Chapter 1 - Sets and Proofs*

Contents

[*] These resources were developed by Joseph Clarke, **Tom Conti-Leslie**, Gemma Crowe, Leticija Dubickaitė, Jack Dunham with support from the Teaching Development Fund at the University of St Andrews

0 Introduction

Many university-level problems in mathematics will require you to do more than just find an expression for a function, or compute the value of an integral: some will ask you to prove more general results, which can then be applied in other situations. This means that, aside from being comfortable working with lots of variables $(x, n, t, a, b, \dots)$ rather than numbers, it will be useful for you to know more about how to construct a good proof, as well as some basic set theory, which many courses at university assume you have knowledge of.

Note: Thorough knowledge of this chapter on Sets and Proofs is not immediately necessary for you as you enter second-year mathematics courses at the University of St Andrews, and you may want to focus on the other chapters of this revision resource before working through this one in detail. However, it might be useful to keep this document handy for quick reference throughout the year: although you will not be asked to prove difficult statements from your first week here (phew!), proofs will continue to appear in questions, and so will sets.

1 Elementary Set Theory

So what is a set? You've probably come across many examples of sets before - for example, $\mathbb{R}$ is a set containing every real number, like 0, 3, -2.5, $\frac{10}{7}$, $\sqrt{2}$, $\pi, \ldots$ More generally:

Definition 1.1. A **set** is a collection of *objects*, or *things* - these can be numbers, or functions, or vectors, or abstract objects, or even other sets. We usually write a set as a list of all the things inside it, surrounded by curly braces.

Example 1.2.

- $\{0, 1, 2\}$ is a set containing the numbers 0, 1 and 2. Order doesn't matter when defining a set, so $\{0, 1, 2\} = \{1, 2, 0\}$, etc.
- {Tinky Winky, Dipsy, Laa Laa, Po} is a set containing the four Teletubbies.
- {Apples that are oranges} is a set containing nothing, as there are no apples which are also oranges! So this set is empty; we call it the **empty set**, which can be referred to using the symbol $\emptyset$.
- $\mathbb{N} = \{1, 2, 3, \ldots\}$ is the set of *positive integers*. The ellipses in the curly braces indicate that to write down everything in the set, we would have to fill in the blank by continuing the pattern in some obvious way. If you wanted to write the set of all integers between 1 and 10, you could write $\{1, 2, \ldots, 10\}$.
- $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ is the set of *integers*. It contains every element in $\mathbb{N}$, as well as 0 and the negative of every element in $\mathbb{N}$.
- $\mathbb{R}$ is the set of all *real numbers*.

1.1 Elements of Sets

At this point, it may be useful for us to be able to quickly write down whether or not some object is in a set or not.

Definition 1.3. Conventionally, we use the symbol $\in$ to indicate that something is in a set.

Example 1.4.

- $0 \in \{0, 1, 2\}$, but $3 \notin \{0, 1, 2\}$. We would read this as "0 is an element of $\{0, 1, 2\}$, but 3 is not an element of $\{0, 1, 2\}$".
- $5 \in \mathbb{N}$ but $-5 \notin \mathbb{N}$; however, $-5 \in \mathbb{Z}$.
- Careful! $3 \notin \{\sqrt{2}, 1, \{3\}\}$, but $\{3\} \in \{\sqrt{2}, 1, \{3\}\}$. Sets can contain other sets!

1.2 Set-Builder Notation

Sometimes it is difficult to write down a set completely, and it is also difficult to use ellipses (i.e. "$\dots$") to shorten the amount of writing. In this case, we can use something called set-builder notation, which is commonly used in mathematics:

Definition 1.5. Set-builder notation refers to a set in the following form:

$$\{x \in X : x \text{ has some property called } P\}.$$

This means that we construct a set by looking at every element of another set X, and only taking the ones which have the property (P) that we're looking for.

Example 1.6. We can use the set-builder notation in Definition 1.5 to define more complicated sets.

- $\{n \in \mathbb{N} : n \text{ is even}\}$ is the set of all positive even integers. We can also write it as $\{2, 4, 8, \dots\}$.
- $\mathbb{Q} = \{\frac{p}{q} : p \in \mathbb{Z}, q \in \mathbb{Z}, q \neq 0\}$ is the set of *rational numbers*. Our set-builder notation says that it contains every number of the form p/q where p and q are integers (and q is non-zero). Note that this set-builder notation is not quite identical to the one described above, but it works in a similar way.
- $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$, where i is the imaginary unit such that $i^2 = -1$, is the set of all *complex numbers*. See Chapter 8 for details.

1.3 The Size of a Set

Now that we can construct and define sets, we can study them in more detail. The first question is: if I have a set A, how many elements are in it?

Definition 1.7. The number of elements in a set A is called the **size** of A and is denoted by $|A|$.

Example 1.8. If $A = \{0, 1, 2\}$ then $|A| = 3$; $|\emptyset| = 0$ (empty set, see above); $|\mathbb{N}| = \infty$.

1.4 Subsets

Given two sets, we can compare them in different ways. For example, you may have noticed that in our Example 1.2 we defined $\mathbb{N}$ and $\mathbb{Z}$ and noted that $\mathbb{Z}$ contained every number in $\mathbb{N}$, as well as other numbers. There is a name for this!

Definition 1.9. Let A and B be sets. Then if every element of A is also in B, we say that A is a **subset** of B and write $A \subseteq B$.

If we also know that $A \neq B$, then A is called a **proper subset** of B and we write $A \subset B$.

Example 1.10.

- $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.
- $\{0,1,2\} \subset \{0,1,2,3,4\} \subset \mathbb{Z}$.
- $\{0,1,2\} \not\subseteq \mathbb{N}$ because $0 \in \{0,1,2\}$ but $0 \notin \mathbb{N}$.
- If A is any set, then $A \subseteq A$ and $\emptyset \subseteq A$.

1.5 Intersection and Union

One other thing we can do when given two sets is look at what they have in common, and what happens when we join them together. These actions are called intersection and union, and are very important in any part of mathematics which uses sets.

Definition 1.11. Let A and B be sets. Then the **intersection** of A and B is the set:

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

and the **union** of A and B is the set

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

This means that $A \cap B$ is the set of all things that A and B have in common, and $A \cup B$ is the set of the combined elements of A and B.

The concepts of intersection and union can be understood visually with Venn diagrams; see here for a video explaining this. You can also play around with a similar idea on these interactive graphs:

- Click here for a graph explaining intersection;
- Click here for a graph explaining subsets.

Example 1.12.

- Let $A = \{0,1,2\}$ and $B = \{1,2,3\}$.
  - $A \cap B = \{0,1,2\} \cap \{1,2,3\} = \{1,2\}$;
  - $A \cup B = \{0,1,2\} \cup \{1,2,3\} = \{0,1,2,3\}$. Although the 1 and 2 appear once in each set, we only write them once each in the union set because you can't have an element twice in the same set!
- Let $C = \{x \in \mathbb{R} : \ x > 1\}$ and $D = \{x \in \mathbb{R} : \ x < 1\}$. Then

  $$C \cap D = \{x \in \mathbb{R} : \ x < 1 \text{ and } x > 1\}.$$

  But no real number is both strictly less than 1 and also strictly greater than 1, so this set is empty! Therefore, $C \cap D = \emptyset$. When this is the case, we can say that C and D are **disjoint**.

We can also look at the intersection and the union of more than two sets. One first thing to notice is that for any sets A, B, C:

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

(This is called *associativity*, but you need not know this or know how to prove that it is true). Associativity means that we can write these intersections and unions of sets without using parentheses at all: for example,

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

This is the set of all elements that are in A *and* in B *and* in C.

Example 1.13.

- $\{0, 1, 2, \dots, 12\} \cap \{0, 2, 4 \dots, 12\} \cap \{0, 3, 6, 9, 12\} = \{0, 6, 12\}$.
- $\{1\} \cup \{2\} \cup \{3\} \cup \dots \cup \{n\} = \{1, 2, 3, \dots, n\}$.

1.6 Set Differences

The last thing we can do when given two sets is look at what one set gives when we remove all elements that it has in common with the other.

Definition 1.14. The **complement** of A with respect to B, also called the **difference** of A and B, is the set of all elements of B which are not in A, and is denoted:

$$B \setminus A = \{b \in B : \ b \notin A\}.$$

Examples 1.15.

- $\{0, 1, 2, 3\} \setminus \{0, 1\} = \{2, 3\}$
- For every set A, $A \setminus \emptyset = A$ and $A \setminus A = \emptyset$.
- $\mathbb{Z} \setminus \mathbb{N} = \{\dots, -2, -1, 0, 1, 2, \dots\} \setminus \{1, 2, \dots\} = \{\dots, -2, -1, 0\}$.
- $\mathbb{R} \setminus \mathbb{Q}$ is the set of all real numbers that are not rational numbers: it is the set of *irrational numbers* and contains numbers such as $\sqrt{2}$ and π.

That's all you'll need to know about sets, phew! Sets can be difficult to get your head around, as they are very abstract and general mathematical objects. But they are extremely useful in many diverse areas of maths, so it's very useful to know how to use them!

2 Some Background on Logic

As we have discussed, proofs are central to the mathematical world and university-level maths often requires you to come up with your own proofs. Before we cover a few methods of proof, we'll introduce what lies behind them: logic.

2.1 Implication

Mathematical arguments rely on strong and stable logic to be considered valid. When proving a statement about something, it is not sufficient to say: "It worked when I tried these numbers, so it must always work"! You need to make sure that every step of your reasoning makes sense, and cannot be argued against. So, every step needs to be an **implication**.

Definition 2.1. A statement of the form "If A, then B" is called an **implication**. It means "If A is true, then B is true" and also means "If A is false, then B can be either true or false". If the statement "If A, then B" is true, we say that A **implies** B and write $A \implies B$.

Here, A and B represent logical statements. They are sentences such as "x is greater than 0", or "$x \in \mathbb{N}$", or "I am tall". These statements will always be either true or false, and the implication $A \implies B$ simply says something about the link between A being true and B being true.

To prove that $A \implies B$ is a logically valid argument, you need to be able to show that there is no situation in which A is true but B isn't. In practice, you do not need to prove that small and obvious implications such as "if $x > 2$ then $x^2 > 4$", or "if $y > 2$ then $y > 1$" are valid; you will simply use these small implications, organised in the right sequence, to prove bigger statements.

Once you have shown that $A \implies B$, or if you have been told that you may *assume* that $A \implies B$, then you've made your life a lot easier, because you know that whenever A is true you can instantly affirm that B is also true!

Example 2.2. Let X and Y be sets, and $x \in X$. Then the following implications are valid:

- $X \subseteq Y \implies x \in Y$, i.e. if X is a subset of Y (see Definition 1.9) then x (an object of X) is also in Y. This is because if the statement "$X \subseteq Y$" is true then by definition of a subset, every element of X is also contained in Y.

- $X \cap Y = \emptyset \implies x \notin Y$, i.e. if the intersection of X and Y (see Definition 1.11) is the empty set then x is not in Y. This is because if x were in Y, then x would be in both X and Y and so x would be in $X \cap Y$. But that would mean that $X \cap Y$ would not be the empty set, which is impossible.

2.2 Converse and Contrapositive

Once we have defined the implication $A \implies B$ in Definition 2.1, we can look at some related implications.

Definition 2.3. The **converse statement** of the implication $A \implies B$ is the implication $B \implies A$. If A implies B, it *does not necessarily mean that the converse is also true*, although it can be.

The **contrapositive statement** of the implication $A \implies B$ is the implication Not $B \implies$ Not A. If A implies B, then *the contrapositive is always true*.

Let's try and get a grasp for this with a real-world example; looking at all of this theoretical stuff can be confusing!

Example 2.4. Let's imagine we are examining an unknown fruit which we will call F. We can't tell what it is by smelling it or tasting it; all we are armed with is the knowledge of its colour, as well as one sole piece of wisdom that we have read in a mysterious ancient scroll: "*all limes are green*".

Let L denote the statement "F is a lime" and G denote the statement "F is green". Then our ancient piece of wisdom states that $L \implies G$, which we will take to be true (it is often at this stage - assuming that the premises are true - that many a logical argument goes wrong, but let's not worry about that for now).

The **converse** of our piece of wisdom is the statement $G \implies L$, which translates to: "if F is green, then F is a lime". This is clearly false, as some apples are green but are not limes. So the converse statement is not always true, and we haven't made any progress towards figuring out what F is.

The **contrapositive** of this piece of wisdom, however, is Not $G \implies$ Not L, also sometimes written $\neg G \implies \neg L$. This translates to "if F is not green, then F is not a lime". This is indeed true, as long as L does indeed imply G as we have assumed. So by the contrapositive of the statement from our ancient scroll, we can make deductions about what fruit F is... but only if it is not green.

2.3 Equivalence

Example 2.4 gave us an example of a situation in which the converse of a statement is false, but this is not always the case. You may remember the Pythagorean Theorem:

A right-angled triangle with hypotenuse length c and other side lengths a, b satisfies the equation $a^2 + b^2 = c^2$.

It turns out that the converse of this statement is actually true! The converse of the Pythagorean Theorem is:

If a triangle with side lengths a, b and c satisfies the equation $a^2 + b^2 = c^2$, then it is a right-angled triangle with hypotenuse length c.

So, in this case, both the statement and its converse are true. We have a specific name for this:

Definition 2.5. Two logical statements A and B are said to be **equivalent** if both $A \implies B$ and $B \implies A$. We can write this as $A \iff B$, and read this as "A **if and only if** B", which can be abbreviated in writing to "A **iff** B".

This means that if you're asked to show that A and B are equivalent, you need to prove both that $A \implies B$ and that $B \implies A$, which means that in most cases your proof will involve two parts.

Example 2.6. *Let A, B be sets. Prove that $A \subseteq B$ if and only if every subset of A is also a subset of B.* Try to prove this yourself before looking at the solution! You may want to look back to Definition 1.9.

Answer. Call S_1 the statement "$A \subseteq B$" and S_2 the statement "Every subset of A is also a subset of B". Then we will separately prove that $S_1 \implies S_2$ and $S_2 \implies S_1$.

- $(S_1 \implies S_2)$: Suppose A is a subset of B. Then every element of A is an element of B. Let C be any subset of A; then every element of C is also in A, and hence is also in B. This implies $C \subseteq B$ for any $C \subseteq A$.

- $(S_2 \implies S_1)$: Suppose every subset of A is also a subset of B. We know that A is a subset of itself: $A \subseteq A$. By our assumption that S_2 is true, this means that A is a subset of B, as required.

Note that questions where you are asked to prove something will be announced with wording like "prove that" or "show that". On the other hand, if you're just asked to check that something is true, you may be asked to "check that" or "verify that".

In the mathematical literature, the end of a proof is marked with a box which looks like this: □ or like this: ■. Many people choose to do this in writing as well; others simply write "Q.E.D.", which stands for the Latin phrase *quod erat demonstrandum*. In any case, it is helpful to show where your proof ends; find a style that suits you!

Sometimes, when you need to prove that two statements are equivalent, you can prove both directions at the same time. The next (easy) example shows this:

Example 2.7. *Let $x \in \mathbb{R}$. Prove that $x \geq 10 \iff \frac{3-x}{7} \leq -1$.*

Answer. We can simply perform some algebraic manipulation which works both ways:

$$\begin{aligned} & x \geq 10 \\ \iff & x - 3 \geq 7 \\ \iff & 3 - x \leq -7 \\ \iff & \frac{3-x}{7} \leq -1. \end{aligned}$$

Every line in this proof works as well one way as it does in the other (for example, when subtracting 3 to both sides on the second line, the operation can be reversed by adding 3 to both sides). So the implication does indeed work both ways.

2.4 Quantifiers

By now, you will have noticed that many logical statements require the use of *quantifiers*: words that say, for example, that a statement is true for any element of A, and not just one element. In English, we can use the words "for all"; but as this appears quite a lot in proofs, we have an abbreviation for such quantifiers.

Definition 2.8. Quantifiers: the symbol $\forall$ means "for all", or "for every", and is called the *universal quantifier*.

The symbol $\exists$ means "there exists", and is called the *existential quantifier*.

These symbols can be used as shorthands to write statements.

Example 2.9.

- $\forall x \in \mathbb{R}$, $x^2 \geq 0$: Every real number has a square that is greater than or equal to 0.
- We denote the set of all real numbers except 0 by the symbol $\mathbb{R}\backslash\{0\}$. Then:

  $$\forall x \in \mathbb{R}\backslash\{0\}, \exists y \in \mathbb{R}\backslash\{0\} \text{ such that } xy = 1.$$

  This means: for every non-zero real number x, there exists a non-zero real number y such that $x \times y = 1$. In fact, it is easy to spot that $y = 1/x$.
- If $A \subseteq B$, then $\forall a \in A$, $a \in B$: If A is a subset of B, then every element of A is an element of B.

Using these quantifiers as substitutes must be done with caution when the statements are long. In particular, note the difference between:

$$\forall x\, \exists y, \quad (1)$$
$$\exists y\, \forall x. \quad (2)$$

Substituting natural language into these expressions we get:

(1) For all people x there exists a word y which is the name of person x;

(2) There exists a word y which is the name of all people x.

Clearly, these statements mean different things. The first allows y to be different for different xs. However, in the second, one singular y must work for all x.

With the knowledge of all of this in mind, we can start looking at some different ways of proving a statement.

3 Methods of Proof

Before we begin this section, it's important to stress the following: when proving a statement about some general object (e.g. a statement which works for any real number, or any matrix, ...), it is not enough to try a few values and say that it works. If you're proving something about x (where x can represent any real number, say), you have to make sure that your proof will work for *any* value of x you plug in, not just a few that you have tried. With this in mind, let's look at some ways we can go about proving such statements.

Suppose we want to prove that $A \implies B$ (see Definition 2.1). There are many different ways of doing this, some of which we have seen already. The most obvious method is by proving a chain of statements which eventually lead to B.

3.1 Proving a Chain of Statements

Most often, when you need to prove that A implies B you will need to **prove some intermediate steps** first, as the direct jump from A to B is not that obvious. So you will try to prove

$$A \implies A_1 \implies A_2 \implies \cdots \implies A_n \implies B.$$

This is similar to Example 2.7 where we were asked to show $x \geq 10 \iff \frac{3-x}{7} \leq -1\ \forall x \in \mathbb{R}$. We'll include an example of a non-proof here.

Example 3.1. *Prove that* $\sqrt{\frac{\sqrt{5}}{2}+3} > 2$.

Note that what we need to prove here is not in the form $A \implies B$ but rather just "show that B is true". This doesn't change the form of the proof, however, because we will still be making a series of deductions; although the initial assumption A is not specified here, you will end up making use of your own initial assumptions (such as, perhaps, $0 < x < y \implies 0 < x^2 < y^2\ \forall x, y \in \mathbb{R}$). Let's go through a non-proof of this statement.

Non-Proof. We write

$$\begin{aligned}\sqrt{\frac{\sqrt{5}}{2}+3} > 2 &\implies \left(\sqrt{\frac{\sqrt{5}}{2}+3}\right)^2 > 4\\ &\implies \frac{\sqrt{5}}{2} > 1\\ &\implies \frac{5}{4} > 1\\ &\implies 5 > 4.\end{aligned}$$

The final line we know to be a true statement, therefore $\sqrt{\frac{\sqrt{5}}{2}+3} > 2$ must be true.

The reason this is not a correct proof is that all we have shown is that *if* $\sqrt{\frac{\sqrt{5}}{2}+3} > 2$, *then* $5 > 4$. What we need to prove is the opposite: that if $5 > 4$ (perhaps along with some other general truths that we will take to be assumptions), then $\sqrt{\frac{\sqrt{5}}{2}+3} > 2$. So although the chain of deductions here is a good example of the general method, make sure your arrows are pointing in the right direction! We'll see an actual proof of this statement a bit later on.

3.2 Proof by Separation of Cases

Sometimes it will be easier to prove $A \implies B$ by **separating** A into some sub-cases so that if A is true, then at least one of $C_1, C_2, \ldots, C_n$ is true. If you prove $C_i \implies B$ for each i you'll have shown that $A \implies B$ is true! Let's look at an example.

Example 3.2. *Let $n \in \mathbb{Z}$. Prove that n^2 never gives remainder 2 when divided by 3.*

Answer. One option here is to look at the different remainders n could have when divided by 3 and separate those cases. If n has remainder 0 then $n = 3k$ for some $k \in \mathbb{Z}$; if n has remainder 1 then $n = 3k+1$; and if it has remainder 2, then $n = 3k+2$. We separate these three cases.

- If $n = 3k$ for some $k \in \mathbb{Z}$, then $n^2 = 9k^2 = 3(3k^3)$ which is divisible by 3 so gives remainder 0 when divided by 3.
- If $n = 3k+1$ for some $k \in \mathbb{Z}$, then $n^2 = (3k+1)^2 = 9k^2+6k+1 = 3(3k^2+2k)+1$ which gives remainder 1 when divided by 3.
- If $n = 3k+2$ for some $k \in \mathbb{Z}$, then $n^2 = (3k+2)^2 = 9k^2+12k+4 = 3(3k^2+12k+1)+1$ which gives remainder 1 when divided by 3.

So in each possible case, n^2 does not give remainder 2, as required. □

3.3 Proof by Contrapositive

The principle of proof by contrapositive relies simply on the fact that proving the statement $A \implies B$ is *logically equivalent* to proving the statement $\neg B \implies \neg A$, i.e. to prove an implication **you can just prove its contrapositive** (see Definition 2.3). This is occasionally easier to prove.

Example 3.3. *Let $n \in \mathbb{Z}$. Prove that if $n^2 - 5n + 10$ is odd, then n is odd.*

Answer. It might be a little difficult to figure out where to start, so why not prove the contrapositive: if n is *not* odd (i.e. even) then $n^2 - 5n + 10$ is even.

If n is even then $n = 2k$ for some $k \in \mathbb{Z}$. Then:

$$\begin{aligned} n^2 - 5n + 10 &= (2k)^2 - 5(2k) + 10 \\ &= 4k^2 - 10k + 10 \\ &= 2(2k^2 - 5k + 5) \end{aligned}$$

So $n^2 - 5n + 10$ is indeed even, as required. □

3.4 Proof by Counterexample

Rather than proving that an implication $A \implies B$ is *true*, sometimes you need to prove that it is *false*. This is, thankfully, a lot easier to do! As we said in Subsection 2.1, an implication $A \implies B$ is valid if there is no context in which A is true but B is not. So to show this isn't the case, all we need to do is find one context in which A is true but B is false: a **counterexample**. Most of the time, this means plugging in some value of a variable which makes the statement false.

Example 3.4. *Disprove the following statement:* $x^2 > 0 \, \forall x \in \mathbb{R}$.

Answer. To find a good counterexample, the best thing to do is to stare at the equation for a bit and see if any values come to mind which would make it false! Here, it doesn't take long to come up with the counterexample: $0 \in \mathbb{R}$ but $0^2 = 0$ which is not strictly greater than 0 as claimed. So the statement is indeed false. □

Example 3.5. *Prove that matrix multiplication is not always commutative, i.e. that if A and B are matrices then AB is not always equal to BA.* (If you need to brush up on matrices first, see Chapter 10.)

Answer. To prove that matrix multiplication is not commutative, we need to find two matrices which do not give the same product when you invert the order of multiplication. We can take matrices of any size, but we're looking for an easy example so we'll stick to 2×2 matrices and see if we can find a counterexample there.

Take, for example, $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$. (When looking for a counterexample, choose some random entries for your matrix that aren't too hard to work with, and change them later if they turn out not to be a valid counterexample). We compute AB and BA:

$$AB = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 \cdot 1 + 1 \cdot 2 & 1 \cdot 2 + 1 \cdot 1 \\ 1 \cdot 1 + 0 \cdot 2 & 1 \cdot 2 + 0 \cdot 1 \end{pmatrix} = \begin{pmatrix} 3 & 3 \\ 1 & 2 \end{pmatrix};$$

$$BA = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 \cdot 1 + 2 \cdot 1 & 1 \cdot 1 + 2 \cdot 0 \\ 2 \cdot 1 + 1 \cdot 1 & 2 \cdot 1 + 1 \cdot 0 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 3 & 2 \end{pmatrix}.$$

So clearly $AB \neq BA$, therefore providing a counterexample proving that matrix multiplication is not commutative in general. □

Here, our use of the words "in general" means that *some* matrices do not commute when you multiply them. However, this is not true for every pair of matrices: it is possible to find pairs of matrices which *do* commute.

3.5 Proof by Contradiction

In certain cases, a very powerful method of proof comes in handy: proof by contradiction. When asked to prove that a statement is true, the method of **proof by contradiction** is to assume that the statement is in fact false, then make deductions from this assumption until we reach a point where what we have deduced contradicts the initial assumptions. This is best seen with some examples.

Example 3.6. Let's return to the question from Example 3.1:

Prove that $\sqrt{\frac{\sqrt{5}}{2}+3} \leq 2$.

We can do this by contradiction.

Answer. Assume this statement is false, i.e. $\sqrt{\frac{\sqrt{5}}{2}+3} \leq 2$. Then:

$$\begin{aligned}\sqrt{\frac{\sqrt{5}}{2}+3} \leq 2 &\implies \left(\sqrt{\frac{\sqrt{5}}{2}+3}\right)^2 \leq 4 \quad \text{(since both sides are positive)}\\ &\implies \frac{\sqrt{5}}{2} \leq 1\\ &\implies \frac{5}{4} \leq 1\\ &\implies 5 \leq 4.\end{aligned}$$

This last line is clearly false, so is a contradiction. Hence, our assumption that $\sqrt{\frac{\sqrt{5}}{2}+3} \leq 2$ must be false.

Note that sometimes, when we reach a contradiction in writing, we denote it by a symbol such as ↯ or ※.

Here's a slightly more difficult example - don't worry if you don't understand it immediately as it is a bit technical! However, it is a good example of how a proof can be constructed and written.

Example 3.7. *Prove that there are infinitely many prime numbers.* (Recall a *prime number* is an integer $n \geq 2$ whose only positive divisors are 1 and itself).

Answer. In this answer, we will use the *Fundamental Theorem of Arithmetic*: that any positive integer can be written as a product of primes. Now assume, for a contradiction, that there is only a finite number of prime numbers. Then we can write them all as $p_1, p_2, \ldots, p_n$. Let $P = p_1 p_2 \ldots p_n + 1$. Since P can be written as a product of primes, there must be some prime number p which is a divisor of P (i.e. P/p is a whole number). But since $p_1, p_2, \ldots p_n$ is a list of all the prime numbers, p must be in there somewhere and so there is an integer i such that $p = p_i$. But p_i is a divisor of $p_1 p_2 \ldots p_n$, so it cannot be a divisor of $p_1 p_2 \ldots p_n + 1 = P$. So we have deduced that p cannot be a divisor of P, which is a contradiction since we assumed that p was a divisor of P. ※

Proof by contradiction can be very powerful, so it's worth keeping in mind as a trick you may need to use at some point. It's a commonly used technique when it comes to proving the uniqueness of something - say you have a set A, and you want to show there is only one element in A that satisfies some property. If you assume that two distinct elements satisfy it and play around with what that implies for a while, you will generally manage to pull a contradiction out of it and your proof is done!

3.6 Proof by Induction

We now discuss the last method of proof in this chapter - **proof by induction**. You may have heard of this type of proof before, and it is quite a powerful technique. Let's start with an analogy.

Suppose you're standing at the foot of a ladder with steps numbered $1, 2, 3, \ldots$ off to infinity, and your aim is to show that you will be able to reach any step of the ladder, i.e. you will be able to climb the ladder to step n for any $n \in \mathbb{N}$. Theoretically, you could even keep climbing forever!

There are many ways of proving that you can do this, and one of them uses inductive reasoning. Suppose you are able to show that:

a) You can reach the first step of the ladder;

b) If you can reach step n ($n \in \mathbb{N}$) of the ladder, then you will be able to reach step $n + 1$.

If you can prove these two things, you've basically finished the proof! Suppose you want to check if you can reach step 10, knowing that these two statements (a and b) are true. Well, you know that you can reach step 1 by statement a). Once you're at step 1, replace n with 1 in statement b) to show that you can reach step 2. When at step 2, you can use statement b) similarly again to show that you can reach step 3, and so on until step 10. In this way you can show that you'll be able to reach any step eventually!

This is the principle of mathematical induction. Suppose you want to prove the following statement about natural numbers:

"*$\forall n \in \mathbb{N}$, n has property P.*"

Perhaps this property is something like "$5^n - 2^n$ is divisible by 3", or "The determinant of an $n \times n$ diagonal matrix is the product of its diagonal entries". In any case, it is a statement that you will need to prove to be true for all values of n in the natural numbers $\mathbb{N}$. Spotting that a statement depends on the natural numbers in this way is a tell-tale sign that induction might be helpful for you to prove it.

To do this, call P_k the statement "the natural number k satisfies property P". Then our full statement can be broken up into statements $P_1, P_2, P_3, \ldots$. If all these sub-statements P_k are true, then our full statement is true. For example, if P is the property "$5^n - 2^n$ is divisible by 3", then the P_k are:

- P_1: "$5^1 - 2^1$ is divisible by 3"
- P_2: "$5^2 - 2^2$ is divisible by 3"
- P_3: "$5^3 - 2^3$ is divisible by 3"
- $\ldots$

and so on. All we need to prove is that P_k is true for all k, and we can do that like we climbed up the ladder:

a) Prove that P_1 is true. This is called the **base case**.

b) Prove that for all k, if P_k is true then P_{k+1} is true. This is called the **inductive step**.

If you can prove these two things, then by the *principle of mathematical induction*, P_k will be true for all k, i.e. your statement will be true. Let's go over an example.

Example 3.8. *Prove that* $2^n < n!\ \forall n \in \mathbb{N}$ *s.t.* $n \geq 4$*, where the exclamation mark denotes the factorial function:* $n! = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 2 \cdot 1.$

Answer. Here, our P_k is "$2^k < k!$", and since we are trying to prove this property for all integers greater than or equal to 4, the base case will be to prove P_4, not P_1. This is fine: the base case can be a different case than 1 (a common alternative being P_0) and all you need to remember is that when you prove something by induction, you are only proving the cases *from the base case onwards*. So since our base case here is P_4, the property will only work for P_4, $P_5, \ldots$ and so on.

Back to business: for P_4 we have $2^4 = 16$ and $4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$, so indeed $2^4 < 4!$. So the base case holds.

Inductive step: assume that P_n is true for some $n \in \mathbb{N}$, $n \geq 4$ (note we've changed from using k to using n here; it really doesn't matter which one you use, although in induction proofs n tends to be the standard notation). We wish to prove that if P_n is true, then P_{n+1} is true, i.e. $2^{n+1} < (n+1)!$. We know:

$$\begin{aligned} & 2^n < n! && \text{(This is the \textit{inductive hypothesis})} \\ \implies & 2^{n+1} < 2 \cdot n! && \text{(Multiplying both sides by 2)} \\ \implies & 2^{n+1} < (n+1) \cdot n! && \text{(Since } n+1 > 2\text{)} \\ \implies & 2^{n+1} < (n+1)! \end{aligned}$$

And hence P_{n+1} is true. So, by the principle of mathematical induction, P_n is true for all $n \geq 4$, i.e. $2^n < n!$.

4 Some Mathematical Symbols

To conclude this chapter, we include a quick reference table containing some mathematical symbols you are likely to come across. Most have been seen in this chapter, but some will be new!

$\forall$	for all
$\exists$	there exists
s.t.	such that
$\Longrightarrow$	implies
$\Longleftarrow$	is implied by
$\Longleftrightarrow$	if and only if
iff	if and only if
WLOG	without loss of generality
$\mathbb{N}$	natural numbers $\{1, 2, 3, \dots\}$
$\mathbb{Z}$	integers $\{\dots, -2, -1, 0, 1, 2, \dots\}$
$\mathbb{Q}$	rational numbers $\{p/q :\ p, q \in \mathbb{Z}\}$
$\mathbb{R}$	real numbers
$\mathbb{C}$	complex numbers $\{a + bi :\ a, b \in \mathbb{R}\}$
$\S$	section
$\square$, $\blacksquare$, Q.E.D.	end of proof
$\subseteq$	subset of
$\subset$	proper subset of
$\cap$	intersection of two sets
$\cup$	union of two sets
$\setminus$	difference of two sets
$\emptyset$	empty set
(a, b)	The **open interval** $\{x \in \mathbb{R} :\ a < x < b\}$
$[a, b]$	The **closed interval** $\{x \in \mathbb{R} :\ a \leq x \leq b\}$
$(a, b]$	The half-open interval $\{x \in \mathbb{R} :\ a < x \leq b\}$
$[a, b)$	The half-open interval $\{x \in \mathbb{R} :\ a \leq x < b\}$

Table 1: Table of useful mathematical symbols