idea is that a universally false hypothesis P can have any implication it wants, since that implication will never be tested. For example, consider the statement

“If pigs can fly, then the sky is black.”

This is a true statement because whenever pigs can fly then the sky is black. This may seem artificial and contrived, but vacuous truths appear in mathematics frequently, so it is important to be aware of how they are handled.

Example 3.11

Let $D(x)$ be the predicate “x is a dog” and let $A(x)$ be the predicate “x is an animal.” Consider the truth of the implications $D(x) \Rightarrow A(x)$, $A(x) \Rightarrow D(x)$ and $\neg A(x) \Rightarrow \neg D(x)$.

Solution. The arguments are given below:

$D(x) \Rightarrow A(x)$ This is the statement "If x is a dog then it is an animal" or "All dogs are animals" and is TRUE.

$A(x) \Rightarrow D(x)$ This is the statement "If x is an animal then it is a dog" or "All animals are dogs." A cat is an animal which is not a dog, so this implication must be FALSE.

$\neg A(x) \Rightarrow \neg D(x)$ This is the statement "If x is not an animal then it is not a dog," and is a TRUE sentence. Indeed, if x is not an animal then it could not be a dog. If it were a dog, then by our first implication, it would be an animal and this would be a contradiction.

■

Definition 3.12

Let P and Q be predicates with the implication $P \Rightarrow Q$.

- The *contrapositive* of $P \Rightarrow Q$ is the statement $\neg Q \Rightarrow \neg P$.
- The *converse* of $P \Rightarrow Q$ is the statement $Q \Rightarrow P$.

Example 3.11 shows that the converse of true statement is not necessarily true. As for the contrapositive, we have the following result:

Proposition 3.13

If P and Q are predicates, then $P \Rightarrow Q$ and $\neg Q \Rightarrow \neg P$ are logically equivalent.

Proof. You should try proving this result on your own before proceeding further.

The truth table for the contrapositive $\neg Q \Rightarrow \neg P$ is as follows:

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

Comparing this to the truth table for $P \Rightarrow Q$ given in Table 2, we see that the truth values are identical as required. □

When both $P \Rightarrow Q$ and its converse $Q \Rightarrow P$ are true, we write $P \Leftrightarrow Q$ and say that "P is true *if and only if* Q is true." This means that the statements P and Q are logically equivalent: whatever truth value $P(x)$ has, $Q(x)$ will have the same. It is difficult at this point to give examples of "if and only if" statements that are not just trivial restatements of one another, but some examples might include:

- An integer $n \in \mathbb{Z}$ is even if and only if $n/2$ is an integer.
- An integer $n \in \mathbb{Z}$ is divisible by 10 if and only if its one's digit is a 0
- A triangle is isosceles if and only if exactly two of its angles are equal.

The words 'necessary' and 'sufficient' are often used to indicate the direction of an implication. If P and Q are predicates, then

- "P is a necessary condition for Q" is the implication $Q \Rightarrow P$,
- "P is a sufficient condition for Q" is the implication $P \Rightarrow Q$,
- "P is necessary and sufficient for Q" is the statement $P \Leftrightarrow Q$.

Example 3.14

Determine the truth table for the statement $(P \vee Q) \Rightarrow (\neg Q \wedge R)$

Solution. Building our truth table in parts, one can find

P	Q	R	$P \vee Q$	$\neg Q \wedge R$	$(P \vee Q) \Rightarrow (\neg Q \wedge R)$
T	T	T	T	F	F
T	T	F	T	F	F
T	F	T	T	T	T
T	F	F	T	F	F
F	T	T	T	F	F
F	T	F	T	F	F
F	F	F	T	F	F
F	F	F	F	F	T

■

Example 3.15

Let $n \in \mathbb{N}$. Show that n is even if and only if n^2 is even.

Proof. We begin with the ($\Rightarrow$) direction, and assume that n is even so that $n = 2k$ for some $k \in \mathbb{N}$. Squaring n gives

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

showing that n^2 is also even.

To prove the ($\Leftarrow$) direction, we will proceed by contrapositive. Assume that n is not even, so that $n = 2k + 1$ for some $k \in \mathbb{N}$. Squaring n gives

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

showing that n^2 is odd. □

3.4.1 Negating an Implication

In Example 3.13 we found that the statement $A(x) \Rightarrow D(x)$, read as "Every animal is a dog," was false. To show that it was false we used the example of a cat, which is an animal but is not a dog. More generally, if P and Q are predicates in a universe S, we say that $x \in S$ is a *counter-example* to $P \Rightarrow Q$ if $P(x)$ is true but $Q(x)$ is not true; that is, $P(x) \wedge \neg Q(x)$ is true. Counter-examples are exactly how implications are negated.

Proposition 3.16

If P and Q are predicates, the negation of the implication $P \Rightarrow Q$ is the statement $P \wedge \neg Q$.

Proof. The truth table for $P \wedge \neg Q$ is given below, along with $P \Rightarrow Q$ for reference

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

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

Comparison of the last column of each table shows that the tables are negations of one another, proving the result. □

Example 3.17

Negate the following sentence: "If x is duck, then x likes peanut butter."

Solution. Here we have the predicates $P(x) =$"x is a duck" and $Q =$"x likes peanut butter' with the sentence above being the implication $P \Rightarrow Q$. The negation of this implication is $P \wedge \neg Q$, or "x is a duck and x does not like peanut butter." ■

Example 3.18

In calculus, we say that $\lim_{x \to c} f(x)$ exists if

$$\exists L \in \mathbb{R}, \forall \epsilon > 0, \exists \delta > 0, \forall x \in \mathbb{R}, |x - c| < \delta \Rightarrow |f(x) - L| < \epsilon.$$

Negate this sentence to determine the mathematical statement that a limit does not exist.

Solution. Applying our rules for negation, the limit does not exist if the following sentence is satisfed:

$$\forall L \in \mathbb{R}, \exists \epsilon > 0, \forall \delta > 0, \exists x \in \mathbb{R}, |x - c| < \delta \text{ and } |f(x) - L| \geq \epsilon. \qquad \blacksquare$$

3.5 Contradiction (*Reductio ad absurdum*)

Let P and Q be predicates, and consider the problem of showing that the statement $T : P \Rightarrow Q$ is true. A proof by contradiction proceeds by assuming that T is false (or $\neg T$ is true), and showing that something bad happens. More specifically, if R is some other predicate which may not be directly related to P or Q, then

$$\neg T \Rightarrow (R \wedge \neg R) \tag{3.4}$$

is a true statement. Here we recall that for any predicate R, $R \wedge \neg R$ is always false, so we have shown that the assumption that $\neg T$ is true leads to a contradiction.

We can use a truth table to verify that the truth of T perfectly corresponds with the truth of (3.4). Indeed

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

Hence one can prove that T is true using Equation (3.4).

There is a small group of mathematicians that objects to using proof by contradiction, the so called *constructivists*. One of the consequences of using contradiction proofs is that one can show an object exists without being able to construct it (by assuming it doesn't exist and arriving at a contradiction). In fact, there are cases where we can show that something exists, but have no examples of it.

Proposition 3.19

In the decimal expansion of π, one of the digits $\{0, 1, 2, \ldots, 8, 9\}$ occurs infinitely often.

Proof. For the sake of contradiction, assume that each of the above digits occurs only finitely many times in the decimal expansion of π. Let N_i be the number of times the digit i appears, so that the decimal expansion of π consists of

$$N_0 + N_1 + \cdots + N_9$$

digits. As each N_i is finite, so too is this sum. If π has only a finite decimal expansion, it is necessarily rational. Since we know that π is not rational, this is a contradiction and we conclude that some digit must occur infinitely often. □

Note that this proof is not constructive: we do not know which digit occurs infinitely often. In fact, it is an open problem whether each digit occurs infinitely often.

Proposition 3.20

If A and B are sets, then $A \cap (B \setminus A) = \emptyset$.

Proof. For the sake of contradiction, assume that $A \cap (B \setminus A) \neq \emptyset$, so that the there exists an element $x \in A \cap (B \setminus A)$. By definition of the intersection, $x \in A$ and $x \in B \setminus A$. However, $x \in B \setminus A$ implies that $x \notin A$, contradicting the fact that $x \in A$. Hence $A \cap (B \setminus A) = \emptyset$. □

Proposition 3.21

The number $\sqrt{2}$ is irrational.

Proof. For the sake of contradiction, assume that $\sqrt{2}$ is rational and write $\sqrt{2} = p/q$ where $\gcd(p, q) = 1$; that is, p/q is in lowest terms. Hence $q\sqrt{2} = p$ and by squaring both sides we get

$$2q^2 = p^2.$$

Notice that $2q^2$ is even, and so therefore p^2 must also be even. By Example 3.15 we know that p is therefore also even, so $p = 2k$ for some $k \in \mathbb{N}$. Substituting this back into our equation, we get

$$2q^2 = (2k)^2 = 4k^2 \qquad \Leftrightarrow \qquad q^2 = 2k^2$$

so that similarly, q^2 is even. This implies that q is even, so $q = 2\ell$. However, this is a contradiction. We assumed that p and q were written in lowest terms, but have demonstrated that both are even. Hence $\sqrt{2}$ is not rational and so must be irrational. □

Example 3.22

Show that there are no natural solutions to the equation $x^2 - 4y^2 = 7$.

Solution. Suppose for the sake of contradiction that a solution exists. Note that we can factor the left hand side, giving $x^2 - 4y^2 = (x - 2y)(x + 2y) = 7$. Since 7 is prime, its two factors are either $-1, -7$ or $1, 7$, but we can throw away the negative factors since $x + 2y > 0$.

Thus we either have $x - 2y = 1$ and $x + 2y = 7$, or $x - 2y = 7$ and $x + 2y = 1$. In either case, if we add the two equations together we get $x = 4$. In the first case, this implies that $y = 3/2$ which is not possible. In the latter case, $y = -3/2$, which is also not possible. Hence we've arrived at a contradiction, and no solutions can exist. ■

Example 3.23

Show that $x^3 + x^2 = 1$ has no rational solutions.

Solution. Suppose that a solution exists, and write it in lowest terms as $x = a/b$. Substituting in we get

$$\frac{a^3}{b^3} + \frac{a^2}{b^2} = 1 \quad \Rightarrow \quad a^3 + a^2 b = b.$$

Now we have three cases: Either both a, b are odd; a is even and b is odd; or a is odd and b is even. Note that both cannot be even, as we've assumed a/b is in lowest terms.

1. If both are odd, then a^3, a^2b, and b are all odd. But this cannot happen, since if a^3 and a^2b are odd, then $a^3 + a^2b$ is even.
2. If a is even and b is odd, a^3 is even, a^2b is even, and b is odd. This leads to the same problem, as $a^3 + a^2b$ is then even.
3. If a is odd and b is even, then a^3 is odd, a^2b is even, and b is even. But then $a^3 + a^2b$ is odd, which is a contradiction.

Thus there cannot be any rational solutions to the given equation. ■

3.6 A Rigmarole of Random Results

Let's practice doing some proofs!

Example 3.24

Show that the function $f(x) = \dfrac{3x}{x+4}$ is injective; namely, if $a \neq b$ then $f(a) \neq f(b)$.

Solution. Proceeding by contrapositive, it is sufficient to show that whenever $f(a) = f(b)$ then $a = b$:

$$\begin{aligned} f(a) = f(b) \quad &\Leftrightarrow \quad \frac{3a}{a+4} = \frac{3b}{b+4} \\ &\Leftrightarrow \quad 3a(b+4) = 3b(a+4) \\ &\Leftrightarrow \quad 3ab + 12a = 3ab + 12b \\ &\Leftrightarrow \quad 12a = 12b \\ &\Leftrightarrow \quad a = b. \end{aligned}$$

This is precisely what we wanted to show, so the result follows. ■

Example 3.25

There exists *irrational* a and b such that a^b is rational.

Solution. We know that $\sqrt{2}$ is irrational (though we have not yet proven this). If $\sqrt{2}^{\sqrt{2}}$ is rational we are done, setting $a = b = \sqrt{2}$. Otherwise, it is irrational, in which case

$$(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^2 = 2$$

works, with $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$. ■

3.6.1 Some Number Theory

Definition 3.26

If $a, b \in \mathbb{Z}$ we say that $a|b$ (read "a divides b") if there exists $k \in \mathbb{Z}$ such that $ak = b$.

For example, $5|35$ since $5 \cdot 7 = 35$, while $2 \not| 5$ since there is no integer k for which $2k = 5$.

Proposition 3.27

If $a|b$ and $a|c$, then for any $m, n \in \mathbb{Z}$, $a|(mb + nc)$.

Proof. Our hypotheses indicate that $a|b$ and $a|c$, so there exist $k, \ell \in \mathbb{Z}$ such that $ak = b$ and $a\ell = c$. Using these equations, we can write

$$mb + nc = m(ak) + n(a\ell) = a(mk + n\ell)$$

showing that $a|(mb + nc)$ as required. □

Proposition 3.28

If $a|b$ and $a|(b + c)$ then $a|c$.

Proof. By assumption, there exists k, ℓ such that $ak = b$ and $a\ell = b + c$. Using the latter equation, we can write

$$c = a\ell - b = a\ell - ak = a(\ell - k)$$

showing that $a|c$ as required. □

Recall that $p \in \mathbb{Z}$ is a prime if its only factors are 1 and p. A number which is not prime is called *composite*, and necessarily has non-trivial factors other than 1 and itself.

Proposition 3.29

Every natural number can be written as a product of primes.

Proof. For the sake of contradiction, assume that not every natural can be written as a product of primes. In particular, there must be a smallest such number, say n. This number cannot be prime itself, otherwise it is trivially a product of primes, so n is necessarily composite and can be written as $n = rs$ for $1 < r \leq s < n$.

Both $r, s < n$, and since n is the smallest number than cannot be written as a product of primes, both r and s must be writable as products of primes. However, combining those primes then gives a decomposition of n into a product of primes, which contradicts our assumption. We conclude the result, as required. □

Theorem 3.30: Euclid's Proof of the Infinitude of Primes

There are infinitely many prime numbers.

Solution. For the sake of contradiction, assume that there are only finitely many primes, and list them as $p_1, p_2, \ldots, p_n$. Consider the number $x = p_1 p_2 \cdots p_n + 1$. This number is larger than any of the given primes, and hence cannot be prime itself.

We claim that x cannot be written as a product of prime numbers. Indeed, suppose that p_k were a factor of x, so that $p_k | x$. Since $p_k | p_1 p_2 \cdots p_k$, by Proposition 3.28 we would have $p_k | 1$, and this is not possible. Hence no prime can be a factor of x, and so x cannot be written as a product of primes. This contradicts Proposition 3.29, so our original assumption must have been false; that is, there are infinitely many primes. ■

4 Induction

Mathematical induction is a proof technique used to show that a result holds for every natural number $\mathbb{N}$. It operates on the domino principle, by creating a chain of implications which extends to every natural number. For example, suppose $\mathbb{N}$ is our universe and we would want to show $P(n)$ is true for every $n \in \mathbb{N}$. If we can show that $P(1)$ is, and then $P(k) \Rightarrow P(k+1)$, then the result holds for any n. This is precisely because

$$P(1) \Rightarrow P(2) \Rightarrow P(3) \Rightarrow \cdots \Rightarrow P(n-1) \Rightarrow P(n) \Rightarrow \cdots$$

and since $P(1)$ is true, so too is every $P(n)$ thereafter.

Mathematical Induction

Let P be some predicate. If $P(1)$ is true, and $P(k) \Rightarrow P(k+1)$ for any k, then $P(n)$ is true *for all* $n \in \mathbb{N}$

Thus mathematical induction consists of two steps. The first is to demonstrate the *base case* that $P(1)$ is true. The second is to invoke the *induction hypothesis* that $P(k)$ is true for some k, and demonstrate that $P(k) \Rightarrow P(k+1)$.

Example 4.1

Show, using mathematical induction, that $2n + 2 \leq 4n$ for all integers $n \geq 1$.

Solution.

1. **Base Case:** The smallest number for which this occurs is $n = 1$, and in this case we have $2n + 2 = 4$ and $4n = 4$, so the result holds in the base case.

2. **Induction Step:** Assume that $2k+2 \leq 4k$ for some natural number k. We want to show that $2(k+1)+2 \leq 4(k+1)$. Indeed, notice that

$$\begin{aligned} 4(k+1) &= 4k+4 \\ &\geq (2k+2)+2 && \text{using the induction hypothesis } 4k \geq 2k+2 \\ &= 2k+4 = 2(k+1)+2. \end{aligned}$$

We conclude from the induction principle that $2k+2 \leq 4k$ for all $k \in \mathbb{N}$. ■

Example 4.2

Show that for every $n \in \mathbb{N}$, $2n \leq 2^n$.

Solution.

1. **Base Case:** When $n=1$ one has $2 \leq 2$ which is a true statement, so the base case holds.
2. **Induction Step:** Assume that for some n we know that $2n \leq 2^n$. Now

$$\begin{aligned} 2^{n+1} &= 2(2^n) \\ &\geq 2(2n) = 4n \\ &\geq 2n+2 && \text{by Example 4.1} \\ &= 2(n+1) \end{aligned}$$

which is what we wanted to show. ■

Example 4.3

Show that the triangle inequality extends to more than two variables; namely,

$$|x_1 + x_2 + \cdots + x_n| \leq |x_1| + |x_2| + \cdots + |x_n|.$$

Solution. The base case occurs when $n=2$, since this is the first instance in which the inequality makes sense. We have already proven this though, so the base case is done.

Assume then that $|x_1 + \cdots + x_n| \leq |x_1| + \cdots + |x_n|$, and notice that

$$\begin{aligned} |x_1 + \cdots + x_n + x_{n+1}| &= |(x_1 + \cdots + x_n) + x_{n+1}| \\ &\leq |x_1 + \cdots + x_n| + |x_{n+1}| && \text{by the base case} \\ &\leq |x_1| + \cdots + |x_n| + |x_{n+1}| && \text{by the induction hypothesis} \end{aligned}$$

giving the desired result. ■

Example 4.4

Prove that for all positive integers k, $5|6^k - 1$.

Solution.

1. **Base Case:** The simplest case is $k = 1$, for which we see that $6^k - 1 = 5$. Clearly $5|5$ since $5/5 = 1$, so the base case is satisfied.

2. **Induction Step:** For some positive integer k, assume that $5|6^k - 1$. Since by hypothesis, we know that $5|6^k - 1$ we know there is some integer d such that $\frac{6^k-1}{5} = d$. Consider $6^{k+1} - 1$ which we may write as

$$\begin{aligned} 6^{k+1} - 1 &= 6(6^k) - 1 \\ &= (1+5)(6^k) - 1 \\ &= 5(6^k) + (6^k - 1) \end{aligned}$$

We claim that 5 divides this number. To see that this is the case, let us divide by 5 and see what we get.

$$\begin{aligned} \frac{6^{k+1} - 1}{5} &= \frac{5(6^k) + (6^k - 1)}{5} \\ &= \frac{5 \cdot 6^k}{5} + \frac{6^k - 1}{5} \\ &= 6^k + d && \text{by induction hypothesis.} \end{aligned}$$

This is clearly an integer, so $5|6^{k+1} - 1$ as required. ■

Example 4.5: Bernoulli's Inequality

Show that for all $x \geq -1$ and $n \in \mathbb{N}$, we have

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

Solution. When $n = 1$ we have $1 + x = 1 + nx$ so the inequality is true. Assume then that $(1+x)^n \geq 1 + nx$, so that

$$\begin{aligned} (1+x)^{n+1} &= (1+x)^n(1+x) \\ &\geq (1+nx)(1+x) = 1 + x + nx + nx^2 \\ &= 1 + (n+1)x + nx^2 \\ &\geq 1 + (n+1)x \end{aligned}$$

where we have used the fact that $nx^2 \geq 0$. This is what we wanted to show, so the inequality is true. ■

Definition 4.6

If S is a set, we denote by $\mathcal{P}(S)$ the *power set of S*, which is the collection of all subsets of S.

Example 4.7

Show that if $|S| < \infty$ is a finite set, then $|\mathcal{P}(S)| = 2^{|S|}$.

Solution. There are actually many ways to show this is true. The simplest is the following: To count the number of elements in $\mathcal{P}(S)$, note that each element $x \in S$ is either in a subset, or not in a subset. Hence each x has two possible states it can be in. The set of all possible states for all possible elements is therefore $2^{|S|}$, and we are done.

However, we can proceed by induction on the size of $|S|$ instead. If $|S| = 0$ then $S = \emptyset$, and $\mathcal{P}(S) = \{\emptyset\}$ has size $2^0 = 1$. The base case is thus true.

Now assume that the number of subsets of a set with n elements is 2^n, and let S have $n+1$ elements

$$S = \{s_1, \ldots, s_n, s_{n+1}\}.$$

Notice that every subset of S either contains s_{n+1} or does not. Of those that do contain s_{n+1}, there are 2^n possible subsets (corresponding to the subsets of $\{s_1, \ldots, s_n\}$). Similarly, of those that do not contain s_{n+1} there are also 2^n such subsets. All together, there are $2^n + 2^n = 2^{n+1}$ such subsets, as required. ■

As a brief aside, one sometimes denotes the power set by 2^S for this reason. Hence $2^{\mathbb{N}}$ and $2^{\mathbb{R}}$ are the power sets of $\mathbb{N}$ and $\mathbb{R}$ respectively. There is yet another reason why this notation is great. In general, if A and B are sets, then

$$A^B = \{f : B \to A\};$$

that is, the set of all functions from A to B. It is possible to show that the subsets of S are in one-to-one correspondence with the functions $f : S \to \{0,1\}$, wherein if $T \subseteq S$, then we define

$$f_T(x) = \begin{cases} 1 & x \in T \\ 0 & x \notin T \end{cases},$$

and so $\mathcal{P}(S) = \{0,1\}^S = 2^S$, where we identify $2 = \{0,1\}$, since this set has two elements.

Example 4.8

Show that for all $n \in \mathbb{N}$ a $2^n \times 2^n$ chessboard with a single tile removed can be L-tiled; that is, tiled by an L-shape consisting of three squares.

Solution. The base case is when $n = 1$, in which we are tasked with tiling a 2×2 chessboard with one tile removed. This is immediately possible, so we are done.

Assume then that any $2^n \times 2^n$ board with a single tile removed admits an L-tiling, and consider a $2^{n+1} \times 2^{n+1}$ board. Divide this board into four quarters, so that each quarter has dimension $2^n \times 2^n$. By rotating the board if necessary, assume that the missing tile is located in the upper-left quadrant. We place our first tile as illustrated in Figure **??**. Note that, excluding the placement of the first tile, every quadrant is now a $2^n \times 2^n$ board with a single tile removed. By the induction hypothesis, each board admits an L-tiling, so those tiling combined give the tiling of the $2^{n+1} \times 2^{n+1}$ board. ■

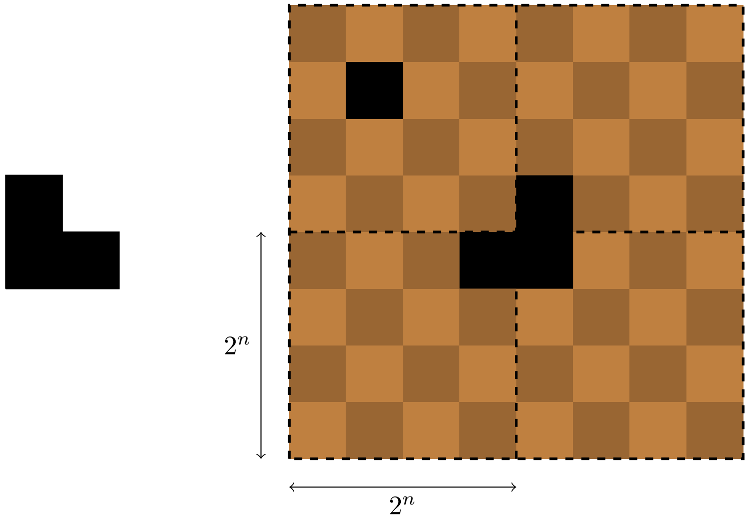


Figure 9: Left: The base case. A 2×2 board with a single tile removed is an L-shape, and so admits an L-tiling. Right: The induction step. By placing the first tile as such, each of the quadrants is a $2^n \times 2^n$ board with a single tile removed.

4.1 Summation and Product Notation

Sigma notation is used to make complicated sums much easier to write down. In particular, we use a summation index to iterate through elements of a list and then sum them together. Consider the expression

$$\boxed{\sum_{i=n}^{m} r_i \qquad (4.1)}$$

which is read as "the sum from $i = n$ to m of r_i." The element i is known as the *dummy* or *summation* index, n and m are known as the *summation bounds*, and r_i is the *summand*. In order to decipher this rather cryptic notation, we adhere to the following algorithm:

1. Set $i = n$ and write down r_i;

2. Add 1 to the index i and add r_i to the current sum;

3. If i is equal to m then stop, otherwise go to step 2 and repeat.

For those computer savvy students out there, this is nothing more than a for-loop. Interpreting (4.1) we thus have

$$\sum_{i=n}^{m} r_i = r_n + r_{n+1} + r_{n+2} + \cdots r_m.$$

Example 4.9

Let k be some fixed positive integer such that $k \geq 1$. Show that

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

Solution. As always, we follow the program enumerated above.

1. **Base Case:** Here we check the easiest possible case, which corresponds to $k = 1$. When $k = 1$ the left-hand-side becomes

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

which the right-hand-side is $\frac{1}{1+1} = \frac{1}{2}$. Clearly both sides agree, so the base case is satisfied.

2. **Induction Step:** Let k be some fixed by arbitrary number and assume that

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

We would like to show that the result holds for $k+1$. It makes most sense to start by working with the left-hand-side, since it will give us the most "flexibility." Notice that

$$\begin{aligned}
\sum_{n=1}^{k+1} \frac{1}{n(n+1)} &= \left.\frac{1}{n(n+1)}\right|_{n=k+1} + \sum_{n=1}^{k} \frac{1}{n(n+1)} \\
&= \frac{1}{(k+1)(k+2)} + \frac{k}{k+1} && \text{via the induction hypothesis} \\
&= \frac{1+k(k+2)}{(k+1)(k+2)} = \frac{k^2+2k+1}{(k+1)(k+2)} && \text{common denominator} \\
&= \frac{(k+1)^2}{(k+1)(k+2)} = \frac{k+1}{k+2} && \text{factoring and cancelling} \\
&= \frac{(k+1)}{(k+1)+1}.
\end{aligned}$$

This is precisely what we wanted to show, and so we are done. ■

Example 4.10

Show that for any $k \geq 1$ we have

$$\sum_{n=1}^{k} n^2 = \frac{n(n+1)(2n+1)}{6}. \tag{4.2}$$

Solution. The base case is $k = 1$, in which case we get

$$1^2 = 1 = \frac{1 \times 2 \times 3}{6},$$

which is a true statement. Thus assume that (4.2) holds for some k, and notice that

$$\begin{aligned}
\sum_{n=1}^{k+1} n^2 &= \sum_{k=1}^{n} n^2 + (n+1)^2 \\
&= \frac{n(n+1)(2n+1)}{6} + (n^2 + 2n + 1) && \text{by Induction Hypothesis} \\
&= \frac{(2n^3 + 3n^2 + n) + (6n^2 + 12n + 6)}{6} \\
&= \frac{2n^3 + 9n^2 + 13n + 6}{6} \\
&= \frac{(n+1)(n+2)(2n+3)}{6},
\end{aligned}$$

which is precisely the correct equation for $n + 1$. ■

Pi notation works in precisely the same way, except that instead of adding we multiply:

$$\prod_{i=1}^{n} r_i = r_1 r_2 r_3 \cdots r_{n-1} r_n.$$

so for example, factorial notation can be expressed using Pi-notation as

$$n! = \prod_{i=1}^{n} i = 1 \cdot 2 \cdot 3 \cdots n$$

or sometimes one sees double factorial notation

$$\begin{aligned}
(2n)!! &= \prod_{i=1}^{n} (2i) = 2 \cdot 4 \cdot 6 \cdots (2n-2) \cdot (2n) \\
(2n+1)!! &= \prod_{i=1}^{n} (2i-1) = 1 \cdot 3 \cdot 5 \cdots (2n-1) \cdot (2n+1)
\end{aligned}$$

Example 4.11

Show that

$$\prod_{r=2}^{n} \left(1 - \frac{1}{r^2}\right) = \frac{n+1}{2n}. \tag{4.3}$$

Solution. In the base case we have $n = 2$, so the left hand side is $1 - 1/4 = 3/4$, while the right hand side is $(2+1)/(2 \cdot 2) = 3/4$. These are equal, so the base case holds.

Assume then that (4.3) holds for some n, so that

$$\begin{aligned}\prod_{r=2}^{n+1}\left(1-\frac{1}{r}^{2}\right) &= \prod_{r=2}^{n}\left(1-\frac{1}{r^2}\right)\left(1-\frac{1}{(n+1)^2}\right)\\ &= \left(\frac{n+1}{2n}\right)\left(\frac{n^2+2n}{(n+1)^2}\right)\\ &= \frac{n(n+1)(n+2)}{2n(n+1)^2}\\ &= \frac{n+2}{2(n+1)}\end{aligned}$$

exactly as desired. ■

4.2 More General Induction

The principle of induction can be extended beyond just $\mathbb{N}$. For example, suppose we want to show that the predicate $P(n)$ is true for all even numbers greater than or equal to 10. Here the base case is to demonstrate $P(10)$, followed by $P(2n) \Rightarrow P(2n+2)$. This creates the chain of implications

$$P(10) \Rightarrow P(12) \Rightarrow P(14) \Rightarrow \cdots \Rightarrow P(2n) \Rightarrow$$

demonstrating $P(n)$ for all even numbers at least 10. This idea is easily generalized to any other induction scheme. Of course, this can be seen as equivalent to induction by renaming $Q(n)$ as the statement $P(2n)$ is true.

An ostensibly different type of induction is that of *strong induction*. We again aim to create a chain of implications, but now we make a stronger induction hypothesis.

Theorem 4.12: Strong Induction

Let P be some predicate. Suppose that $P(1)$ is true, and moreover

$$P(1) \wedge P(2) \wedge \cdots \wedge P(k) \Rightarrow P(k+1)$$

for any k, then $P(n)$ is true *for all* $n \in \mathbb{N}$

Proof. We will proceed by using (normal) induction. Let $Q(k) = P(1) \wedge \cdots \wedge P(k)$. Since $Q(1) = P(1)$, the base case is true. Now assume that $Q(n)$ is true. Since $Q(n) \Rightarrow P(n+1)$, then $Q(n+1)$ is true as well. By induction, $Q(n)$ holds for all n, and this is only possible if all $P(n)$ are true, as required. □

Hence (Induction) ⇒ (Strong Induction). Moreover, since normal induction uses a weaker hypothesis, we see that (Strong Induction) ⇒ (Induction). This shows that induction and strong induction are actually equivalent.

Example 4.13

Show that any postage amount greater than 8 cents can be formed by using 3 cent and 5 cent stamps.

Solution. Let $P(n)$ be the statement "A postage of n cents can be made of 3 and 5 cent stamps." As our base cases,

$$P(8) = 3(1) + 5(1), \qquad P(9) = 3(3) + 5(0), \qquad P(10) = 3(0) + 5(2).$$

Now assume that $P(k)$ is true for all $8 \leq k \leq n$, for which we will show that $P(n+1)$ is true. Indeed, notice that we can write $n + 1 = (n - 2) + 3$. By our induction hypothesis, we know that a postage of $n - 2$ stamps can be resolved, say by r three-cent stamps and s five cent stamps, thus

$$n + 1 = (n - 2) + 3 = [3(r) + 5(s)] + 3 = 3(r + 1) + 5(s)$$

as required. ■

Example 4.14

Consider a two-player game, consisting of two bowls of marbles. Each player takes a turn removing any *positive* number of marbles from a *single* bowl. The player that removes the last marble wins. Show that if both bowls have an identical number of marbles, the player who goes second always has a winning strategy.

Solution. Let $P(n)$ be the statement "Player two wins when both bowls have n marbles." The base case is $n = 1$, in which both bowls have a single marble. Player one must remove at least one marble from a single bowl. This leaves only one bowl with one marble, so player two wins.

Now assume that $P(k)$ is true for all $1 \leq k \leq n$, for which we will demonstrate $P(k+1)$. Player One must go first, and so remove ℓ marbles from any bowl, leaving a bowl with $(k + 1)$ marbles, and one with $(k + 1 - \ell)$ marbles. Player Two now moves by removing ℓ marbles from the other bowl, leaving each bowl with $k + 1 - \ell$ marbles. The game has thus been reduced to the game with $(k + 1 - \ell) < k$ marbles, and we know $P(k + 1 - \ell)$, so Player Two has a winning strategy. ■

4.2.1 Recursion

Recursive sequences are those sequences whose elements depend explicitly upon previous entries. For example, the well known *Fibonacci* sequence is defined as $x_1 = x_2 = 1$ and $x_n = x_{n-1} + x_{n-2}$. Unfortunately, computing x_n means computing x_k for all $k \leq n$. More appealing would be to find a closed form solution for x_n.

The problem of determining a closed form solution can be rather tricky, and is often relegated to the realm of combinatorial enumeration. However, given a closed form we can use induction to verify the result.

Example 4.15

Consider the recurrence relation $x_1 = 3, x_2 = 7$ and

$$x_k = 5x_{k-1} - 6x_{k-2}.$$

Show that $x_k = 2^k + 3^{k-1}$.

Solution. We will proceed by strong induction. The base cases are

$$x_1 = 2^1 + 3^0 = 3, \qquad x_2 = 2^2 + 3 = 7$$

which agree with our initial configuration. Now assume that $x_k = 2^k + 3^{k-1}$ for all $1 \leq k \leq n$. Examining x_{n+1} we have

$$\begin{aligned} x_{n+1} &= 5x_n - 6x_{n-1} = 5(2^n + 3^{n-1}) - 6(2^{n-1} + 3^{n-2}) \\ &= 5(2^n + 3^{n-1}) - \left[3 \cdot 2^n + 2 \cdot 3^{n-1}\right] \\ &= 2 \cdot 2^n + 3 \cdot 3^{n-1} \\ &= 2^{n+1} + 3^n. \end{aligned}$$

exactly as desired. ■

Example 4.16

Let $x_1 = x_2 = 1$ and $x_n = x_{n-1} + x_{n-2}$ so that x_n is the Fibonacci sequence. Define

$$\alpha_\pm = \frac{1 + \sqrt{5}}{2}.$$

Show that $x_n = (\alpha_+^n - \alpha_-^n)/\sqrt{5}$.

Solution. First note that

$$1 + \alpha_\pm = \alpha_\pm^2$$

owing to the fact that these are the roots of the polynomial $x^2 - x - 1$. It can also be verified by straightforward computation:

$$1 + \alpha_\pm = \frac{1 \pm \sqrt{5}}{2} + 1 = \frac{3 \pm \sqrt{5}}{2}$$

and

$$\alpha_\pm^2 = \frac{1 \pm 2\sqrt{5} + 5}{4} = \frac{6 \pm \sqrt{5}}{4} = \frac{3 \pm \sqrt{5}}{2}.$$

We begin by checking the base cases:

$$\begin{aligned}
\frac{\alpha_+ - \alpha_1}{\sqrt{5}} &= \frac{1}{2\sqrt{5}}\left[(1+\sqrt{5}) - (1-\sqrt{5})\right] \\
&= \frac{2\sqrt{5}}{2\sqrt{5}} = 1 \\
\frac{\alpha_+^2 - \alpha_1^2}{\sqrt{5}} &= \frac{1}{4\sqrt{5}}\left[(1+\sqrt{5})^2 - (1-\sqrt{5})^2\right] \\
&= \frac{(1+2\sqrt{5}+5) - (1-2\sqrt{5}+5)}{4\sqrt{5}} \\
&= 1,
\end{aligned}$$

so both base cases are satisfied. Assume then that $x_k = (\alpha_+^k - \alpha_-^k)/\sqrt{5}$ for all $1 \leq k \leq n$, for which we demonstrate the result for x_{n+1}. Indeed,

$$\begin{aligned}
x_{n+1} = x_n + x_{n-1} &= \frac{\alpha_+^n - \alpha_-^n}{\sqrt{5}} + \frac{\alpha_+^{n-1} - \alpha_-^{n-1}}{\sqrt{5}} \\
&= \frac{\alpha_+^{n-1}(\alpha_+ + 1) - \alpha_-^{n-1}(\alpha_- + 1)}{\sqrt{5}} \\
&= \frac{\alpha_+^{n-1}\alpha_+^2 - \alpha_-^{n-1}\alpha_-^2}{\sqrt{5}} \\
&= \frac{\alpha_+^{n+1} - \alpha_-^{n+1}}{\sqrt{5}}
\end{aligned}$$

as required. ■

4.3 Fallacies

One must think carefully about both the base case and induction step, and ensure that everything is being done correctly. There are some subtly wrong arguments that can be made.

Example 4.17

Let $x_0 = 0$ and $x_1 = 1$ and define $x_n = x_{n-1} + x_{n-2}$. Every x_n is even.

Solution. Let $P(n)$ be the statement x_n is even. Clearly $P(0) = 0$ is even, so the base case is true. Now assume that $P(k)$ is true for all $1 \leq k \leq n$. Since $x_{n+1} = x_n + x_{n-1}$ is the sum of two even numbers, it is even. ■

This proof is certainly wrong, since $x_1 = 1$ and $x_3 = 3$, so what happened? Since x_n depends upon both x_{n-1} and x_{n-2}, we must check two base cases.

Example 4.18

All horses are the same color.

Solution. Let $P(n)$ be the statement "Any group of n horses all have the same colour." Clearly $P(1)$ is true since there is only a single horse in the collection. Now assume that any group of n horses has the same colour, and let $H = \{h_1, \ldots, h_{n+1}\}$ be a set of $n+1$ horses. Break this into the subsets

$$H_1 = \{h_1, \ldots, h_n\}, \qquad H_2 = \{h_2, \ldots, h_{n+1}\}.$$

Each set H_i has only n-horses, so by the induction hypothesis, all horses in each group are the same color. Since $H_1 \cap H_2 \neq \emptyset$, there is a common horse in both H_1 and H_2, implying that every horse in $H = H_1 \cup H_2$ has the same colour. ■

Here the issue is the induction step. The assumption $H_1 \cap H_2 \neq \emptyset$ fails when $n = 2$, since in that case $H = \{h_1, h_2\}$ making $H_1 = \{h_1\}$ and $H_2 = \{h_2\}$.

5 Bijections and Cardinality

5.1 Injective and Surjective Functions

Injectivity is a powerful property of functions. In our context, it will facilitate discussion of inverse functions, to be taken up in Section 5.2

Definition 5.1

A function $f : S \to T$ is said to be *injective* or *one-to-one* if whenever $f(s_1) = f(s_2)$ then $s_1 = s_2$.

The output of an injective function uniquely corresponds to the input; that is, the only way for two outputs to be equal $(f(s_1) = f(s_2))$ is for the inputs to have also been equal $(s_1 = s_2)$. The is also alluded to in the phrase *one-to-one.*

When S and T are both subsets of the real numbers, one can test whether a function f is injective by applying the *Horizontal Line Test* to the graph of f. A function satisfies the Horizontal Line Test if whenever we draw a horizontal line in the plane, it intersects the graph of the function function *at most once.*

A third perspective is to view a function as a collection of arrows as in Figure 10. In this case, a function is injective if every element of the codomain has *at most one* arrow pointing to it.

Example 5.2

Consider the functions $f(x) = x^2$, $g(x) = 1/x$, and $h(x) = 1 + x$. Determine which, if any, of these functions is injective.

Solution. We claim that $f(x) = x^2$ is not injective; that is, we can find two different points $x_1 \neq x_2$ such that $f(x_1) = f(x_2)$. Indeed, notice that $f(-1) = (-1)^2 = 1$ and $f(1) = (1)^2 = 1$ so that $f(-1) = f(1)$. If $f(x)$ were injective, Definition 5.1 would imply that $-1 = 1$, and this is certainly not the case. In fact, it is not too hard to convince ourselves that for any non-zero real number r, we have $f(r) = f(-r)$ since $r^2 = (-r)^2$, but $r \neq -r$.

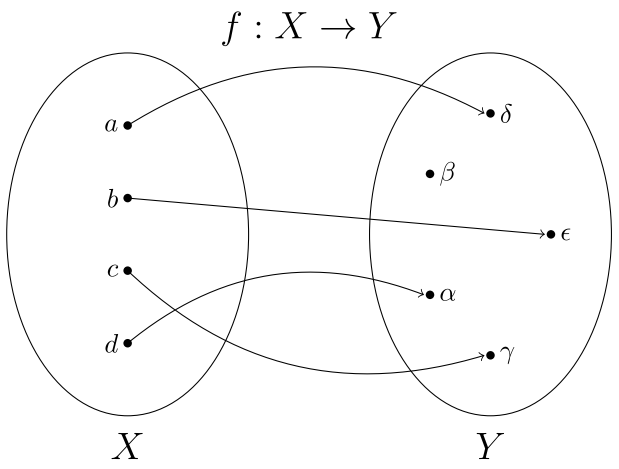


Figure 10: If $f : X \to Y$ is an injective function, each element of the codomain Y has *at most* one arrow pointing at it.

On the other hand, the function g is injective. Assume that $g(x) = g(y)$, which by definition of g this tells us that $1/x = 1/y$. By taking the reciprocal of both sides we get $x = y$ and this is what we wanted to show.

Finally, the function $h(x)$ is injective, since if $h(x) = h(y)$ then $1 + x = 1 + y$. By subtracting 1 from both sides, we get $x = y$ as required. ■

Proposition 5.3

If $f : B \to C$ and $g : A \to B$ are injective functions, then $h = f \circ g : A \to C$ is also injective.

Solution. Assume that $h(x) = h(y)$ for some $x, y \in A$. By definition of h we have $f(g(x)) = f(g(y))$. Since the function f is injective, the only way $f(m_1) = f(m_2)$ is if $m_1 = m_2$, so $f(g(x)) = f(g(y))$ implies that $g(x) = g(y)$. Since g is also injective, it must be the case that $x = y$. Thus we have show that if $h(x) = h(y)$ then $x = y$, showing that h is injective as required. ■

Proposition 5.4

Let $f : B \to C$ and $g : A \to B$ be injective functions. If $f \circ g$ is injective, then g is injective.

Solution. Assume that $g(a_1) = g(a_2)$. Applying f to both sides gives $f(g(a_1)) = f(g(a_1))$. Since the composition $f \circ g$ is injective, this means that $a_1 = a_2$, which is what we wanted to show. ■

The dual notion to an injective function is a surjective function, and this duality will be made clearer in Section 5.2

Definition 5.5

A function $f : S \to T$ is said to be *surjective* or *onto* if for every element $t \in T$, there is an element $s \in S$ such that $f(s) = t$.

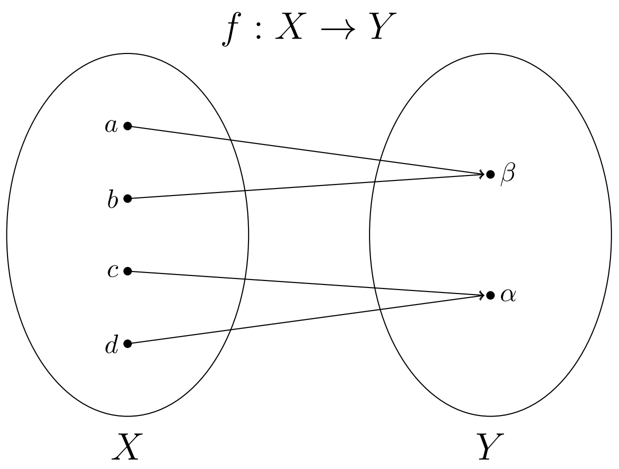


Figure 11: If $f : X \to Y$ is surjective, then every element of the codomain has *at least* one arrow pointing pointing at it.

When thinking about surjective functions, the idea to keep in mind is that every element in T is the image of something in S. Put another way, if f maps elements of S to elements of T, everything in T is hit by something in S. If we describe a function as arrows between sets, a function f is surjective if everything in T has an arrow pointing to it.

Example 5.6

Of the following functions which map $\mathbb{R} \to \mathbb{R}$, determine which maps are surjective:

$$f(x) = x^2, \qquad g(x) = \frac{1}{x}, \qquad h(x) = 1 + x.$$

Solution. For functions $\mathbb{R} \to \mathbb{R}$, a surjective function is the same as a function whose range is all of $\mathbb{R}$. The function $f(x) = x^2$ is therefore not surjective since the range of $f(x)$ is $[0, \infty)$. Similarly, $h(x)$ has range $\mathbb{R}\backslash_{\{0\}}$, so is not surjective. However, the function $h(x)$ is surjective: if y is any real number, we have that y is hit by $y - 1$, since

$$h(y-1) = 1 + (y-1) = y.$$

Thus the range of $h(x)$ is all of $\mathbb{R}$ and we conclude that $h(x)$ is surjective. ■

Proposition 5.7

If $f : B \to C$ and $g : A \to B$ are surjective functions, then $f \circ g : A \to C$ is also surjective.

Solution. Let $c \in C$ be an arbitrary element, for which we need to find an $a \in A$ such that $f(g(a)) = c$. Since f is surjective, there exists $b \in B$ such that $f(b) = c$. Since g is surjective, there exists $a \in A$ such that $g(a) = b$. Now $f(g(a)) = f(b) = c$ as required. ■

Leaving functions we might see in calculus, the following are some further examples:

1. The function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = \sin(x)$ is neither injective nor surjective. Indeed, $\sin(0) = \sin(\pi)$ and $f(\mathbb{R}) = [0, 1]$. No amount of finagling can make f surjective, but we can restrict the domain to ensure that f is injective. An interval of length π is the largest we can take, and a common choices is $[-\pi/2, \pi/2]$.
2. The function $d : \mathbb{R} \to \mathbb{R}^2, x \mapsto (x, x)$ is injective but not surjective. It is injective since if $d(x) = d(y)$ then $(x, x) = (y, y)$ and equating any component gives $x = y$. On the other hand, there is no point in the domain such that $d(x) = (0, 1)$.
3. The function $p : \mathbb{R}^2 \to \mathbb{R}, (x, y) \mapsto x$ is surjective but not injective. It fails to be injective since $f(x, y_1) = x = f(x, y_2)$ for any y_1, y_2. On the other hand, if $x_0 \in \mathbb{R}$ then $f(x_0, 0) = x_0$, showing that the map is surjective.
4. Let $\text{Poly}_{\mathbb{R}}$ be the polynomials with real coefficients, and define $\text{ev}_0 : \text{Poly}_{\mathbb{R}} \to \mathbb{R}$ as $\text{ev}_0(p) = p(0)$. This map is surjective but not injective. Indeed, $\text{ev}_0(x^2 + a) = a = \text{ev}_0(x + a)$ for any $a \in \mathbb{R}$, showing both surjectivity and the failure of injectivity at the same time.

Definition 5.8

A function $f : S \to T$ is bijective if it is both injective and surjective.

If $f : S \to T$ is injective, every element of T has *at most* one arrow pointing at it. If f is surjective, then every element of T has *at least* one arrow pointing at it. If f is bijective (and hence both injective and surjective), this must mean that every element of T has *exactly* one arrow pointing at it. We've shown that compositions of injective/surjective functions are injective/surjective, so it immediately follows that composition of bijections are bijections.

5.2 Inverse Functions

The word "inverse" has many different meanings depending on the context in which it is used. For example, what if we were to ask the student to find the inverse of the number 2? What does this mean? To what are we taking the inverse? To properly understand this, we need to understand the following: Given a binary operator (an operator which takes in two things and produces a single thing in return, such as addition and multiplication of real numbers), we say that a number id is the *identity* of that operator if operating against it does nothing to the input. In the case of addition, the operator will satisfy $x + \text{id}_+ = x$ for all possible x; for example,

$$2 + \text{id}_+ = 2, \qquad -5 + \text{id}_+ = -5.$$

Our experience tells us that $\text{id}_+ = 0$. Similarly, for multiplication the identity $\text{id}_\times$ will satisfy $x \times \text{id}_\times = x$ for all x; for example,

$$3 \times \text{id}_\times = 3, \qquad \pi \times \text{id}_\times = \pi.$$

Again our experience tells us that $\mathrm{id}_\times = 1$. We say that 0 is the *additive identity* and 1 is the *multiplicative identity.*

Given an operator and an identity, we say that the *inverse of* x is an element which, when paired against x, gives the identity. The additive inverse of 2 is the number y such that $2 + y = \mathrm{id}_+ = 0$. In this case $y = -2$, and more generally the additive inverse of n is $-n$. For multiplication, we can convince ourselves that the multiplicative inverse of x is $1/x$; for example, $2 \times (1/2) = 1 = \mathrm{id}_\times$.

Notice that every real number has an additive inverse, while there is no multiplicative inverse for the number 0. In general, one cannot be guaranteed that an inverse always exists.

If $f, g : A \to A$, then function composition $f \circ g$ is another example of a binary operator. What is the identity for this operation? Well, we would like a function $\mathrm{id}_\circ : A \to A$ such that

$$\begin{aligned} f(\mathrm{id}_\circ(x)) &= f(x) \\ &= \mathrm{id}_\circ(f(x)). \end{aligned}$$

The identity function is therefore the function $\mathrm{id}_\circ(x) = x$, the function which does nothing to the argument! Therefore the inverse of a function $f : A \to A$ is another function $f^{-1} : A \to A$ such that $f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}_\circ$.

This conversation can be generalized for functions whose domain and codomain are not equal. For example, if $f : A \to B$ then $f^{-1} : B \to A$. However, we now require two identities functions, $\mathrm{id}_\circ^A : A \to A$ and $\mathrm{id}_\circ^B : B \to B$ such that

$$f^{-1}(f(y)) = \mathrm{id}_\circ^B(y) = y, \qquad f^{-1}(f(x)) = \mathrm{id}_\circ^A(x) = x.$$

Definition 5.9

Let $f : S \to T$ be a function. We say that $g : T \to S$ is a

- *left-inverse* of f if $g(f(s)) = s$ for all $s \in S$,
- *right-inverse* of f if $f(g(t)) = t$ for all $t \in T$,
- *inverse* of f if it is both a left- and right-inverse. We denote the inverse of f as f^{-1}.

Injective functions and surjective functions have left- and right-inverses respectively, as demonstrated in the following propositions:

Proposition 5.10

A function $f : S \to T$ is injective if and only if it has a left-inverse $g : T \to S$.

Proof. Let's begin by assuming that $f : S \to T$ is injective. Define the function $g : T \to S$ as follows: Let $s_0 \in S$ be any element and set

$$g(t) = \begin{cases} s & \text{if } f(s) = t \\ s_0 & \text{otherwise} \end{cases}.$$

If you reexamine Figure **??**, the idea is to simply reverse each given arrow. However, anything which does not already have an arrow pointing to it needs to map somewhere. Hence we choose an arbitrary element s_0 in the domain and map all those points to s_0. To see that g is a left inverse of f, let $s \in S$, in which case $g(f(s)) = s$ by definition of g.

Conversely, assume that f has a left inverse $g : T \to S$ so that $g(f(s)) = s$ for any $s \in S$. Set $f(x) = f(y)$ for which we would like to show that $x = y$. By applying g to both sides we get

$$g(f(x)) = g(f(y)) \quad \Rightarrow \quad x = y$$

so that f is injective as required. □

Proposition 5.11

A function $f : S \to T$ is surjective if and only if it has a right-inverse $g : T \to S$.

Proof. We begin by assuming that $f : S \to T$ is surjective. For each $t \in T$, let $P(t)$ denote the set[5]

$$P(t) = \{s \in S : f(s) = t\} ;$$

that is, $P(t)$ consists of the elements of S which map to t. Since f is surjective, each set $P(t)$ has at least one element, so for each $t \in T$ we choose[6] an element $s_t \in P(t)$. Define the function $g : T \to S$ by $g(t) = s_t$, which we claim is a right-inverse to f. Indeed, $f(g(t)) = f(s_t) = t$ by definition of s_t, as required.

Conversely, assume that there is a function $g : T \to S$ such that $f(g(t)) = t$ for all $t \in T$. We want to show that for each $t \in T$ there is an element $s \in S$ such that $f(s) = t$. The function $g : T \to S$ gives us a way of picking an element in S, so we choose the element $s = g(t) \in S$. It then follows that $f(s) = f(g(t)) = t$ as required. □

Injective functions are precisely those with left-inverses, and surjective functions are those with right-inverses. This is the notion of duality we mentioned before. Definition 5.9 says that a function $f : S \to T$ has an inverse if it has both a left- and a right-inverse, so we can combine Proposition 5.10 and Proposition 5.11 to get the following corollary:

Corollary 5.12

A function $f : S \to T$ is bijective if and only if it has a two-sided inverse $f^{-1} : T \to S$.

Proposition 5.13

If $f : A \to B$ is invertible, its inverse is unique.

[5] The set $P(t)$ is called the *pre-image* of an element t under f, and is usually denoted by $f^{-1}(t)$. However, this is just notation and does not mean that an inverse function f^{-1} exists! To avoid possible confusion, we have chosen not to use this notation for this proof.

[6] Here we have had to use something called the Axiom of Choice. Not all mathematicians believe that such a choice is allowed to be made, but the author is not one of those mathematicians.

Proof. Let $f^{-1} : B \to A$ and $g : B \to A$ be inverses to f, so that

$$f \circ f^{-1} = \mathrm{id}_B, \quad f^{-1} \circ f = \mathrm{id}_A, \qquad f \circ g = \mathrm{id}_B, \quad g \circ f = \mathrm{id}_A.$$

We now exploit the defining property of the identity function and associativity of function composition:

$$g = g \circ \mathrm{id}_B = g \circ (f \circ f^{-1}) = (g \circ f) \circ f^{-1} = \mathrm{id}_A \circ f^{-1} = f^{-1}.$$

Hence $g = f^{-1}$, showing that the inverse function is unique. □

If the function is only left/right invertible, the left/right inverse is certainly not unique.

Example 5.14

If they exist, find the inverses of the following functions:

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto x^2 \end{aligned}, \qquad \begin{aligned} g : \mathbb{R} \setminus \{0\} &\to \mathbb{R} \\ x &\mapsto 1/x \end{aligned}, \qquad \begin{aligned} h : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto 1 + x \end{aligned}.$$

In each case, if the inverse does not exist, determine a necessary change to the function to guarantee an inverse.

Solution. We start with $h(x) = 1 + x$ as it is the easiest. Examples 5.2 and 5.6 demonstrated that $h(x)$ is both injective and surjective, and hence is bijective. By Corollary 5.12, we know there is an inverse function $h^{-1} : \mathbb{R} \to \mathbb{R}$ such that $(h \circ h^{-1})(x) = x$ and $(h^{-1} \circ h)(x) = x$. The reader can easily check that the desired inverse function is $h^{-1}(x) = x - 1$.

Now $f(x) = x^2$ is neither injective nor surjective, so certainly it will have neither a left nor a right-inverse. However, if we make a small change to the codomain of the function then we can arrive a partial answer. If $f : \mathbb{R} \to [0, \infty)$ then we have a right-inverse $r(x) = \sqrt{x}$

$$(f \circ r)(x) = (\sqrt{x})^2 = x, \qquad (r \circ f)(x) = \sqrt{x^2} = |x|.$$

Notice that r still fails to be a left-inverse. If we also change the domain so that $f : [0, \infty) \to [0, \infty)$ then $(r \circ f)(x) = x$ since there are no negative values of x to realize the absolute value. With these changes in place the function f is now invertible.

Finally, the function $g(x) = \frac{1}{x}$ is injective but fails to be surjective, since there is not values of $x \in \mathbb{R} \setminus \{0\}$ such that $g(x) = 0$. This is the only value we miss, so by removing it we have a bijective function, whose inverse is $s(x) = 1/x$.

$$(g \circ s)(x) = \frac{1}{1/x} = x, \qquad (s \circ g)(x) = \frac{1}{1/x} = x.$$ ■

The above example demonstrates how critical the domain and codomain are to the definition of a function. By changing the domain and codomain, one can change whether the function is injective, surjective, or bijective, and hence whether or not it is invertible. In pratice, injectivity is more critical than surjectivity. If $f : A \to B$ in injective, restricting the codomain to the range of f does not result in any loss of information about the function. On the other hand, if f is not injective, we have to restrict the domain to a subset on which the function is injective. This means throwing away information about the function, which is less than ideal.

$f : x \mapsto x^2$

(Co)domain			Injective	Surjective
$\mathbb{R}$	$\longrightarrow$	$\mathbb{R}$	No	No
$[0,\infty)$	$\longrightarrow$	$\mathbb{R}$	Yes	No
$\mathbb{R}$	$\longrightarrow$	$[0,\infty)$	No	Yes
$[0,\infty)$	$\longrightarrow$	$[0,\infty)$	Yes	Yes

Warning

Many students confuse the notion of the function inverse with that of a reciprocal. The reciprocal of a function f is the function $1/f$, and is such that

$$f(x) \times \frac{1}{f(x)} = 1.$$

The inverse of a function is such that $(f \circ f^{-1})(x) = x$. Because this mistake occurs so frequently, we make the message loud and clear:

"The inverse of a function is not the same as the reciprocal of a function."

Proposition 5.15

If $f : B \to C$ and $g : A \to B$ are both bijections, then $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.

Solution. Since inverses are unique, it suffices to show that $g^{-1} \circ f^{-1}$ gives the identity function. Indeed,

$$(f \circ g) \circ (g^{-1} \circ f^{-1}) = f \circ (g \circ g^{-1}) \circ f^{-1} = f \circ \mathrm{id}_B \circ f^{-1} = f \circ f^{-1} = \mathrm{id}_C$$

and similarly

$$(g^{-1} \circ f^{-1}) \circ (f \circ g) = \mathrm{id}_A$$

showing that $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$ as required. ■

5.3 Cardinality

The cardinality of a set S is how many elements are within the set, and is denoted $|S|$. When S is finite, $|S|$ is simple to define; however, the issue becomes trickier when S is an infinite set. For example, we will see that $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}|$, which is surprising given that it *looks* as though $\mathbb{Q}$ is much larger than $\mathbb{N}$.

Consider the following situation: you are given two boxes, let's call them box S and box T. Each box contains an unknown number of rubber balls, and your job is to determine which box contains more balls. One strategy is to reach into both boxes at the same time, withdrawing a single ball from each. If, say, box S runs out of balls before box T, you know that box S contained fewer balls than T. If S and T are sets, we know $|S| < |T|$.

How does this help us in determining the size of sets? Let $f : S \to T$ is a function, thought of as a collection of arrows from S to T. The function f must define exactly $|S|$ arrows, one emanating from each element of S. If $|S| > |T|$ it is possible to define a surjective function $f : S \to T$, but not an injective function. For each object in S we must choose an object in T. Since $|S| > |T|$ we have enough arrows to hit every element in T, giving us a surjective function. On the other hand, the pigeonhole principle tells us that at some point we are going to have to send two elements of S to the same element of T, breaking injectivity.

One can imagine a similar situation if $|S| < |T|$, wherein one can define an injective function from S to T, but not a surjective function. It is this idea for finite sets that allows us to define the notion of cardinality in general.

Definition 5.16

Let S and T be sets. We say $|S| \leq |T|$ if there is an injective function $S \to T$.

For example, if $S = \{1, 2, 3\}$ and $T = \{-3, -6, -9, -12\}$ we could define an injection $f : S \to T$ by $f(s) = -3s$, showing that $|S| \leq |T|$. This agrees with our usual notion of counting, since $|S| = 3$ and $|T| = 4$. However, we can extend this idea to infinite sets. For example, if $S = \{1, 2, 3, \ldots\}$ and $T = \{-1, -2, -3, \ldots\}$ then $|S| \leq |T|$ via the injection $s \mapsto -s$. Of course, in this latter case we expect $|S| = |T|$, but we are not yet able to discuss these things.

Before going any further, let's ground our definition in reality.

Proposition 5.17

If $S = \{s_1, \ldots, s_n\}$ and $T = \{t_1, \ldots, t_m\}$ are finite sets, then $|S| \leq |T|$ if and only if $n \leq m$.

Proof. [$\Leftarrow$] Suppose $n \leq m$ and define a map $f : S \to T$ by $f(s_i) = t_i$. This map makes sense only if $n \leq m$, and moreover it is certainly injective. Hence $|S| \leq |T|$.

[$\Rightarrow$] By contrapositive, suppose $n > m$. Suppose for the sake of contradiction that an injective function $f : S \to T$ exists. The data of f includes n outputs, so by the Pigeonhole principle at least one of these output must be repeated; that is, there exist s_1 and s_2 such that $s_1 \neq s_2$ and $f(s_1) = f(s_2)$, but this contradicts the fact that f is an injection. □

Proposition 5.18

If $S \subseteq T$ then $|S| \leq |T|$.

Proof. Let $\iota : S \to T$ be the inclusion function; that is, $\iota(s) = s$. This function is certainly injective, since if $\iota(s_1) = \iota(s_2)$ then by definition, $s_1 = s_2$. By Definition 5.16, $|S| \leq |T|$. □

The hierarchy of counting thus immediately implies that $|\mathbb{N}| \leq |\mathbb{Z}| \leq |\mathbb{Q}| \leq |\mathbb{R}|$. Similarly, $|[0, 1]| \leq \mathbb{R}$, and any other cardinality relation induced by the subset relation.

One can also use the notion of a surjection to compare cardinalities, as the following example demonstrates:

Proposition 5.19

If S and T are non-empty sets and $f : S \to T$ is a surjection, then $|T| \geq |S|$; that is, there is an injection $g : T \to S$.

Proof. Let $f : S \to T$ be surjective. By Proposition 5.11 we know that f has a right inverse; namely, there is a function $g : T \to S$ such that $f \circ g = \mathrm{id}_T$. The symmetry in this relationship means that f is a left-inverse for g, which by Proposition 5.10 means that g is injective. Hence we have an injective function from T to S, and $|T| \leq |S|$. □

Once again, we immediately get that if $S = \{s_1, \ldots, s_n\}$ and $T = \{t_1, \ldots, t_m\}$ are finite sets, then there is a surjection from S to T if and only if $m \leq n$. This leads us to the following definition:

Definition 5.20

If S and T are sets, then $|S| = |T|$ if there is a bijection $S \to T$.

If $f : S \to T$ is a bijection, it is both surjective and injective, so $|S| \leq |T|$ and $|T| \leq |S|$. Thus it makes sense to define equality of cardinality this way.

Note as well that this relationship is immediately transitive, so that if $|A| = |B|$ and $|B| = |C|$, then $|A| = |B|$. Indeed, there is a bijection $f : A \to B$ and a bijection $g : B \to C$, then $g \circ f : A \to C$ is a bijection.

Example 5.21

Consider the sets

$$2\mathbb{N} = \{0, 2, 4, 6, \ldots\}.$$

Show that $|2\mathbb{N}| = |\mathbb{N}|$.

Solution. Certainly $2\mathbb{N} \subseteq \mathbb{N}$, so that $|2\mathbb{N}| \leq |\mathbb{N}|$, but we have been asked to go one step further. Define the function $f : \mathbb{N} \to 2\mathbb{N}$ by $f(n) = 2n$, which we shall show is a bijection.

To see that it is injective, notice that if $f(n) = f(m)$ then $2n = 2m$. Dividing by 2 gives $n = m$ as required. To see that f is surjective, notice that every positive even number k can be written as $k = 2m$ for some $m \in \mathbb{N}$. Hence $f(m) = 2m = k$ so f is surjective. Since there is a bijection between $\mathbb{N}$ and $2\mathbb{N}$, we conclude that $|\mathbb{N}| = |2\mathbb{N}|$. ■

Example 5.21 demonstrates that, unlike finite sets, infinite sets can have the same cardinality as their subsets. This is just the first surprising statement in a plethora of unintuitive but interesting results. A similar example is the following:

Example 5.22

Show that $|(0, 1)| = |\mathbb{R}|$.

Solution. We need to find a bijective function that maps $(0,1)$ to $\mathbb{R}$, or alternatively an injection from $\mathbb{R} \to (0,1)$. The former is just as easy as the later, once one recognizes that $\arctan : (-\pi/2, \pi/2) \to \mathbb{R}$ is a bijection. By appropriately modifying the arctangent function, we get

$$f : (0,1) \to \mathbb{R}, \qquad t \mapsto \frac{2\arctan(t) + \pi}{2},$$

is the desired bijection. ■

Exercise: Modify Example 5.22 to show that $|(a,b)| = |\mathbb{R}|$ for any $a < b$. What about the closed interval $[a,b]$?

A subtle question at this point is whether knowing $|S| \leq |T|$ and $|T| \leq |S|$ tells us that $|T| = |S|$. Remember, these "inequalities" are just notation – notation that happens to coincide with our usual inequality on $\mathbb{N}$, but we can't say more than that in general.

Let's think about this more. We're asking if knowing that there is an injection $f : S \to T$ ($|S| \leq |T|$) and an injection $g : T \to S$ ($|T| \leq |S|$) guarantees the existence of a bijection from S to T. That's not at all obvious.

Theorem 5.23: Cantor-Bernstein-Schroeder

If $f : A \to B$ and $g : B \to A$ are injective functions, then there is a bijection $h : A \to B$, and hence $|A| = |B|$.

The proof is somewhat involved, and so is omitted. However, it's worth pointing out that this is not immediately obvious, and is difficult to prove.

Example 5.24

Show that $|(0,1)| = |[0,1]|$.

Solution. The inclusion map $\iota : (0,1) \to [0,1], x \mapsto x$ is an injection, so we need only construct an injection in the other direction. Define $f : [0,1] \to [0,1]$ by $f(t) = (1+2t)/4$, and note that $f([0,1]) = [1/4, 3/4]$. This function is injective, for if $f(t_1) = f(t_2)$ then

$$\frac{1+2t_1}{4} = \frac{1+2t_2}{4} \quad \Rightarrow 1 + 2t_1 = 1 + 2t_2 \quad \Rightarrow t_1 = t_2.$$

Thus by the Canotor-Bernstein-Schroeder theorem, there is a bijection between $(0,1)$ and $[0,1]$; hence, $|(0,1)| = |[0,1]$. ■

Definition 5.25

A set S is said to be *countable* if $|S| \leq |\mathbb{N}|$. Equivalently, S is countable if there is an injective function $f : S \hookrightarrow \mathbb{N}$. We say that S is *countably infinite* if $|S| = |\mathbb{N}|$.

Our goal is to show that $\mathbb{Z}$ and $\mathbb{Q}$ are countable, but that $\mathbb{R}$ is not. For the former, we need the following result:

Proposition 5.26

A countable union of (pairwise disjoint) countable sets sets is countable.

Proof. Let $\{A_i\}_{i\in I}$ be a countable collection of countable sets, so I is countable, as is each A_i. Let $g : I \hookrightarrow \mathbb{N}$ be an injective function, and for each A_i let $f_i : A_i \hookrightarrow \mathbb{N}$ be an injective function. Define the map

$$f : \bigcup_{i\in I} A_i \to \mathbb{N}, \qquad a \mapsto 2^{g(n)}3^{f_n(a)}, \qquad a \in A_n.$$

This map is well-defined by the uniqueness of prime decompositions and the fact that the A_n are pairwise disjoint. The same uniqueness condition gives injectivity; that is, the only way $2^n3^m = 2^r3^s$ is if $n = r$ and $m = s$. Thus a countable union of countable sets is countable. □

Theorem 5.27

The integers are the same size as the natural numbers: $|\mathbb{Z}| = |\mathbb{N}|$.

Proof. Note that

$$\mathbb{N}\times\mathbb{N} = \{(n,m) : n,m\in\mathbb{N}\} = \bigcup_{n\in\mathbb{N}} \{n\}\times\mathbb{N}$$

is a countable union of countable sets, and hence is countable itself by Proposition 5.26. Define the map $f : \mathbb{Z} \to \mathbb{N}\times\mathbb{N}$ as $n \mapsto (|n|, \operatorname{sgn}(n))$. As an example of what this map does, we have

$$\begin{array}{cc} -5 \mapsto (5,-1) & 5 \mapsto (5,1) \\ -4 \mapsto (4,-1) & 4 \mapsto (4,1) \\ -3 \mapsto (3,-1) & 3 \mapsto (3,1) \\ -2 \mapsto (2,-1) & 2 \mapsto (2,1) \\ -1 \mapsto (1,-1) & 1 \mapsto (1,1) \\ \multicolumn{2}{c}{0 \mapsto (0,0)} \end{array}$$

so that the second number just keeps track of whether the number is positive, negative, or zero. This map is injective, since if $f(n) = f(m)$ then $(|n|, \operatorname{sgn}(n)) = (|m|, \operatorname{sgn}(m))$. Equality in the first component, $|n| = |m|$, implies that $n = \pm m$. Equality in the second component, $\operatorname{sgn}(n) = \operatorname{sgn}(m)$, implies that that $n = m$.

Since f is injective, we thus have that $|\mathbb{Z}| \le |\mathbb{N}\times\mathbb{N}| \le |\mathbb{N}|$. On the other hand, since $\mathbb{N} \subseteq \mathbb{Z}$ it must be that $|\mathbb{N}| \le |\mathbb{Z}|$. Both inclusions give us that $|\mathbb{N}| = |\mathbb{Z}|$. □

Theorem 5.28

The rational numbers are countably infinite: $|\mathbb{Q}| = |\mathbb{N}|$.

Proof. Consider the map $f : \mathbb{Q} \to \mathbb{Z}\times\mathbb{N}$ given by $f(p/q) = (p,q)$ where the fraction p/q is in lowest terms (if the fraction is negative, we always take the sign in the p-component). Again this map is injective, since if $f(p/q) = f(r/s)$ then $(p,q) = (r,s)$ which is true only if $p = r$ and $q = s$. Since $\mathbb{Z}$

and $\mathbb{N}$ are both countable, so too is $\mathbb{Z} \times \mathbb{N}$ and so $|\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{N}| \leq |\mathbb{N}|$. On the other hand, $\mathbb{N} \subseteq \mathbb{Q}$ so $|\mathbb{N}| \leq |\mathbb{Q}|$ and this gives us that $|\mathbb{Q}| = |\mathbb{N}|$. □

One might expect that this pattern continues forever, and that every infinite set has the same cardinality as the naturals. The real numbers are our first counterexample.

Theorem 5.29

The real numbers are *strictly larger* than the natural numbers, and so not countable: $|\mathbb{R}| > |\mathbb{N}|$.

Proof. It is sufficient to show that the real numbers $[0, 1]$ are not countable, since then certainly all of $\mathbb{R}$ will be uncountable also. For the sake of contradiction, assume that the real numbers are countable and list them $\{r_1, r_2, r_3, \ldots\}$. Write each r_i in its decimal expansion as $r_i = 0.d_1^i d_2^i d_3^i d_4^i \cdots$ so that

$$\begin{aligned} r_1 &= 0.d_1^1\ d_2^1\ d_3^1\ d_4^1 \cdots \\ r_2 &= 0.d_1^2\ d_2^2\ d_3^2\ d_4^2 \cdots \\ r_3 &= 0.d_1^3\ d_2^3\ d_3^3\ d_4^3 \cdots \\ r_4 &= 0.d_1^4\ d_2^4\ d_3^4\ d_4^4 \cdots \\ &\vdots \end{aligned}$$

Define a new number s as follows. Let $s = 0.s_1\ s_2\ s_3\ s_4 \cdots$ where

$$s_i = \begin{cases} 0 & \text{if } d_i^i = 1 \\ 1 & \text{if } d_i^i \neq 1 \end{cases}.$$

The number s_i is not in the list $\{r_1, r_2, r_3, \ldots\}$ by construction (think about this and you will see it is true), but is a real number. This is a contradiction, since we assumed that we listed all of the real numbers. We conclude that the real numbers are not countable as required. □

So what goes wrong with the reals? The problem is that, given a fixed real number. There is no reasonable way to say what the "next" real number is. In the case of $\mathbb{N}$ and $\mathbb{Z}$ it is easy, and in this case of $\mathbb{Q}$ it is a bit tricky but still doable. But lets say you start at the real number 0. What is the next real number? 0.1? Why not 0.01 or 0.001 or 0.0001? I can put an arbitrary number of zeroes before putting that 1, so it does not make sense to say "the next real number." This is precisely what breaks.

So is there a cardinal strictly between $|\mathbb{N}|$ and $|\mathbb{R}|$? This turns out to be an incredibly deep and subtle question, and one that cannot be proven with our standard set of axioms. One must either *assume* that there is such a cardinal, or *assume* there is no such cardinal, it cannot be proven either way. However, there is a systematic way of taking a set, and getting a set with a strictly larger cardinality.

Definition 5.30

Let S be a set, and define the power set $\mathcal{P}(S)$ to be the set of all subsets of S. The power set is sometimes denoted 2^S.

Theorem 5.31: Cantor's Theorem

If S is a set, then $|S| < |\mathcal{P}(S)|$.

Proof. First we show that $|S| \leq |\mathcal{P}(S)|$ by demonstrating an injection $S \to \mathcal{P}(S)$. Define the function $f : S \to \mathcal{P}(S)$ by $x \mapsto \{x\}$. This map is evidently injective.

The remainder of the proof is a generalization of the proof given in Theorem 5.29, and proceeds by diagonalization. Assume that a surjective $f : S \to \mathcal{P}(S)$ exists and define the set

$$D = \{x \in S : x \notin f(x)\} \in \mathcal{P}(S).$$

We claim D is not the image of any point in S. Indeed, for each element $a \in S$, either $a \in f(a)$ or $a \notin f(a)$. In the first case, if $a \in f(a)$ then $a \notin D$, so $f(a) \neq D$. On the other hand, if $a \notin f(a)$ then $a \in D$, again showing that $D \neq f(a)$. Thus D is not the image of any point, contradicting the assumption that f was a surjection. We conclude that $|S| < |\mathcal{P}(S)|$. □

There is no greatest cardinal, since we can keep taking power sets to create a hierarchy of cardinals. This leads to an interesting paradox: The set of all sets is its own power set, so must have cardinality strictly greater than itself. This is resolved by declaring that the set of all sets is not a set, but rather a *proper class*. Proper classes are strictly larger than sets, and therefore do not have the same restrictions as sets.

6 Divisibility and Modular Arithmetic

6.1 Divisibility and Primes

We introduced the basics of divisibility in Definition 3.26. This section will focus on this topic, and other number theoretical ideas.

Recall that if $a, b \in \mathbb{Z}$ we say that $a|b$ if there exists as $k \in \mathbb{Z}$ such that $ak = b$. You can think of a as being a factor of b. Furthermore, we've already proven several useful facts, which we recount below:

1. [Proposition 3.27] If $a|b$ and $a|c$ then for any $m, n \in \mathbb{Z}$, $a|(mb + nc)$.
2. [Proposition 3.28] If $a|b$ and $a|(b + c)$ then $a|c$.
3. [Proposition 3.29] Every integer can be written as the product of primes.
4. [Theorem 3.30] There are infinitely many prime numbers.

Definition 6.1

If $a, b \in \mathbb{Z}$, we define the *greatest common divisor* of a and b, written $\gcd(a, b)$, to be the largest positive integer that divides both a and b. More precisely,

$$\gcd(a, b) = \max\{d \in \mathbb{Z} : d > 0 \text{ and } d|a \text{ and } d|b\}.$$

For example,

$$\gcd(4,6)=2, \qquad \gcd(15,25)=5, \qquad \gcd(15,33)=3, \qquad \gcd(17,4)=1.$$

Note that since every number divides 0, $\gcd(a,0)=|a|$.

If p is a prime number, then $\gcd(p,a)=1$ unless a is a multiple of p. A somewhat more interesting notion is that of coprimality:

Definition 6.2

If $a,b\in\mathbb{Z}$, we say that a and b are *coprime* or *relatively prime* if $\gcd(a,b)=1$.

Theorem 6.3

If $a,b\in\mathbb{Z}$ and $\gcd(a,b)=d$, then there exist $m,n\in\mathbb{Z}$ such that $ma+nb=d$.

We do not yet have the tools to prove Theorem 6.3, but the result is sufficiently worthwhile now for perspective. In some cases, the m,n guaranteed by the theorem are simple to see. For example,

- $\gcd(17,4)=1$, and $17(1)+(4)(-4)=1$,
- $\gcd(15,25)=5$ and $15(-3)+25(2)=5$,
- $\gcd(15,33)=3$ and $15(-2)+33(1)=3$.

These were easy enough to do by inspection, but what if we are asked to find $\gcd(1053,481)$? Can you see this by simple inspection? The answer is 13, but is there a systematic way of deducing this answer? Furthermore, how do we find the m,n guaranteed by Theorem 6.3? Here the answer is

$$13=481(46)+1053(-21)$$

but there is no way we can see that just by inspection! These are some of the answers we will eventually answer.

6.1.1 Prime Divisibility and its Implications

Number theory really is the study of primes, and those prime numbers have special properties when it comes to divisibility.

Proposition 6.4

If $a|bc$ and $\gcd(a,b)=1$ then $a|c$.

Solution. Since $a|bc$ we know there is a $k\in\mathbb{Z}$ such that $ak=bc$. Furthermore, Theorem 6.3 we know that there exist $m,n\in\mathbb{Z}$ such that $am+bn=1$, since we assumed that $\gcd(a,b)=1$. Multiplying through by c we get

$$c=amc+bcn=amc+(ak)c=a(mc+kc)$$

showing that $a|c$. ■

Theorem 6.5

A number $p \in \mathbb{Z}$ is prime if and only if whenever $p|ab$ then $p|a$ or $p|b$.

Proof. ($\Rightarrow$) Assume that p is prime and that $p|ab$. If $p|a$ we are done, so assume that p does not divide a, in which case $\gcd(a,p) = 1$. By Theorem 6.4, it then follows that $p|b$.

($\Leftarrow$) Conversely, we will proceed by the contrapositive; that is, we will show that if p is not prime, then there exists a, b such that $p|ab$ but neither $p|a$ nor $p|b$. Assume that p is not a prime, so it is necessarily composite. We can thus write $p = rs$ for $1 < r \leq s < p$. Hence $p|rs$ but p divides neither r nor s, □

This fact is equivalent to being a prime number, and is in fact the definition of prime in higher mathematics. It is a straightforward induction proof to show that if $p|a_1 a_2 \cdots a_n$ then $p|a_i$ for some $i \in \{1, \ldots, n\}$.

In fact, we have used this divisibility fact before, but not in an obvious way. Recall in Example 3.15 we showed that "n is even if and only if n^2 is even." Since 2 is a prime number, and being divisible by 2 is equivalent to being even, this is the statement that "$2|n$ if and only if $2|n^2$." This generalizes:

Proposition 6.6

If $n \in \mathbb{Z}$ and p is prime, then $p|n$ if and only if $p|n^2$.

Proof. ($\Rightarrow$) Suppose that $p|n$ so that $pk = n$ for some $k \in \mathbb{Z}$. Squaring n we get $n^2 = p^2k^2 = p(pk^2)$ so $p|n^2$.

($\Leftarrow$) Converse, suppose that $p|n^2$. Since p is a prime, Theorem 6.5 shows that $p|n$. □

We used the fact that n is even if and only if n^2 is even to show that $\sqrt{2}$ is irrational. The same proof now applies to show that $\sqrt{p}$ is irrational for any prime p.

Theorem 6.7

If p is a prime, then $\sqrt{p}$ is irrational.

Proof. For the sake of contradiction, assume that p is rational, and write $p = a/b$ where $\gcd(a,b) = 1$; that is, a/b is in lowest terms. Multiplying both sides by b and squaring gives $b^2p = a^2$. Certainly $p|b^2p$ and so $p|a^2$, which in turn implies that $p|a$. Hence we can write $a = pk$ for some $k \in \mathbb{Z}$. Substituting this into $b^2p = a^2$ gives

$$b^2p = p^2k^2 \quad \Rightarrow \quad b^2 = pk^2.$$

Once again $p|pk^2$ so $p|b^2$, showing that $p|b$, hence $b = p\ell$ for some $\ell \in \mathbb{Z}$. This is a contradiction, since

$$1 = \gcd(a,b) = \gcd(pk, p\ell)$$

and the right hand side *at least* p. Thus $\sqrt{p}$ is irrational. □

Theorem 6.8: The Fundamental Theorem of Arithmetic

Every positive integer greater than 1 can be uniquely expressed as a product of primes.

Proof. We have already shown that every number can be written as a product of primes, so it only remains to show that this decomposition is unique. For the sake of contradiction, assume that there exists some integer $n > 1$ which can be expressed with two different prime factorizations, say

$$n = p_1 \cdots p_n = q_1 \cdots q_m,$$

where all the p_i and q_j are prime. Since $p_1 | n$, it must also be the case that $p_1 | q_1 \cdots q_m$. Since p_1 is a prime, by Theorem 6.5 we must have $p_1 | q_j$ for some j. By reordering if necessary, let this be q_1. Since q_1 is also prime, the only way $p_1 | q_1$ is if $p_1 = q_1$. Cancelling p_1 and q_1 thus gives

$$p_2 p_3 \cdots p_n = q_2 q_3 \cdots q_m.$$

We repeat the same argument above, deducing that $p_2 = q_2$, $p_3 = q_3$, and generally that $p_i = q_i$. Hence $n = m$ and, up to reordering the factors, the prime decomposition is unique. □

Example 6.9

The number $\log_{36}(105)$ is irrational.

Solution. For the sake of contradiction, assume $\log_{36}(105) = p/q$ where $\gcd(p, q) = 1$.By definition of the logarithm, $36^{p/q} = 105$, or equivalently $36^p = 105^q$. Factoring 36 and 105 into primes gives

$$(2^2 \cdot 3^2)p = (3 \cdot 5 \cdot 7)^q \quad \Rightarrow \quad 2^{2p} 3^{2p} = 3^q 5^q 7^q.$$

By the Fundamental Theorem of Arithmetic, it must be the case that $2p = 0, 2p = q, q = 0$, for which the only solution is $p = q = 0$. However, the number $0/0$ is not rational, so this is a contradiction. ■

6.2 The Euclidean Algorithm

We now develop an algorithm for determining the greatest common divisor of two numbers, together with the integer linear combination that achieves that number.

Proposition 6.10: The Division Algorithm

If $a, b \in \mathbb{Z}$ with $b > 0$, there exists unique q and r such that $a = qb + r$ where $0 \leq r < b$.

Proof. Assume that both $a, b > 0$, for which the case when $a < 0$ follows similarly. We proceed by strong induction. As a base case, note that when $a = 1$ then

$$a = \begin{cases} b \cdot 0 + 1 & \text{if } b > 1 \\ b \cdot 1 + 0 & \text{if } b = 1, \end{cases}$$

so the base case holds. Assume then that for all $1 \leq n \leq a$, we can write $n = bq + r$ for some unique q and r, and consider $a + 1$. If $a + 1 \leq b$ then the result is trivial, so assume that $a + 1 > b$. Now $(a + 1 - b) \leq a$ so by the induction hypothesis

$$a + 1 - b = bq + r$$

for some unique q and r, so $a + 1 = b(q + 1) + r$. It must also be the case that $q + 1$ and r are unique, for otherwise q and r would not be unique. □

Proposition 6.11

If $a, b, q, r \in \mathbb{Z}$ satisfy $a = qb + r$ then $\gcd(a, b) = \gcd(b, r)$.

Proof. Write $r = a - qb$. If $a = b = 0$ the necessarily $q = r = 0$ and so the result is trivially true. Therefore, assume that not both of a and b are zero, and set $d = \gcd(a, b)$. Since $d|a$ and $d|b$ then $d|(a - qb) = r$ by Proposition 3.27. Now we must show that d is in fact the greatest common divisor or r and b.

If c is any other divisor of b and r, then by Proposition 3.27 we have $c|(bq + r) = a$. Since d is the greatest common divisor of a and b, it must be the case that $c \leq d$, showing that d is the greatest common divisor of b and r as required. □

Theorem 6.12: The Euclidean Algorithm

Let $a, b \in \mathbb{Z}$ with $b \neq 0$ and assume that b does not divide a. Consider the following algorithm:

$$\begin{aligned}
a &= q_1\underline{b} + \underline{r_1}, && \text{where } 0 < r_1 < |b| \\
b &= q_2\underline{r_1} + \underline{r_2}, && \text{where } 0 < r_2 < r_1 \\
r_1 &= q_3\underline{r_2} + \underline{r_3}, && \text{where } 0 < r_3 < r_2 \\
&\vdots \\
r_{n-2} &= q_n\underline{r_{n-1}} + \mathbf{r_n}, && \text{where } 0 < r_n < r_{-1} \\
r_{n-1} &= q_{n+1}r_n + 0.
\end{aligned}$$

This algorithm must terminate in finitely many steps, and moreover $\gcd(a, b) = r_n$.

Proof. The remainders form a strictly decreasing sequence of positive integers: $a \geq b > r_1 > r_2 > r_3 > \cdots$ and so must eventually reach zero, showing that the algorithm must eventually terminate. Furthermore, by repeatedly applying Proposition 6.11 we get

$$\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \gcd(r_2, r_3) \cdots = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n.$$ □

Example 6.13

Find the greatest common divisor of 504 and 1155.

Solution. Proceeding with our Euclidean algorithm, we have

$$\begin{aligned} 1155 &= 504(2) + 147 \\ 504 &= 147(3) + 63 \\ 147 &= 63(2) + \mathbf{21} \\ 63 &= 21(3) + 0 \end{aligned}$$

By the Euclidean algorithm, it must then be the case that $\gcd(1155, 504) = 21$. ■

Another trick to finding the greatest common divisor of two numbers is to use their prime factorizations. Let $a, b \in \mathbb{Z}$ and, allowing powers to be zero if necessary, write a and b with the same primes

$$a = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}, \qquad b = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}.$$

The greatest common divisor of a and b must therefore be

$$d = \gcd(a, b) = p_1^{\min\{n_1, m_1\}} p_1^{\min\{n_2, m_2\}} \cdots p_k^{\min\{n_k, m_k\}}.$$

Example 6.14

Find the greatest common divisor of 2^{100} and 100^2.

Solution. The prime factorization of 2^{100} is just 2^{100}, while for 100^2 we get

$$100^2 = (2^2 \cdot 5^2)^2 = 2^4 \cdot 5^4.$$

The greatest common divisor is thus

$$d = \gcd(2^{100}, 100^2) = 2^{\min\{4,100\}} 5^{\min\{0,4\}} = 2^4 = 16.$$ ■

6.3 Linear Diophantine Equations

Definition 6.15

Given $a, b, d \in \mathbb{Z}$, a Linear Diophantine Equation (in two variables) is any equation of the form

$$ax + by = d.$$

Certainly there are rational solutions to this equation, but we are more interested in finding integer solutions.

Theorem 6.16

If $a, b, c \in \mathbb{Z}$, then $ax + by = c$ has a solution if and only if $\gcd(a, b) | c$.

Proof. In both proofs, let $d = \gcd(a, b)$.

($\Rightarrow$) Suppose that the equation has a solution, say x_0 and y_0, so that $ax_0 + by_0 = c$. Necessarily, $d|a$ and $d|b$ so $d|(ax_0 + by_0) = c$

($\Leftarrow$) Suppose that $d|c$ so that $dk = c$ for some $k \in \mathbb{Z}$. Applying the Euclidean algorithm to a and b there is a sequence

$$\begin{aligned} a &= q_1\underline{b} + \underline{r_1}, \\ b &= q_2\underline{r_1} + \underline{r_2}, \\ r_1 &= q_3\underline{r_2} + \underline{r_3}, \\ &\vdots \\ r_{n-2} &= q_n\underline{r_{n-1}} + d, \end{aligned}$$

Working back up through these equations, allows us to write d in terms of a and b, so there is an x_0, y_0 such that $ax_0 + by_0 = d$. Multiplying through by k we get

$$a(kx_0) + b(ky_0) = dk = c$$

as required. □

Example 6.17

In Example 6.13 we showed that $\gcd(504, 1155) = 21$. Find a solution to the Diophantine equation $504x + 1155y = 42$.

Solution. Since $\gcd(504, 1155) = 21|42$ we know that a solution exists. We found in Example 6.13 that

$$\begin{aligned} 1155 &= 504(2) + 147 \\ 504 &= 147(3) + 63 \\ 147 &= 63(2) + 21 \end{aligned}$$

Write the last line as $21 = 147 + 63(-2)$. We now solve each remaining equation for the remainder to find $63 = 504 + 147(-3)$ and $147 = 1155 + 504(-2)$. Substituting these we get

$$\begin{aligned} 21 &= 147 + 63(-2) \\ &= 147 + [504 + 147(-3)](-2) && \text{from } 63 = 504 + 147(-3) \\ &= 147(7) + 504(-2) \\ &= [1155 + 504(-2)](7) + 504(-2) && \text{from } 147 = 1155 + 504(-2) \\ &= 1155(7) + 504(-16). \end{aligned}$$

This is not the desired solution though, so we multiply through by 2 to get

$$504(-32) + 1155(14) = 42$$

as required. ■

There are in fact infinitely many solutions to a solvable Diophantine equation. How do we find them in general?

Proposition 6.18

Suppose that $a, b, c \in \mathbb{Z}$ and (x_0, y_0) satisfy $ax_0 + by_0 = c$. If $d = \gcd(a, b) \neq 0$ then the general solution to the Diophantine equation $ax + by = c$ is given by

$$x = x_0 + n\frac{b}{d}, \qquad y = y_0 - n\frac{a}{d}, \qquad \text{for all } n \in \mathbb{Z}.$$

Note that it does not matter whether you put the minus sign in the x term or the y term, so long as they are opposiing signs.

Proof. Subtract the equations $ax_0 + by_0 = c$ and $ax + by = c$ to find that $a(x - x_0) + b(y - y_0) = 0$. Divide through by d and re-arrange to find that

$$\frac{a}{d}(x - x_0) = -\frac{b}{d}(y - y_0).$$

The student can show that $\gcd(a/d, b/d) = 1$ (Good exercise!). Moreover, a/d divides the left hand side, and so must also divide the right hand side. Since $\gcd(a/d, b/d) = 1$, then by Proposition 6.4 we know that $(a/d)|(y - y_0)$. Similarly, $(b/d)|(x - x_0)$, so there exists $n \in integ$ such that $x - x_0 = n(b/d)$ so that

$$-\frac{b}{d}(y - y_0) = \frac{a}{d}(x - x_0) = n\frac{a}{d}\frac{b}{d} \qquad \Rightarrow bd(y_0 - y) = anb$$

In both cases, we can solve for x and y to find that

$$x = x_0 + n\frac{b}{d}, \qquad y = y_0 - n\frac{a}{d}.$$

Now in fact every such n works, since

$$ax + by = a\left(x_0 + n\frac{b}{d}\right) + b\left(y_0 - n\frac{a}{d}\right) = (ax_0 + by_0) + \left(\frac{anb}{d} - \frac{anb}{d}\right) = ax_0 + by_0 = c. \qquad \square$$

Example 6.19

Find the general solutions to $504x + 1155y = 42$.

Solution. We have already found a particular solution; namely, $504(-32) + 1155(14) = 42$. Furthermore, $d = \gcd(504, 1155) = 21$ and so the general solutions are of the form

$$x = -32 + n\frac{1155}{21} = -32 + 55n, \qquad y = 14 - n\frac{504}{21} = 14 - 24n. \qquad \blacksquare$$

It is sometimes easier to normalize by the greatest common denominator before starting. Take our carry-through example, where we want to solve $504x + 1155y = 42$. Dividing through by the greatest common divisor $d = \gcd(504, 1155) = 21$ we get the equation

$$24x + 55y = 2.$$

Since $\gcd(24, 55) = 1$ we can find a solutions to $24x + 55y = 1$, then multiply by 2. To do this, we again use the Euclidean algorithm to find

$$\begin{aligned} 55 &= 24(2) + 7 \\ 24 &= 7(3) + 3 \\ 7 &= 3(2) + 1 \\ 3 &= 3(1) + 0 \end{aligned}$$

(where of course we already knew the greatest common divisor is 1). Now working backwards

$$\begin{aligned} 1 &= 7 + 3(-2) \\ &= 7 + [24 + 7(-3)](-2) \\ &= 7(7) + 24(-2) \\ &= [55 + 24(-2)](7) + 24(-2) \\ &= 55(7) + 24(-16). \end{aligned}$$

Multiplying by 2 gives us our solution $24(-32) + 55(14) = 2$. Notice that $(-32, 14)$ are the same as the solutions we found above, as should be the case. Moreover, the general solutions are easily read off as $x = -32 + 55n$ and $y = 14 - 24n$, which is again the same solution we found above.

Example 6.20

Find all non-negative solutions to $504x + 1155y = 42$, if they exist.

Solution. We know that the general solutions are of the form $x = -32 + 55n$ and $y = 14 - 24n$. We require both numbers to be positive, giving $-32 + 55n > 0$ and $14 - 24n > 0$, which we can solve for n to get

$$\frac{32}{55} < n < \frac{14}{24}.$$

There are no integers which satisfy this equation, so there are no non-negative solution. ■

6.4 Relations on Sets

Given a set S, a *relation* on S is a way of comparing two elements of the set, or rather, specifying their relationship. For example, equality is a relation, for when we write $a = b$ we are specifying a relationship between a and b. Similarly, $a < b$ is a relation. Abstractly, if $a, b \in S$ we write the relation as aRb or $R(a, b)$. This describes a heuristic, but is not a formal definition, which is the following:

Definition 6.21

Given a set S, a *relation on S* is any subset of $S_R \subseteq S \times S$.

This seems pretty nebulous, but the subset precisely captures when elements are related. For example, if $S = \mathbb{Z}$ and $R =<$ then $S_R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : a < b\}$. Here we see that $(-2, 5) \in S_R$ since $-2 < 5$, while $(15, 14) \notin S_R$ since $15 \not< 14$.

Given a relation R as in the first paragraph, we can define the set S_R as follows: Define a function $r : S \times S \to \{0,1\}$ such that

$$r(a,b) = \begin{cases} 1 & aRb \\ 0 & \text{otherwise} \end{cases}$$

and set $S_R = r^{-1}(1)$. Conversely, given a set S_R we say aRb if $(a,b) \in S_R$.

To distinguish between different types of relations, we define properties that the relation can exhibit. If R is a relation on S then

- R is *reflexive* if for all a, aRa,
- R is *transitive* if whenever aRb and bRc then aRc,
- R is *symmetric* if whenever aRb then bRa,
- R is *anti-symmetric* if whenever aRb and bRa then $a = b$,
- R is *total* if for all a and b either aRb or bRa.

For example, equality $a = b$ is reflexive ($a = a$ is always true), transitive (if $a = b$ and $b = c$ then $a = c$), and symmetric (when $a = b$ then $b = a$), but not total. On the other hand, inequality $a \leq b$ is reflexive ($a \leq a$ is always true), transitive (if $a \leq b$ and $b \leq c$ then $a \leq c$), anti-symmetric ($a \leq b$ and $b \leq a$ implies $a = b$), and total (either $a \leq b$ or $b \leq a$).

Definition 6.22

An relation R on a set S is said to be an *equivalence relation* if R is reflexive, transitive, and symmetric. It is said to be an *order relation* if R is reflexive, transitive, and anti-symmetric.

Example 6.23

Let X be a set, and define a relation on the power set $\mathcal{P}(X)$ by subset inclusion; namely ARB if $A \subseteq B$. Determine which of the five previous properties are satisfied by this relation.

Solution. This relation is reflexive, since $A \subseteq A$ is always true. It is transitive, since if $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$. Finally, it is also anti-symmetric, for if $A \subseteq B$ and $B \subseteq A$ then $A = B$. Hence subset inclusion is a order relation.

However, notice that inclusion is *not* total. Given two arbitrary subsets $A, B \in X$, there need not be a relation on them. It could be the case that $A \subseteq B$ or $B \subseteq A$, but in general neither need be true. We say that subset inclusion is a *partial ordering*. ■

Example 6.24

Show that divisibility on $\mathbb{N}$ is a partial order relation, though not on $\mathbb{Z}$.

Solution. We need to check that divisibility is transitive, reflexive, and anti-symmetric, but non-total. Being reflexive is immediate, since $a|a$ for all $a \in \mathbb{Z}$. Transitivity is true, for we have shown that if $a|b$ and $b|c$ then $a|c$.

Anti-symmetry requires a bit of work, but isn't too bad. Assume that $a|b$ and $b|a$. If either is zero then the relation $x|0$ can only be true if $x = 0$, so $a = b$. Thus assume that neither a nor b is zero, so there exist $k, \ell \in \mathbb{N}$ such that $ak = b$ and $b\ell = a$. Multiplying the first equation by ℓ we get

$$ak\ell = b\ell = a \quad \Rightarrow \quad a(k\ell - 1) = 0$$

Since $a \neq 0$ we must have $k\ell = 1$ which implies that $k = \ell = \pm 1$. Since $k, \ell \in \mathbb{N}$, it must be that $k = \ell = 1$ so $a = b$. On the other hand, notice that if we are taking divisibility in $\mathbb{Z}$, then $k = \ell = -1$ is also a possibility, showing that $a = -b$. ■

Example 6.25

Let $S = \mathbb{R}$ and let $f : \mathbb{R} \to \mathbb{R}$ be any function. Define a relation on $\mathbb{R}$ by saying that $a \cong b$ if $f(a) = f(b)$. Show that $\cong$ is an equivalence relation.

Solution. We need to show that $\cong$ is reflexive, transitive, and symmetric.

- [Reflexive] Let $a \in \mathbb{R}$. Since functions have unique outputs, $f(a) = f(a)$ showing that $a \cong a$.
- [Transitive] Assume that $a \cong b$ and $b \cong c$, so that $f(a) = f(b)$ and $f(b) = f(c)$. But then $f(a) = f(b) = f(c)$, so $a \cong c$.
- [Symmetric] If $a \cong c$ then $f(a) = f(c)$, or equivalently $f(c) = f(a)$, showing that $c \cong a$. ■

Definition 6.26

Given an equivalence relation $\cong$ on a set S, the *equivalence class* of an element $a \in S$ is the set

$$[a] = \{x \in S : x \cong a\}.$$

If $\sim$ is an equivalence class on S, the set of equivalence classes in S is sometimes denoted $S/\sim$.

Example 6.27

Define an equivalence relation on $\mathbb{R}$ by saying that $a \sim b$ if $a - b \in \mathbb{Z}$. What do elements of an equivalence class look like?

Solution. Let's start with a simple example, and look at the equivalence class $[0]$. By definition,

$$[0] = \{x \in \mathbb{R} : x \sim 0\} = \{x \in \mathbb{R} : x - 0 \in \mathbb{Z}\} = \mathbb{Z}$$

so the equivalence class of $[0]$ is precisely the integers. What about something like $[1.5]$?

$$[1.5] = \{x \in \mathbb{R} : x \sim 1.5\} = \{x \in \mathbb{R} : x - 1.5 \in \mathbb{Z}\}$$

So when will $x - 1.5$ look like an integer? Precisely when x the decimal part of x is 0.5; for example, $4.5 - 1.5 \in \mathbb{Z}$ and $-2.5 - 1.5 \in \mathbb{Z}$.

In general, equivalence classes $[x]$ are the all those real numbers that have the same decimal component as x. ■

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

Theorem 6.28

If $\sim$ is an equivalence relation on S, then $\sim$ partitions S into disjoint equivalence classes; that is, every element $x \in S$ belongs to a unique equivalence class.

Solution. Certainly every element belongs to an equivalence class, so we need only show that two disjoint equivalent classes have no intersection. Let $[x]$ and $[y]$ be disjoint equivalence classes, and for the sake of contradiction assume that $[x] \cap [y] \neq \emptyset$. Choose $z \in [x] \cap [y]$, so that $z \sim x$ and $z \sim y$. By transitivity, $x \sim y$, which contradicts the fact that these were disjoint equivalence classes. We conclude that all equivalence classes are disjoint. ■

6.5 Modular Arithmetic

Definition 6.29

If $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$, we say that $a \equiv b \pmod{n}$ (read: a is congruent to b mod n) if $n|(b-a)$.

For example, if $n = 4$ then $1 \equiv 29 \pmod 4$, since $4|(29-1) = 28$. The congruence classes are precisely

$$\begin{aligned}
[0] &= \{\ldots, -12, -8, -4, 0, 4, 8, 12, \ldots\} \\
[1] &= \{\ldots, -11, -7, -3, 1, 5, 9, 13, \ldots\} \\
[2] &= \{\ldots, -10, -6, -2, 2, 6, 10, 14, \ldots\} \\
[3] &= \{\ldots, -9, -6, -1, 3, 7, 11, 15, \ldots\}
\end{aligned}$$

Proposition 6.30

Congruence mod n is an equivalence relation.

Proof. We need to show that congruence is reflexive, transitive, and symmetric.

- [Reflexive] Fix an $a \in \mathbb{Z}$. Note that $a - a = 0$ and $n|0$, so $a \cong a \pmod{n}$.
- [Transitive] Suppose that $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, or equivalently $n|(b-a)$ and $n|(c-b)$. Now
$$(c-a) = (c - b + b - a) = (c-b) + (b-a)$$

and since n divides each of above terms, by Proposition 3.27, we know it divides the sum as well. Thus $n|(c-a)$, or $a \equiv c \pmod n$.

- [Symmetric] Suppose that $a \equiv b \pmod n$, so that $n|(b-a)$. Then $n|(a-b) = -(b-a)$, so $b \equiv a \pmod n$ as required. □

Proposition 6.31

Fix an $n \in \mathbb{N}$. If $a \equiv r \pmod n$ and $b \equiv s \pmod n$ then

1. $(a+b) \equiv (r+s) \pmod n$.
2. $ab \equiv rs \pmod n$

Proof. Fix a, b, r, s and assume that $a \equiv r \pmod n$ and $b \equiv s \pmod n$. Hence $n|(r-a)$ and $n|(s-b)$. Equivalently, there exist k, ℓ such that $nk = r - a$ and $n\ell = s - b$.

1. Summing together our two equation above, we get

$$n(k+\ell) = (r+s) - (a+b)$$

so $n|[(r+s)-(a+b)]$ or equivalently, $(a+b) \equiv (r+s) \pmod n$

2. We can write

$$rs - ab = rs - rb + rb - ab = r(s-b) + (r-a)b = n\ell r + nkb = n(\ell r + kb)$$

so $n|(rs-ab)$ or equivalently, $ab \equiv rs \pmod n$. □

For a fixed $n \in \mathbb{N}$ we define the *congruence class* of $a \in \mathbb{Z}$ to be the equivalence class

$$[a] = \{x \in \mathbb{Z} : x \equiv a \pmod n\},$$

of which there precisely n; namely $[0], [1], [2], \ldots, [n-1]$. We often denote this set of equivalence classes by

$$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{[0]_n, [1]_n, \ldots, [n-1]_n\}.$$

According to Proposition 6.31, we can add and multiply congruence classes exactly as we would integers, as long as we reduce modulo n. So for example, working modulo 3 we have

$$[3]_4 + [2]_4 = [5]_4 = [1]_4, \qquad [3]_4 \cdot [2]_4 = [6]_4 = [2]_4.$$

Exercise: Show that $\mathbb{Z}/p\mathbb{Z}$ is a field if and only if p is a prime.

Example 6.32

What is the last digit in 4^{441}?

Solution. Note that the last digit d satisfies $d \equiv 4^{441} \pmod{10}$. Moreover,

$$4^{441} = (4^3)^{147} = (64)^{147} \equiv 4^{147} \pmod{10}.$$

The same trick again gives

$$4^{147} = 64^{49} \equiv 4^{49} \pmod{10}.$$

Here we need to be a bit more clever. Rather than try to decompose this into $49 = 7 \cdot 7$, lets write $49 = 1 + 48$ so that

$$\begin{aligned}
4^{49} &= 4 \cdot 4^{48} = 4 \cdot (64)^{12} \equiv 4 \cdot 4^{16} \pmod{10} \\
&\equiv 4 \cdot (256)^4 \pmod{10} \equiv 4 \cdot 6^4 \pmod{10} \\
&\equiv 4 \cdot (36)^2 \pmod{10} \equiv 4 \cdot \cdot 6 \pmod{10} \\
&\equiv 4 \pmod{10}.
\end{aligned}$$

Hence the last digit of 4^{441} is 4. ■

Example 6.33

Show that if $a^2 - 2$ is not divisible by 7, then $a - 4$ is not divisible by 7.

Solution. By contrapositive, assume that $a - 4$ is divisible by 7; that is, $a \equiv 4 \pmod{7}$. Then

$$a^2 \equiv 16 \mod 7 \equiv 2 \mod 7 \quad \Rightarrow \quad a^2 - 2 \equiv 0 \mod 7$$

showing that $a^2 - 7$ is divisible by 7. ■