UNIVERSITY OF BIRMINGHAM

Proofs and Mathematical Reasoning

University of Birmingham

Author:
Agata Stefanowicz

Supervisors:
Joe Kyle
Michael Grove

September 2014

Contents

Foreword

Talk to any group of lecturers about how their students handle proof and reasoning when presenting mathematics and you will soon hear a long list of 'improvements' they would wish for. And yet, if no one has ever explained clearly, in simple but rigorous terms, what is expected it is hardly a surprise that this is a regular comment. The project that Agata Stefanowicz worked on at the University of Birmingham over the summer of 2014 had as its aim, clarifying and codifying views of staff on these matters and then using these as the basis of an introduction to the basic methods of proof and reasoning in a single document that might help new (and indeed continuing) students to gain a deeper understanding of how we write good proofs and present clear and logical mathematics. Through a judicious selection of examples and techniques, students are presented with instructive examples and straightforward advice on how to improve the way they produce and present good mathematics. An added feature that further enhances the written text is the use of linked videos files that offer the reader the experience of 'live' mathematics developed by an expert. And Chapter 9, that looks at common mistakes that are made when students present proofs, should be compulsory reading for every student of mathematics. We are confident that, regardless of ability, all students will find something to improve their study of mathematics within the pages that follow. But this will be doubly true if they engage with the problems by trying them as they go through this guide.

Michael Grove & Joe Kyle
September 2014

Acknowledgements

I would like to say a big thank you to the Mathematics Support Centre team for the opportunity to work on an interesting project and for the help and advice from the very first day. Special gratitude goes to Dr Joe Kyle for his detailed comments on my work and tips on creating the document. Thank you also to Michael Grove for his cheerful supervision, fruitful brainstorming conversations and many ideas on improving the document. I cannot forget to mention Dr Simon Goodwin and Dr Corneliu Hoffman; thank you for your time and friendly advice. The document would not be the same without help from the lecturers at the University of Birmingham who took part in my survey - thank you all.

Finally, thank you to my fellow interns, Heather Collis, Allan Cunningham, Mano Sivantharajah and Rory Whelan for making the internship an excellent experience.

1 Introduction

From the first day at university you will hear mention of writing Mathematics in a good style and using "proper English". You will probably start wondering what is the whole deal with *words*, when you just wanted to work with *numbers.* If, on top of this scary welcome talk, you get a number of definitions and theorems thrown at you in your first week, where most of them include strange notions that you cannot completely make sense of - do not worry! It is important to notice how big difference there is between mathematics at school and at the university. Before the start of the course, many of us visualise really hard differential equations, long calculations and x-long digit numbers. Most of us will be struck seeing theorems like "$a \times 0 = 0$". Now, while it is *obvious* to everybody, mathematicians are the ones who will not take things for granted and would like to see the *proof.*

This booklet is intended to give the gist of mathematics at university, present the language used and the methods of proofs. A number of examples will be given, which should be a good resource for further study and an extra exercise in constructing your own arguments. We will start with introducing the mathematical language and symbols before moving onto the serious matter of writing the mathematical proofs. Each theorem is followed by the "notes", which are the thoughts on the topic, intended to give a deeper idea of the statement. You will find that some proofs are missing the steps and the purple notes will hopefully guide you to complete the proof yourself. If stuck, you can watch the videos which should explain the argument step by step. Most of the theorems presented, some easier and others more complicated, are discussed in first year of the mathematics course. The last two chapters give the basics of sets and functions as well as present plenty of examples for the reader's practice.

2 Mathematical language and symbols

2.1 Mathematics is a language

Mathematics at school gives us good basics; in a country where mathematical language is spoken, after GCSEs and A-Levels we would be able to introduce ourselves, buy a train ticket or order a pizza. To have a fluent conversation, however, a lot of work still needs to be done.

Mathematics at university is going to surprise you. First, you will need to learn the *language* to be able to communicate clearly with others. This section will provide the "grammar notes", i.e. the commonly used symbols and notation, so that you can start writing your mathematical statements in a good style. And like with any other foreign language, "practice makes perfect", so take advantage of any extra exercises, which over time will make you fluent in a mathematical world.

2.2 Greek alphabet

Greek alphabet - upper and lower cases and the names of the letters.

2.3 Symbols

Writing proofs is much more efficient if you get used to the simple symbols that save us writing long sentences (very useful during fast paced lectures!). Below you will find the basic list, with the symbols on the left and their meaning on the right hand side, which should be a good start to exploring further mathematics. Note that these are useful shorthands when you need to note the ideas down quickly. In general though, when writing your own proofs, your lecturers will advise you to use *words* instead of the fancy notation - especially at the beginning until you are totally comfortable with the statements "if..., then...". When reading mathematical books you will notice that the word "implies" appears more often than the symbol $\implies$.

A	α	alpha	N	ν	nu
B	β	beta	Ξ	ξ	xi
Γ	γ	gamma	O	o	omicron
Δ	δ	delta	Π	π	pi
E	ϵ	epsilon	P	ρ	rho
Z	ζ	zeta	Σ	σ	sigma
H	η	eta	T	τ	tau
Θ	θ	theta	Y	υ	upsilon
I	ι	iota	Φ	ϕ	phi
K	κ	kappa	X	χ	chi
Λ	λ	lambda	Ψ	ψ	psi
M	μ	mu	Ω	ω	omega

Table 1: Greek letters

- Quantifiers

$\forall$ (universal quantifier)	for all
$\exists$ (existential quantifier)	there exists

- Symbols in set theory

$\cup$	union
$\cap$	intersection
$\subseteq$	subset
$\subset, \subsetneq$ or $\subsetneqq$	proper subset
$\circ$	composition of functions

- Common symbols used when writing proofs and definitions

$\Longrightarrow$	implies
$\Longleftrightarrow$	if and only if
$:=$	is defined as
$\equiv$	is equivalent to
$:$ or $\mid$	such that
$\therefore$	therefore
$\lightning$ or $\frownie$	contradiction
$\blacksquare$ or $\square$	end of proof

2.4 Words in mathematics

Many symbols presented above are useful tools in writing mathematical statements but nothing more than a convenient shorthand. You must always remember that a good proof should also include *words*. As mentioned at the beginning of the paper, "correct English" (or any other language in which you are literate) is as important as the symbols and numbers when writing mathematics. Since it is important to present proofs clearly, it is good to add the explanation of what is happening at each step using full sentences. The whole page with just numbers and symbols, without a single word, will nearly always be an example of a bad proof!

Tea or coffee? Mathematical language, though using mentioned earlier "correct English", differs slightly from our everyday communication. The classic example is a joke about a mathematician,

who asked whether they would like a tea or coffee, answers simply "yes". This is because "or" in mathematics is inclusive, so A **or** B is a set of things where each of them must be either in A or in B. In another words, elements of A or B are both those in A *and* those in B. On the other hand, when considering a set A **and** B, then each of its elements must be both in A and B.

Exercise 2.1. *Question: There are 3 spoons, 4 forks and 4 knives on the table. What fraction of the utensils are forks OR knives?*

Answer: "Forks or knives" means that we consider both of these sets. We have 4 of each, so there are 8 together. Therefore we have that forks or knives constitute to $\frac{8}{11}$ *of all the utensils.*

If we were asked what fraction of the utensils are "forks and knives", then the answer would be 0, since no utensil is both fork and knive.

Please refer to section 10, where the operations on sets are explained in detail. The notions "or" and "and" are illustrated on the Venn diagrams, which should help to understand them better.

3 What is a proof?

"The search for a mathematical proof is the search for a knowledge which is more absolute than the knowledge accumulated by any other discipline."
Simon Singh

A proof is a sequence of logical statements, one implying another, which gives an explanation of why a given statement is true. Previously established theorems may be used to deduce the new ones; one may also refer to axioms, which are the starting points, "rules" accepted by everyone. Mathematical proof is *absolute*, which means that once a theorem is proved, it is proved for ever. Until proven though, the statement is never accepted as a true one.

Writing proofs is the essence of mathematics studies. You will notice very quickly that from day one at university, lecturers will be very thorough with their explanations. Every word will be *defined*, notations clearly presented and each theorem *proved*. We learn how to construct logical arguments and what a good proof looks like. It is not easy though and requires practice, therefore it is always tempting for students to learn theorems and apply them, leaving proofs behind. This is a really bad habit (and does not pay off during final examinations!); instead, go through the proofs given in lectures and textbooks, understand them and ask for help whenever you are stuck. There are a number of methods which can be used to prove statements, some of which will be presented in the next sections. Hard and tiring at the beginning, constructing proofs gives a lot of satisfaction when the end is reached successfully.

3.1 Writer versus reader

Kevin Houston in his book[2] gives an idea to think of a proof like a small "battle" between the reader and the writer. At the beginning of mathematics studies you will often be the reader, learning the proofs given by your lecturers or found in textbooks. You should then take the **active attitude**, which means working through the given proof with pen and paper. Reading proofs is not easy and may get boring if you just try to read it like a novel, comfortable on your sofa with the half-concentration level. Probably the most important part is to **question** everything, what the writer is telling you. Treat it as the argument between yourself and the author of the proof and ask them "why?" at each step of their reasoning.

When it comes to writing your own proof, the final version should be clear and have no gaps in understanding. Here, a good idea is to think about someone else as the person who would question each of the steps you present. The argument should flow and have enough explanations, so that the reader will find the answer to every "why?" they might ask.

3.2 Methods of proofs

There are many techniques that can be used to prove the statements. It is often not obvious at the beginning which one to use, although with a bit of practice, we may be able to give an "educated guess" and hopefully reach the required conclusion. It is important to notice that there is no one ideal proof - a theorem can be established using different techniques and none of them will be better or worse (as long as they are all valid). For example, in "Proofs from the book", we may find *six* different proofs of the infinity of primes (one of which is presented in section 7). Go ahead and master the techniques - you might discover the passion for pure mathematics!

We can divide the techniques presented in this document into two groups; direct proofs and indirect proofs. Direct proof assumes a given hypothesis, or any other known statement, and then logically deduces a conclusion.

Indirect proof, also called proof by contradiction, assumes the hypothesis (if given) together with a negation of a conclusion to reach the contradictory statement. It is often equivalent to proof by contrapositive, though it is subtly different (see the examples). Both direct and indirect proofs may also include additional tools to reach the required conclusions, namely proof by cases or mathematical induction.

3.3 Implications and if and only if statements

> *"If our hypothesis is about anything and everything and not about one or more particular things, then our deductions constitute mathematics. Thus mathematics may be defined as the subject in which we never know what we are talking about, nor whether what we are saying is true".*
> *Bertrand Russell*

The formula $A \implies B$ means "A implies B" or "if A then B", where A and B are two statements. Saying $A \implies B$ indicates that whenever A is accepted, then we also must accept B. The important point is that the **direction of the implication should not be mixed**! When $A \implies B$, then the argument goes *from* A *to* B, so if A holds, then B does too (we cannot have A without B). On the other hand, when we have that B is accepted, then it does *not* have to happen that A is also accepted (so we can have B without A). This can be illustrated by the following example:

$$\text{it is raining} \implies \text{it is cloudy}.$$

Now, if the first statement is true (so it is raining), then we automatically accept that it is also cloudy. However, it does not work the other way round; the fact that it is cloudy does *not* imply the rain. Notice further, that *accepted* does not mean *true*! We have that if it is raining, then it is cloudy and we accept both statements, but we do not know whether they are actually *true* (we might have a nice sunny day!). Also, genuineness of the second statement does not give any information whether the first statement is true or not. It may happen that the false statement will lead to the truth via a number of implications!

"If and only if", often abbreviated "iff", is expressed mathematically $A \iff B$ and means that if A holds, then B also holds **and vice versa.** To prove the theorems of such form, we must show the implications in both directions, so the proof splits into two parts - showing that "$A \Rightarrow B$" and that "$B \Rightarrow A$". The proof of the statement

$$\text{it is raining} \Leftrightarrow \text{it is cloudy},$$

requires from us showing that whenever it is raining, then it is cloudy **and** showing that whenever it is cloudy, it is always raining.

Necessary and sufficient.

$A \Rightarrow B$ means that A is *sufficient* for B;
$A \Leftarrow B$ means that A is *necessary* for B;
$A \Leftrightarrow B$ means that A is *both* necessary and sufficient for B.

4 Direct proof

4.1 Description of method

Direct proof is probably the easiest approach to establish the theorems, as it does not require knowledge of any special techniques. The argument is constructed using a series of simple statements, where each one should follow directly from the previous one. It is important not to miss out any steps as this may lead to a gap in reasoning. To prove the hypothesis, one may use axioms, as well as the previously established statements of different theorems. Propositions of the form

$$A \implies B$$

are shown to be valid by **starting at** A by writing down what the hypothesis means and consequently approaching B using correct implications.

4.2 Hard parts?

- it is tempting to skip simple steps, but in mathematics nothing is "obvious" - all steps of reasoning must be included;
- not enough explanations; "I know what I mean" is no good - the reader must know what you mean to be able to follow your argument;
- it is hard to find a starting point to the proof of theorems, which seem "obvious" - we often forget about the axioms.

4.3 Examples

Below you will find the theorems from various areas of mathematics. Some of them will be new and techniques used not previously seen by the reader. To help with an understanding, the proofs are preceded by the "rough notes" which should give a little introduction to the reasoning and show the thought process.

Theorem 4.1. *Let n and m be integers. Then*

i. if n and m are both even, then $n+m$ is even,

ii. if n and m are both odd, then $n+m$ is even,

iii. if one of n and m is even and the other is odd, then $n+m$ is odd.

Rough notes. *This is a warm-up theorem to make us comfortable with writing mathematical arguments. Start with the hypothesis, which tells you that both n and m are even integers (for part i.). Use your knowledge about the even and odd numbers, writing them in forms $2k$ or $2k+1$ for some integer k.*

Proof. i. If n and m are even, then there exist integers k and j such that $n = 2k$ and $m = 2j$. Then

$$n + m = 2k + 2j = 2(k + j).$$

And since $k, j \in \mathbb{Z}, (k + j) \in \mathbb{Z}$. $\therefore n + m$ is even.

ii. and iii. are left for a reader as an exercise. □

Theorem 4.2. *Let $n \in \mathbb{N}, n > 1$. Suppose that n is not prime $\implies$ $2^n - 1$ is not a prime.*

Rough notes. *Notice that this statement gives us a starting point; we know what it means to be a prime, so it is reasonable to begin by writing n as a product of two natural numbers $n = a \times b$.*
To find the next step, we have to "play" with the numbers so we receive the expression of the required form.
We are looking at $2^{ab} - 1$ and we want to factorise this. We know the identity

$$t^m - 1 = (t-1)(1 + t + t^2 + \cdots + t^{m-1}).$$

Apply this identity with $t = 2^b$ and $m = a$ to obtain

$$2^{ab} - 1 = (2^b - 1)(1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b}).$$

Always keep in mind where you are trying to get to - it is a useful advice here!

Proof. Since n is **not** a prime, $\exists\ a, b \in \mathbb{N}$ such that $n = a \times b,\ 1 < a, b < n$. Let $x = 2^b - 1$ and $y = 1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b}$. Then

$$\begin{aligned}
xy &= (2^b - 1)(1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b}) && \text{(substituting for } x \text{ and } y\text{)} \\
&= 2^b + 2^{2b} + 2^{3b} + \cdots + 2^{ab} \\
&\quad - 1 - 2^b - 2^{2b} - 2^{3b} - \cdots - 2^{(a-1)b} && \text{(multiplying out the brackets)} \\
&= 2^{ab} - 1 && \text{(taking away the similar items)} \\
&= 2^n - 1. && \text{(as } n = ab\text{)}
\end{aligned}$$

Now notice that since $1 < b < n$, we have that $1 < 2^b - 1 < 2^n - 1$, so $1 < x < 2^n - 1$. Therefore, x is a positive factor, hence $2^n - 1$ is **not** prime number. □

Note: It is **not** true that: $n \in \mathbb{N}$, if n is prime $\implies$ $2^n - 1$ is prime; see the counterexample of this statement in section 4.5.

Proposition 4.3. *Let $x, y, z \in \mathbb{Z}$. If $x + y = x + z$, then $y = z$.*

Rough notes. *The proof of this proposition is an example of an **axiomatic proof**, i.e. the proof that refers explicitly to the axioms. To prove the statements of the simplest form like the one above, we need to find a starting point. Referring to axioms is often a good idea.*

Proof.

$$\begin{aligned}
& x + y = x + z \\
& \implies (-x) + (x + y) = (-x) + (x + z) && \text{(by the existence of additive inverse)} \\
& \implies ((-x) + x) + y = ((-x) + x) + z && \text{(by the associativity of addition)} \\
& \implies (x + (-x)) + y = (x + (-x)) + z && \text{(by the commutativity of addition)} \\
& \implies 0 + y = 0 + z && \text{(by existence of additive inverse)} \\
& \implies y = z.
\end{aligned}$$

□

Proposition 4.4. $\forall x \in \mathbb{Z},\ 0 \times x = x \times 0 = 0$

Rough notes. *Striking theorem seen in the second year lecture! We all know it since our early years, though now is the time to* proove *it! Again, we will refer to the axioms.*

Proof.

$$\begin{aligned} x \times 0 &= x \times (0+0) && \text{(because } 0 = 0+0\text{)} \\ &\implies x \times 0 = x \times 0 + x \times 0 && \text{(by the distributivity)} \\ &\implies 0 + (x \times 0) = x \times 0 + x \times 0 && \text{(by the existence of zero)} \\ &\implies 0 = x \times 0 && \text{(by the cancellation)} \end{aligned}$$

Similarly, $0 = 0 \times x$ (try to prove it yourself!) □

Theorem 4.5. $\frac{n^2+5}{n+1} \to \infty$ *as* $n \to \infty$.

Rough notes. *Before we proceed, we need to recap the definitions.*

Definition 4.1. *A sequence (of real numbers) is a function from* $\mathbb{N}$ *to* $\mathbb{R}$.

Definition 4.2. *A sequence* (a_n) *of real numbers tends to infinity, if given any* $A > 0$, $\exists N \in \mathbb{N}$ *such that* $a_n > A$ *whenever* $n > N$.

The above definitions are the key to proving the statement. We follow their structure, so we assume A *being given and try to find* N *such that* $a_n > A$ *whenever* $n > N$. *Proving statements of this form is not very hard, but requires practice to be able to get the expression of required form. We will "play" with the fraction to make it smaller, which will prove that it tends to infinity.*

Proof. Let $a_n \coloneqq \frac{n^2+5}{n+1}$ and let $A > 0$ be given. Observe that

$$\begin{aligned} a_n \coloneqq \frac{n^2+5}{n+1} &\geq \frac{n^2}{n+1} && \text{(find an expression smaller than } a_n \text{ by taking away 5 in the numerator)} \\ &\geq \frac{n^2}{n+n} && \text{(decrease an expression by increasing the denominator; holds as } n \in \mathbb{N}\text{)} \\ &= \frac{n^2}{2n} && \text{(adding } n\text{s in the denominator)} \\ &= \frac{n}{2} && \text{(cancelling } n\text{s in the numerator and denominator)} \end{aligned}$$

and $\frac{n}{2} > A$ provided that $n > 2A$.

So, let N be any natural number larger that $2A$. Then if $n > N$, we have $a_n > \frac{n}{2} > \frac{N}{2} > A$. Therefore, a_n tends to infinity. □

Lemma 4.6 (Gibb's Lemma). *Assume $(p_1, \dots, p_m)$ is probability distribution and let $(r_1, \dots, r_m)$ be such that $r_i > 0$ $\forall i$ and $\sum_{i=1}^{r} r_i \leq 1$. Then $\sum_i p_i \log \frac{1}{p_i} \geq \sum_i p_i \log \frac{1}{r_i}$.*

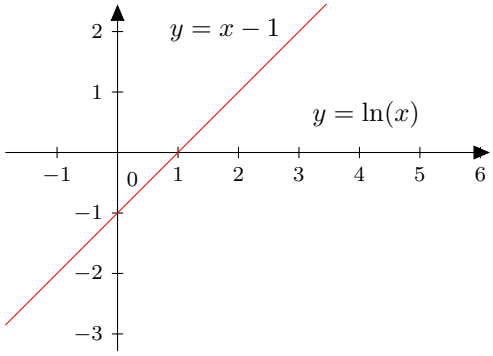
Rough notes. You will probably not see this lemma until year 3, although a year 1 student should be able to prove it, as it requires only manipulations with logs and using simple claims. Notice, that we want to show the equivalent statement:

$$\sum_i p_i \Big(\log \frac{1}{p_i} - \log \frac{1}{r_i} \Big) \geq 0.$$

Then there are just laws of logs and a simple claim that help us to arrive at the statement.

$$\textit{CLAIM: for } x > 0, \ \ln x \leq x - 1.$$

This is illustrated in the sketch below, however the formal proof is given in the appendix.



We now have all the tools needed to write proof of the lemma. See how it works step by step and then check if you can do it yourself!

Proof. We want to show that $\sum_i p_i \Big(\log \frac{1}{p_i} - \log \frac{1}{r_i} \Big) \geq 0.$

Write

$$\begin{aligned}
\sum_i p_i \Big(\log \frac{1}{p_i} - \log \frac{1}{r_i} \Big) &= \sum_i p_i \Big(\log \frac{1}{p_i} + \log r_i \Big) && (\log(a^{-1}) = -\log a) \\
&= \sum_i p_i \Big(\log \frac{r_i}{p_i} \Big) && (\log a + \log b = \log(ab)) \\
&= \frac{1}{\ln m} \sum_i p_i \Big(\ln \frac{r_i}{p_i} \Big) \\
& && \text{(using the fact that } \log_m a = \tfrac{\ln a}{\ln m}\text{; } m \text{ is a base of logarithm)} \\
&\leq \frac{1}{\ln m} \sum_i p_i \Big(\frac{r_i}{p_i} - 1 \Big) && \text{(by the claim)} \\
&= \frac{1}{\ln m} \sum_i \Big(r_i - p_i \Big) && \text{(multiplying out the brackets)} \\
&= \frac{1}{\ln m} \underbrace{\Big(\sum_i r_i}_{\leq 1} - \underbrace{\sum_i p_i \Big)}_{=1} && \text{(by the assumptions)} \\
&\leq 0. && \square
\end{aligned}$$

4.4 Fallacious "proofs"

Example 4.7. Study the sequence of sentences below and try to find what went wrong. You can find the answer in the footnote[1]. We "prove" that $1 = 2$.

BAD "proof"!

$$\begin{aligned} & a = b \\ \implies & a^2 = ab \\ \implies & a^2 + a^2 = a^2 + ab \\ \implies & 2a^2 = a^2 + ab \\ \implies & 2a^2 - 2ab = a^2 + ab - 2ab \\ \implies & 2a^2 - 2ab = a^2 - ab \\ \implies & 2(a^2 - ab) = a^2 - ab \\ \implies & 2 = 1. \end{aligned}$$

Example 4.8. This example will be similar to the previous one (again, we will "prove that $2 = 1$), although it does not contain the same mistake. Try to find what goes wrong here and again, the solution is given at the bottom of the page[2].

BAD "proof"!

$$\begin{aligned} & -2 = -2 \\ \implies & 4 - 6 = 1 - 3 \\ \implies & 4 - 6 + \frac{9}{4} = 1 - 3 + \frac{9}{4} \\ \implies & \left(2 - \frac{3}{2}\right)^2 = \left(1 - \frac{3}{2}\right)^2 \\ \implies & 2 - \frac{3}{2} = 1 - \frac{3}{2} \\ \implies & 2 = 1. \end{aligned}$$

Example 4.9. Below we will present the classic mistake of assuming true the statement which is yet to be proved. The task is to prove that the statement $\sqrt{2} + \sqrt{6} < \sqrt{15}$ is true.

BAD "proof"!

$$\begin{aligned} & \sqrt{2} + \sqrt{6} < \sqrt{15} \\ \implies & (\sqrt{2} + \sqrt{6})^2 < 15 \\ \implies & 8 + 2\sqrt{12} < 15 \\ \implies & 2\sqrt{12} < 7 \\ \implies & 48 < 49. \end{aligned}$$

[1] Notice that we assumed that $a = b$, so $(a^2 - ab) = 0$ and hence we cannot cancel these expressions out! The last step is not correct, hence the "proof" is not valid.

[2] The problem occurs when we take the square root of both sides. Remember that the square root function returns a positive output, however its input might come from a negative number raised to the power: $|x| = \sqrt{x^2}$ and therefore $x = \pm\sqrt{x^2}$. You can check that taking the left hand side negative, we will actually arrive at the true statement.

It may seem that the above argument is correct as we have reached true statement $(48 < 49)$, but this is not the case. It is important to remember that

$$\text{statement } \mathcal{X} \implies \text{true statement}$$

does **NOT** mean that statement $\mathcal{X}$ is necessarily true! We *assumed* that $\sqrt{2} + \sqrt{6} < \sqrt{15}$ is true, where this is what we need to *prove*. Therefore, our implications are going in the wrong direction (go back to section about the implications if you are still confused). Valid proof would be of the form

$$\text{true statement} \implies \text{statement } \mathcal{X}$$

showing that $\mathcal{X}$ is true.

The "proof" above is not correct, however it is not totally useless! Check if you can reverse the implications to obtain the proof we are looking for. Note that it is alright to write arguments in the wrong direction when *finding* the proof but not when *writing* it in the final form.

Reversed implications would give a valid argument, however, presented in its final form might make a reader wonder where did the idea of starting from "$48 < 49$" came from (looks pretty random). Generally, the easier approach would be the proof by contradiction (see section 7).

4.5 Counterexamples

Having in mind a little "writer - reader battle", we should be sceptical about any presented statement and try to find a counterexample, which will disprove the conjecture. It may happen that the theorem is true, so it is not obvious in which direction to go - trying to prove or disprove? One counterexample is enough to say that the statement is not true, even though there will be many examples in its favour.

Example 4.10. *Conjecture: let $n \in \mathbb{N}$ and suppose that n is prime. Then $2^n - 1$ is prime.*

Counterexample: when $n = 11$,

$$2^{11} - 1 = 23 \times 89.$$

Example 4.11. *Conjecture: every positive integer is equal to the sum of two integer squares.*

Counterexample: $n = 3$. All integer squares, apart from $(-1)^2, (0)^2, (1)^2$, are greater than 3 and we need only consider the situation when one of the squares is either 0 or 1. Neither $(3-1)$, nor $(3-0)$ is an integer square. Hence result.

Example 4.12. *Conjecture: every man is Chinese.*

Counterexample: it suffices to find at least one man who is not Chinese.

5 Proof by cases

5.1 Method

Proof by cases is sometimes also called proof by exhaustion, because the aim is to exhaust all possibilities. The problem is split into parts and then each one is considered separately. During lectures you will usually see proofs containing two or three cases but there is no upper limit for the number of them. For example, the first proof of the Four Colour Theorem used 1936 cases. Over the time, mathematicians managed to reduce this number to over 600 - still lots!

It is often very useful to split the problem into many small problems. Be aware though, the more cases, the more room for errors. You must be careful to cover all the possibilities, otherwise the proof is useless!

5.2 Hard parts?

- split the problem wisely - it is sometimes not obvious how to divide the problem into cases;
- a big number of cases may result in skipping one of them in the proof - make sure each possibility is included in your resoning!

5.3 Examples of proof by cases

Theorem 5.1. *The square of any integer is of the form $3k$ or $3k+1$.*

Rough notes. *This is a simple example of the proof, where at some point it is easier to split the problem into 2 cases and consider them separately - otherwise it would be hard to find a conclusion. Start by expressing an integer a as $3q+r, (q, r \in \mathbb{Z})$ and then square it. Then split the problem and show that the statement holds for both cases.*

Proof. We know that every integer[3] can be written in the form: $3q+1$ or $3q+2$ or $3q$.
So let $a = 3q + r$, where $q \in \mathbb{Z}, r \in 0, 1, 2$. Then

$$a^2 = (3q+r)^2 = 9q^2 + 6qr + r^2 = 3\underbrace{(3q^2+2qr)}_{\in\mathbb{Z} \text{ as } q,r\in\mathbb{Z}} + r^2$$

So let $3q^2 + 2qr := k,\ k \in \mathbb{Z}$. We have $a^2 = 3k + r^2$. Now,

case I: if $r = 0$ or $r = 1$, we are done;

case II: if $r = 2 \implies r^2 = 4$ and then $a^2 = 3k + 4 = 3k + 3 + 1 = 3(k+1) + 1$ which is in the required form.

□

Theorem 5.2. *Let $n \in \mathbb{Z}$. Then $n^2 + n$ is even.*

Rough notes. *To show that the expression is even, it may be helpful to consider the cases when n is even and odd - what does it mean?*

Click here to see a video example.

[3]The proof is given in section "Examples of Mathematical Induction"

- *CASE I: n is even (express it mathematically);*
- *CASE II: n is odd;*

now, the simple algebra should bring us to the required conclusion.

Proof. Exercise for a reader □

Theorem 5.3 (Triangle Inequality)**.** *Suppose* $x, y \in \mathbb{R}$. *Then* $|x+y| \leq |x| + |y|$.

Notes. *To split the proof into small problems, we need to recall the modulus function, which is defined using cases:*

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

Then, using the definition, carefully substitute x or $(-x)$ for $|x|$, depending on the case. The triangle inequality is a very useful tool in proving many statements, hence it is worth to study the proof and memorise the inequality - you will see it lots in the future.

Proof.

case I: $x \geq 0, y \geq 0$, so by the definition, $|x| = x$ and $|y| = y$. Hence, $x + y \geq 0$.
So
$$|x+y| = x + y = |x| + |y|$$

case II: $x < 0, y < 0$. So, $|x| = -x, |y| = -y$. Then $x + y < 0$.
So
$$|x+y| = -(x+y) = -x + -(y) = |x| + |y|$$

case III: One of x and y is positive and the other is negative. Without loss of generality, assume that x is positive ($x \geq 0 so |x| = x$) and y is negative ($y < 0, |y| = -y$). Now we need to split the problem into 2 subcases:

i. $x + y \geq 0$,
So
$$|x+y| = x + y \leq x + (-y) = |x| + |y|$$

ii. $x + y < 0$,
So
$$|x+y| = -x + (-y) \leq x + (-y) = |x| + |y|$$

□

6 Mathematical Induction

6.1 Method

How to use it, when to use it? Mathematical induction is a very useful mathematical tool to prove theorems on natural numbers. Although many first year students are familiar with it, it is very often challenging not only at the beginning of our studies. It may come from the fact that it is not as straightforward as it seems.

Formally, this method of proof is referred to as Principle of Mathematical Induction.

Principle of Mathematical Induction

Let $P(n)$ be an infinite collection of statements with $n \in \mathbb{N}$. Suppose that
(i) $P(1)$ is true, and
(ii) $P(k) \implies P(k+1), \forall k \in \mathbb{N}$.
Then, $P(n)$ is true $\forall n \in \mathbb{N}$.

When constructing the proof by induction, you need to present the statement $P(n)$ and then follow three simple steps (simple in a sense that they can be described easily; they might be very complicated for some examples though, especially the induction step):

- **INDUCTION BASE** check if $P(1)$ is true, i.e. the statement holds for $n = 1$,
- **INDUCTION HYPOTHESIS** assume $P(k)$ is true, i.e. the statement holds for $n = k$,
- **INDUCTION STEP** show that if $P(k)$ holds, then $P(k+1)$ also does.

We finish the proof with the conclusion "since $P(1)$ is true and $P(k) \implies P(k+1)$, the statement $P(n)$ holds by the Principle of Mathematical Induction".

Dominoes effect. Induction is often compared to dominoes toppling. When we push the first domino, all consecutive ones will also fall (provided each domino is close enough to its neighbour); similarly with $P(1)$ being true, it can be shown by induction that also $P(2), P(3), P(4), ...$ and so on, will be true. Hence we prove $P(n)$ for infinite n.

6.2 Versions of induction.

Principle of Strong Mathematical Induction

Let $P(n)$ be an infinite collection of statements with $n, r, k \in \mathbb{N}$ and $r \leq k$. Suppose that
(i) $P(r)$ is true, and
(ii) $P(j) \implies P(k+1), \forall r \leq j \leq k$.
Then, $P(n)$ is true $\forall n \in \mathbb{N},\ n \geq r$.

Changing base step. There are different variants of Mathematical Induction, all useful in slightly different situations. We may, for example, prove a statement which fails for the first couple of values of n, but can be proved for all natural numbers n greater than some $r \in \mathbb{N}$. We then change the **base step** of Principle of Mathematical Induction to

"check if $P(r)$ is true, for some $r \in \mathbb{N}''$

and continue with the induction hypothesis and induction step for the values greater or equal than r.

More assumptions. In the hypothesis step, we are allowed to assume $P(n)$ for more values of n than just one. Sometimes to be able to show that the statement $P(k+1)$ is true , you may have to use both $P(k)$ and $P(k-1)$, so assume that both of them are true. In this case the induction base will consist of checking $P(1)$ and $P(2)$. It may also happen that we will deduce $P(k+1)$ once we assumed that *all* $P(1), P(2), \ldots, P(k)$ hold.

Mixture The most complicated case would combine the last two, such that we start the induction base for some $r \in \mathbb{N}$ and then prove that $P(r), P(r+1), P(r+2), ..., P(k-1), P(k)$ imply that $P(k+1)$. Then by induction $P(n)$ is true for all natural numbers $n \geq r$.

6.3 Hard parts?

- the induction hypothesis looks like we are assuming something that needs to be proved;
- it is easy to get confused and get the inductive step wrong. Ethan Bloch [1] gives an example of "proof" by induction which fails to be true - see exercise 6.5.

6.4 Examples of mathematical induction

Example 6.1. *Show that* $2^{3n+1}+5$ *is always a multiple of* 7.

Notes. *This is a typical statement which can be proved by induction. We start by checking if it holds for* $n=1$. *Then if we are able to show that* $P(k) \implies P(k+1)$, *then we know that statement is true by induction.*

Proof. The statement $P(n): 2^{3n+1}+5$ is always a multiple of 7.

- BASE (n=1)
$$2^{3\times 1+1}+5 = 2^4+5 = 16+5 = 21 = 7\times 3$$
$\therefore P(1)$ holds.
- INDUCTION HYPOTHESIS: Assume that $P(k)$ is true, so
$$2^{3k+1}+5 \text{ is always a multiple of } 7, \mathrm{k} \in \mathbb{N}.$$
- INDUCTION STEP: Now, we want to show that $P(k) \implies P(k+1)$, where
$$P(k+1): 2^{3(k+1)+1}+5 = 2^{3k+4}+5 \text{ is a multiple of } 7.$$
We know from induction hypothesis that $2^{3k+1}+5$ is always a multiple of 7, so we can write
$$\begin{aligned}
&2^{3k+1}+5 = 7\times x \text{ for some } x\in\mathbb{Z}\\
&\implies (2^{3k+1}+5)\times 2^3 = 7\times x\times 2^3 && \text{(multiplying by } 2^3\text{)}\\
&\implies 2^{3k+4}+40 = 7\times x\times 8\\
&\implies 2^{3k+4}+5 = 56x-35 && (-35 \text{ from both sides})\\
&\implies 2^{3k+4}+5 = 7\underbrace{(8x-5)}_{\in\mathbb{Z}}
\end{aligned}$$

So $2^{3k+4} + 5$ is a multiple by 7 ($P(k+1)$ holds), provided that $P(k)$ is true.

We have shown that $P(1)$ holds and if $P(k)$, then $P(k+1)$ is also true. Hence by the Principle of Mathematical Induction, it follows that $P(n)$ holds for all natural n.

□

Theorem 6.2 (De Moivre's Theorem)**.** *If $n \in \mathbb{N}$ and $\theta \in \mathbb{R}$, then* $[\cos(\theta) + i\sin(\theta)]^n = \cos(n\theta) + i\sin(n\theta)$.

Notes. The well known De Moivre's Theorem can be easily proved using Mathematical Induction. We show it is true for $n = 2$, remembering the rule for the product of complex numbers:

$$\begin{aligned} z_1 \times z_2 &= r_1(\cos\theta_1 + i\sin\theta_1) \times r_2(\cos\theta_2 + i\sin\theta_2) \\ &= r_1 r_2((\cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2) + i(\sin\theta_1\cos\theta_2 + \cos\theta_1\sin\theta_2)) \\ &= r_1 r_2(\cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2)). \end{aligned}$$

Then we assume the statement is true for $n = k$ and use this assumption to show it holds for $n = k+1$. At the induction step we will need the trigonometric identities:

$$\cos(A+B) = \cos A\cos B - \sin A\sin B,$$

$$\sin(A+B) - \sin A\cos B + \cos A\sin B.$$

Proof. The theorem is true for $n = 1$, trivially.

- BASE ($n = 2$):
$$z^2 = (\cos\theta + i\sin\theta)^2 = (\cos 2\theta + i\sin 2\theta)$$
- INDUCTION HYPOTHESIS: assume that it is true for $n = k$, so
$$[\cos(\theta) + i\sin(\theta)]^k = \cos(k\theta) + i\sin(k\theta).$$
- INDUCTION STEP: Now,

$$\begin{aligned} (\cos\theta + i\sin\theta)^{k+1} &= (\cos\theta + i\sin\theta)^k(\cos\theta + i\sin\theta) \\ &= (\cos(k\theta) + i\sin(k\theta))(\cos\theta + i\sin\theta) && \text{(by the induction hypothesis)} \\ &= \cos(k\theta)\cos\theta + i\cos(k\theta)\sin\theta + i\cos\theta\sin(k\theta) - \sin(k\theta)\sin\theta \\ & && \text{(multiplying out the brackets)} \\ &= \cos(k\theta+\theta) + i\sin(k\theta+\theta) && \text{(follows from the trigonometric identities)} \\ &= \cos(k+1)\theta + i\sin(k+1)\theta && \text{(taking } \theta \text{ outside the bracket)} \end{aligned}$$

Hence we have shown that $P(1)$ and $P(2)$ hold and $\forall k \geq 2, P(k) \implies P(k+1)$. Therefore $P(n)$ is true $\forall n \geq 2$ by the Mathematical Induction. □

Proposition 6.3. *Let* $a_{n+1} = \frac{1}{5}\left(a_n^2 + 6\right)$ *and* $a_1 = \frac{5}{2}$. *Then* (a_n) *is decreasing.*

Notes. *We have defined a sequence earlier and here is the definition of the* decreasing *sequence.*

Definition 6.1. *A sequence* (a_n) *is decreasing if* $a_{n+1} \leq a_n$ *for all* $n \in \mathbb{N}$.

We will use the definition to prove the statement. Notice that we need to show $a_{n+1} \leq a_n$ *for all* n *- this should suddenly bring to your mind induction.*
As always, we start by checking the base, (here for $n = 1$*) and then we assume that* $P(n)$ *is true for* $n = k$. *The hard part is usually the induction step, although it is not very complicated here. That we want to show that* $a_{k+2} \leq a_{k+1}$ *using our previous assumption.*

Proof. We will show that the statement $P(n)$ holds for all n.

$$P(n) : a_{n+1} \leq a_n \text{ for all } n.$$

- BASE:
$$a_n = \frac{1}{5}\left(\left(\frac{5}{2}\right)^2 + 6\right) = \frac{1}{5}\left(\frac{25}{4} + 6\right) = \frac{49}{20}.$$
Note: $a_2 = \frac{49}{20} < \frac{5}{2} = a_1$. Hence, $P(1)$ holds.
- HYPOTHESIS: Suppose that for some $k \leq 1, a_{k+1} \geq a_k$.
- INDUCTION STEP:
$$\begin{aligned} a_{k+2} &= \frac{(a_{k+1})^2}{5} + \frac{6}{5} \\ &\leq \frac{(a_k)^2}{5} + \frac{6}{5} \\ &= a_{k+1}. \end{aligned}$$

Hence $a_{k+2} \leq a_{k+1}$.
Since $P(1)$ is true and $P(k) \implies P(k+1)$, it follows that the sequence is decreasing by the Mathematical Induction. □

Exercise 6.4. *For which positive integers* n *is* $2^n < n!$ *?*

Notes. *Notice that this is a different example to the ones we have presented above. Here, you must find* n *first and then show that it actually holds. You may want to check the first couple of values of* n *and then formulate the statement* $P(n)$ *for which you can use Induction. Structure your proof as above, the notes on side should also help.*

Click here to see a video example.

Proof. First, let us find the value of n for which we will prove the statement.

(does the statement hold for $n = 1, 2, 3, \ldots$? Have you found n for which this is true?)

Let $P(n) : 2^n < n!$ be the statement. We will show that it holds for all $n \geq \ldots$

- BASE STEP

  (show $P(n)$ holds for n smallest possible)

- INDUCTION HYPOTHESIS $P(k) : \ldots$

  (state the assumption for $P(k)$)

- INDUCTION STEP

  (keep in mind what you are trying to prove - it helps to note it on the side)

  (hint: notice that $2 < k + 1$ $\forall k > 1$)

- CONCLUSION

  (finish the proof by writing the conclusion)

□

Exercise 6.5. Use Principle of Mathematical Induction to show that $\left(\bigcup_{k=1}^{n} A_k\right)' = \bigcap_{k=1}^{n} A_k'$ $\forall n \geq 2$.

The above theorem is one of the De Morgan's laws for an arbitrary collection of subsets (see section on sets for De Morgan's Laws in case of two subsets). Below there are two examples of the first year students' approach to prove this theorem by mathematical induction. Have a look at their work (figures 1 and 2). Can you see which student's work gained more marks and why? Are all the steps of induction correct?

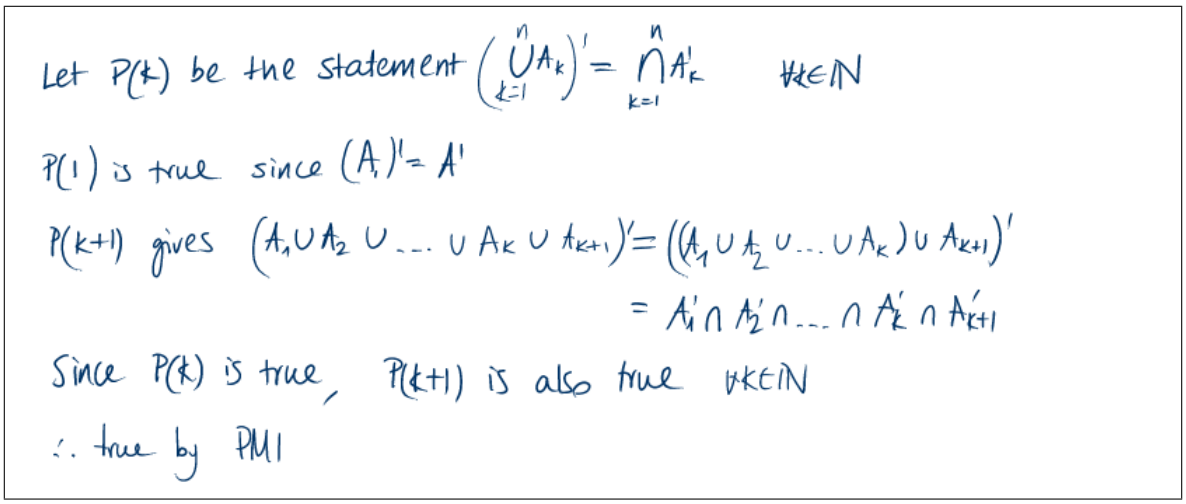


Figure 1: Proof by induction attempted by student A

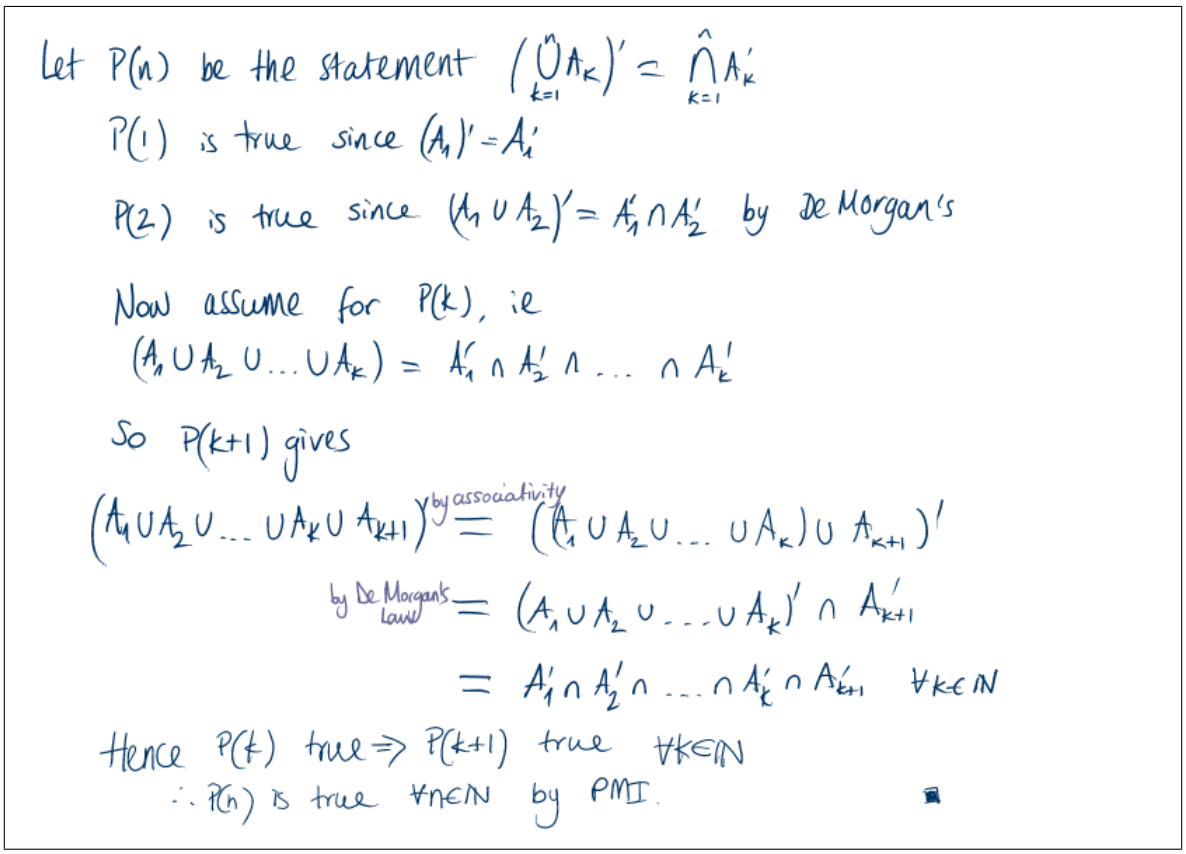


Figure 2: Proof by induction attempted by student B

Two "proofs", both written by first year students, are a good example to see why the induction is hard. The fact that the argument looks as if it contains all the required steps, like base, hypothesis

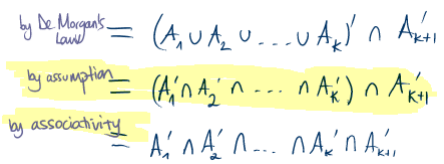
and induction step, does not make it correct proof. We will now analyse both arguments and point out where the problems are. You have probably spotted already that the proof written by student B is much better. It received 4 out of 5 points, because the argument flows well and contains all required parts of induction, though the induction step needs more explanation. You must also watch the details closely, because the statement is proved for $n \geq 2$, so this should be mentioned in our conclusion. Student A received 0 marks for their work and the details are discussed below.

STUDENT A:

- the argument starts with the wrong statement - we want to state $P(n)$ at the beginning, so prove the equality in terms of n;
- De Morgan's Laws are necessary to show that base step holds and it should be checked for n=2, because we are proving the statement for all $n \geq 2$;
- there is hypothesis stated clearly;
- induction step is not stated properly - steps are missing when deducing $P(k+1)$;
- conclusion is incorrect as it was not in fact shown that $P(k) \implies P(k+1)$.

STUDENT B:

- it is not necessary to check $P(1)$ since we are proving $P(n)$ for $n \geq 2$;
- induction step is missing one line of argument, we should not "jump" to the required form straight away but show all reasoning (the highlighted step is missing);



- in the conclusion "$P(k) \Rightarrow P(k+1)$ true $\forall k \in \mathbb{N}$", we should also add "$k \geq 2$".

Exercise 6.6. In Bloch's book[1] we read an argument, which clearly fails at some point. It is hard to detect the mistake though and it seems that induction is correct. See if you can spot a problem - the answer is given in a footnote[4].

BAD "proof"!

Proof. $P(n)$: in any collection of n horses, all of them have the same colour.

Since there are finite number of horses in the world, the statement means that all horses in the world have the same colour!

- BASE (n=1): $P(n)$ clearly holds as in any group of only 1 horse, it is trivially true that "all horses have the same colour"
- HYPOTHESIS: Now we assume that $P(k)$ holds, so in any group of k horses, it is true that all of them have the same colour.
- INDUCTION STEP: Now imagine a collection of $k+1$ horses, let's call it $\{H_1, H_2, \ldots, H_{k+1}\}$. Now, if we take the first k of them, then by induction hypothesis we know that they are all of the same colour. We may also consider another set of k horses $\{H_2, H_3, \ldots H_{k+1}\}$ which, again, are all of the same colour. Since $\{H_1, H_2, \ldots, H_k\}$ and $\{H_2, H_3, \ldots H_{k+1}\}$ all have the same colour, then we may deduce that all $k+1$ horses have the same colour. Hence all horses have the same colour.

Since $P(1)$ holds and $P(k) \implies P(k+1)$, we have that $P(n)$ is true for all natural n by the Principle of Mathematical Induction. □

[4]The problem lies in an inductive step which will fail for some particular value of n. So if we take n big enough, then we may not be able to find set of n horses, where all would have the same colour

7 Contradiction

7.1 Method

Proof by contradiction is a very powerful technique, but the method itself is simple to understand.

When trying to prove

$$\text{statement } A \implies \text{statement } B,$$

assume that A is true and that **not** B is true and try to reach a contradiction.

The method is often used in proofs of the existence theorems, so the statements of the form "there is no x such that…". Here, instead of proving that something does not exist, we can assume that it does and try to reach nonsense. We finish the proof with the word "contradiction!", where some people prefer the lightning symbol or a double cross (see section 2 on symbols) to indicate that they reached the contradiction.

7.2 Hard parts?

- when proving more complex theorems, it is easy to get confused and make a mistake. Then we arrive at contradiction, which does not come from the original assumption but form the error in the middle of the proof.

7.3 Examples of proof by contradiction

Theorem 7.1. *Let a be rational number and b irrational. Then*

i. $a+b$ is irrational

ii. if $a \neq 0$, then ab is also irrational.

> Notes. *First of all we need to recall what it means to be rational (can be expressed as a fraction) or irrational (cannot be expressed as a fraction). So if we want to show that $a+b$ is irrational, we do not really know how to describe it generally. Instead, we may assume the opposite, express it as a rational number (which is easy to do in general) and show that it leads to a contradiction. Notice how a big role the definitions play when constructing the proof!*

Proof. i. Suppose that $a+b$ is rational, so $a+b := \frac{m}{n}$. Now, as a is rational, we can write it as $a := \frac{p}{q}$. So

$$b = (a+b) - a = \frac{m}{n} - \frac{p}{q} = \frac{mq - pn}{nq},$$

hence b is rational, which contradicts the assumption.

ii. left as an exercise

□

Exercise 7.2. *Prove that $\sqrt{2} + \sqrt{6} < \sqrt{15}$*

Notes. *We have seen this statement before as an example of "fallacious proof" and now we will show how to prove such expressions using contradiction. It has been shown that it is easy to fall in the trap of assuming that the statement is true and then arguing from there; it is popular mistake probably because there is no other "starting point" that seems sensible. To avoid the mistake of assuming of what has to be proved, it is better suppose the opposite of a given statement. If we reach a contradiction, then our assumption was wrong and the statement is proven true.*

Proof. Assume for a contradiction that $\sqrt{2}+\sqrt{6} \geq \sqrt{15}$

$$\begin{aligned} &\implies (\sqrt{2}+\sqrt{6})^2 \geq 15 \\ &\implies 8+2\sqrt{12} \geq 15 \\ &\implies 2\sqrt{12} \geq 7 \\ &\implies 48 \geq 49 \end{aligned}$$

The last statement is clearly not true, hence we reached the contradiction. Therefore, we proved that $\sqrt{2}+\sqrt{6} < \sqrt{15}$. □

Theorem 7.3. *Let $f : A \to B$ and $g : B \to C$ be functions. If $g \circ f$ is bijective, then f is injective and g is surjective.*

Notes. *Refer to the section on functions to recall that "bijective" means "injective and surjective" - have a look at the definitions in section 11, because again these will help to construct the proof. Now, you may want to start with the statement "$g \circ f$ is bijective" and follow from there, however it may be hard to conclude that f is injective and g is surjective. The quickest way to bring us to the required statement is to assume the opposite and try to reach the contradiction.*

Proof. Suppose the statement does not hold, so f is not injective or g is not surjective. Let us consider both cases:

- f is not injective, which means that $\exists\ a, a' \in A$ such that $f(a) = f(a')$.

  Now,
  $$(g \circ f)(a) = g(f(a)) = g(f(a'))$$
  so we have $(g \circ f)(a) = (g \circ f)(a')$ but $a \neq a'$. So $g \circ f$ is not injective, hence it is not bijective.

- g is not surjective, which means that $\exists c \in C$ such that for all $b \in B$, $g(b) \neq c$. Moreover, $g \circ f$ is surjective, so $\exists a \in A$ such that $(g \circ f)(a) = c$. Now, if $b = f(a)$, then $g(b) = c$, which is a contradiction!

Both cases lead us to the contradiction, hence we may conclude that if $g \circ f$ is bijective, then f is injective and g is surjective. □

Theorem 7.4. *There are infinitely many primes.*

Notes. *Having seen many theorems and proofs, let us try to prove the famous theorem stating the infinity of primes. This comment should guide you to writing the statements in the mathematical language - do not worry if you don't get it first time; a final proof often needs changing and polishing a few times!* ***Click here to see a video example.***

Proof. Suppose for a contradiction that...

(write the statement)

Since... *(insert the statament)* ,we can list them: ...

(list the primes - you need to pick a suitable notation)

Now, consider the number n, which is *not* a prime.

(you can define this number in many different ways, but you need a number which is not a prime (consider multiplying all the listed primes by each other - then n is greater that any of them) and that leads us to the contradiction (this is a tricky part) - we may want to come back to this point later, because the next lines of the argument should help us to pick appropriate n here)

Since n is *not* a prime,...

(what does it tell us? Write down what does it mean mathematically that n is not a prime. Think about the factor of n - what if we take it the smallest possible?)

Take the factor the smallest possible, so it is prime.

Now, it follows that $\exists z \in \mathbb{Z}$, such that

$$n = z \times \ldots, \tag{1}$$

hence

$$z = \frac{n}{\ldots} = \frac{\ldots}{\ldots} \tag{2}$$

At this stage, we can get the contradiction to our assumption, but it depends on our choice of n. Let us come back to the definition of n - what would guarantee it? What did we assume about the factor of n? What assumptions did we state at the equation(1)? Try to change n slightly if your argument does not reach the contradiction yet.

□

8 Contrapositive

8.1 Method

Proof by contrapositive is in essence a "submethod" of a proof by contradiction. The argument begins in the same way in both cases, by assuming the opposite of the statement. So when showing that

$$\text{statement } A \implies \text{statement } B,$$

we assume "not B", but this time we argue to arrive at "not A". The trick here is the fact that the statements "$A \implies B$" and "not $B \implies$ not A" are **equivalent**.

To understand this relationship better, you may want to read more about the Wason selection task, which is the logic puzzle formulated by Peter Wason in 1966. The example below is based on his work and it illustrates very well the reasoning used in proof by contrapositive.

Imagine four cards placed on the table, each with a letter on one face and a number on the other one.

A	D	9	5

You are given the rule which states: "if A is on a card, then 5 is on its other side". Now, the task is to indicate which card(s) need to be turned over to check whether the rule holds?

While most of the people give the automatic response "A" and "5", the correct answer is "A" and "9". Notice that according to our rule, if the card shows "A" on one face, it must have "5" on the other. The rule however does not say anything about the card showing "5"!

Hence, only checking "A" and "9" can test the rule:

- if A does *not* have 5 on the other side, the rule is broken;
- if D has (or not) 5 on the other side - it does not tell us anything;
- if 5 has (or not) A on the other side - again, the rule is not broken;
- if 9 *does* have A on the other side - the rule is broken.

8.2 Hard parts?

- the method itself requires the knowledge of the fact "$A \Rightarrow B$" is equivalent to "not $B \Rightarrow$ not A";
- similarly as in the proof by contradiction, the theorems proved may be complex and it is easy to make mistakes and arrive at the incorrect conclusion.

8.3 Examples

Theorem 8.1. *Let $n \in \mathbb{Z}$. If n^2 is odd, then n is odd.*

Notes. The direct proof would not really work here, because writing n^2 in the form $2k+1$ (for some $k \in \mathbb{Z}$) does not really help to continue. Neither is the contradiction useful, as we cannot find the required conclusion. In this case we need a special technique, which is the contrapositive. This means that we start by assuming the opposite of the statement (here: "n is NOT odd") and then use the fact that

$$A \implies B \text{ is equivalent to: } \text{not } B \implies \text{not } A.$$

In this example statement A is: "n^2 is odd" and B: "n is odd".

Proof. Let n be even *(which is "not B")*.

$$\begin{aligned} &\implies n = 2k, k \in \mathbb{Z} \\ &\implies n^2 = (2k)^2 = 4k^2 = 2 \times 2k^2 \\ &\implies n^2 \text{ is even} \end{aligned}$$

(up to this point we proceed as we would in the proof by contradiction, although the conclusion would be: n even $\implies$ n^2 even, which is not what we are trying to prove)

So we proved that n is even $\implies$ n^2 is even. Now using the contrapositive we conclude that

$$n^2 \text{not even (odd)} \implies n \text{ not even (odd)},$$

which proves the statement. □

Theorem 8.2. *If mn is odd, then m and n are odd.*

Notes. Representing mn as an odd integer does not really give us any tips on how to carry on with our proof. Much easier thing is to assume the opposite of the second part of the statement and see where we arrive at - is it contradiction? Or opposite of the first part of the statement? We have the tools to arrive at the conclusion in any case, so let us see where will our assumption get us to.

Click here to see a video example.

Proof. Assume that ... , so m and n are....

(assume "not B")

So $m = 2 \times \ldots, \ldots \in \mathbb{Z}$ and $n = 2 \times \ldots, \ldots \in \mathbb{Z}$.

Now, $mn = \ldots \times \ldots = \ldots$

(substitute for m and n)

Hence, we conclude that...

(you should arrive at "not A")

So, by contrapositive, ...

(remember "not B $\implies$ not A" $\equiv$ "A $\implies$ B")

□

9 Tips

"Proofs are hard to create - but there is a hope."
K. Houston

This section has been created with help of lecturers from the University of Birmingham who took part in a short survey, so the problems and common mistakes in areas of pure mathematics could be detected. All the quotations throughout this section come from the short questionnaire. Many good tips have also been found in [1] and [2] and the reader is strongly advised to look into this literature. It is good to find out what the common mistakes are, and to watch out closely and try to avoid them.

Writing proofs is hard. It often requires a good amount of time and paper, before the neat proof is finally produced. You will find yourself crossing things out and changing it many times before you reach what is required. Making mistakes is natural and it is better to think about them as a *"step in learning to write proofs. Writing proofs in pure mathematics university courses is different from what has been done during school, so it will take some time to get used to doing this properly."*

9.1 What common mistakes do students make when trying to present the proofs?

Misunderstanding of definitions The absolute number one problem mentioned by most lecturers taking part in a survey is the fact that students do not learn definitions. It is important to be on track of the terminology - there will be a lot of it, so it will be hard to learn it all if you leave it for later!

> *"(Students) do not know where to start because they do not know the definitions of the objects they are working with"*

Not enough words Lecturers are *waiting* for your words! Prioritising symbols to words especially at the beginning of mathematics studies is a common mistake, because it seems like a page with lots of symbols "looks clever".

> *"I have found it common in particular for first year students not to explain the steps in their arguments, as if they think they are not allowed to use words, only symbols"*

Lack of understanding

> *"When a student gets to a point in a proof that they cannot proceed from, often the conclusion of the result follows immediately, and it is clear that the student does not understand the necessary missing arguments"*

> *"They are trying to memorise the proofs rather than understand them"*

Incorrect steps Although your argument should start at the beginning and then lead to the final statement, while constructing the proof you may want to look at the conclusion and imagine how it may be arrived from the hypothesis. You may then be able to reverse the steps to produce a good proof - not always though, be careful! Another idea is to work from both ends (both from the beginning and from the end) and "meet" somewhere in the middle. This is all allowed during constructing the proof but remember to then produce a neat final version with all steps well explained. Good knowledge of different methods of proofs is also essential.

> *"Contradiction arguments often have incorrect conclusions; induction arguments often start at the incorrect point, and the induction hypothesis is often abused'*

9.2 What are the reasons for mistakes?

Again we come back to definitions, as incorrect arguments may come from the fact that students *"do not appreciate the importance of mathematical definitions"*. Sometimes we lack the motivation and sometimes also ability, hence practise is key to success. Mistakes may also come from the fact that *"school maths does not prepare students adequately in how to present a mathematical argument"*. A good method to develop mathematical reasoning is to create your own examples on which you can practice writing proofs. How many teachers challenge their students in this way though? How much is there of *understanding* maths and how much of getting the required grade?

"Additionally, students are often asked questions which have 'nice looking answers' and the final steps of a calculation can be somewhat guessed to obtain an answer that looks correct. However, it is very difficult to guess parts of a proof correctly". It seems that there is no *"magic fix for this, other than practice and feedback"*. Finally though, *"this should not necessarily be considered a mistake rather a step in learning. Writing proofs in pure mathematics university courses is different from what has been done during school, so it will take some time to get used to doing this properly"*.

9.3 Advice to students for writing good proofs

Here are the tips collected together, which come from the lecturers at University of Birmingham. Have a look at what they think and what they are looking for when marking your work!

> *"Often you'll need to do some rough work to figure out how your proof should go. Some of the time, you will be able to get a good idea of how a proof should go by noticing that it can be similar to the proof of something else."*
>
> *"Understand every line that you write, and do not make bogus claims."*
>
> *"Understanding the proofs in the lectures/ lecture notes as a way of understanding of the type of reasoning that is involved in a proof."*
>
> *"How you lay out a proof is at least as important as the content (it's not ok if 'it's all in there somewhere')."*
>
> *"Try to make your proofs easier to follow by including brief phrases where appropriate. For example rather than writing (statement A) implies (statement B) it may be more enlightening to write (statement B) follows from (statement A) because..."*
>
> *"Try to write out many of them, understanding every step. Ask others about unclear points. Try to follow proofs in class or in books, and ask about unclear points."*

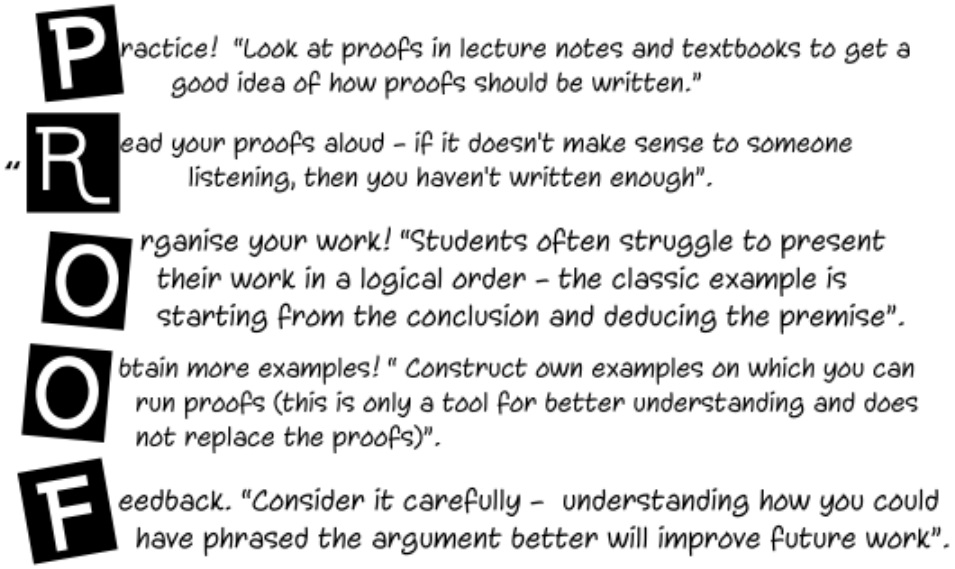
9.4 Friendly reminder

> ***"The importance of proofs goes well beyond a university degree. It is eventually about using reason in everyday life. This could contribute to solving major and global problems."***

You have seen many methods of proofs presented in previous sections and they are all used in different areas of mathematics. It has been underlined many times that writing proofs is not easy, but with a lot of practice and open mind, pure mathematics is not as scary. Here are some final tips to keep in your head when starting the next proof. Good luck!

- Experiment! If one method does not work, try a different one. Lots of practice allows for an "educated guess" in the future;
- do not start with what you are trying to prove;

- use correct English with full punctuation;
- begin by outlining what is assumed and what needs to be proved; do not skip this step!
- remove initial working when writing up the final version of the proof, but include all steps of reasoning.



10 Sets

10.1 Basics

To be able to write well in mathematical language, you will need at least the basics of the set theory. Most lecturers will assume that you know it, or will include it in the "zero chapter" in their lecture notes, so you must know all these definitions and symbols before you start working on your first proofs.

Definition 10.1. A **set** is a collection of objects, which are called the elements or members of a set.

Sets are usually denoted by capital letters and the members by lower case letters. We usually write all elements in curly brackets. The notation

$$A = \{a, b, c\}$$

means that the set A consists of 3 elements: a, b and c. We can say that the element a belongs to the set A, write $a \in A$, or that d is not a member of A, write $d \notin A$.

Example 10.1. *Examples of the sets:*

$$B = \{1, 2, 3\},\ C = \{0\},\ D = \{x, y, \emptyset\},\ E = \{\{red, white\}, blue\},\ F = \{-1, 0, \cos\pi, 1\}.$$

Note: the order of the elements in a set does NOT matter, i.e. $\{2, 3, 1\}$ is exactly the same as set B in the example given above. Observe also the difference between the sets $E = \{\{red, white\}, blue\}$ and $\{red, white, blue\}$. Here *blue* is an element of both sets, but $red \notin E$. We have that $\{red, white\} \in E$. So a set can be an element of another set.

The symbol $\emptyset$ represents the **empty set**, which contains no elements. Note that $\{\emptyset\}$ is NOT an empty set!

10.2 Subsets and power sets

Definition 10.2. If A is a **subset** of B (write $A \subseteq B$), then all elements of A are also elements of B; $A \subseteq B \Leftrightarrow \forall x \in A, x \in B$. So A is "contained" in B.

If you want to say that A is NOT subset of B, write mathematically $A \nsubseteq B$.

Example 10.2.

$$\{1, 10\} \subseteq \{1, 10, 100\},$$
$$\{1000, 10\} \nsubseteq \{1, 10, 100\},$$
$$\emptyset \subseteq \{\emptyset\}.$$

Notice that the empty set is a subset of any set.

To show that $A \subseteq B$, you need to show that *every* element of A is also an element of B.

We will present a very simple theorem and its proof. It should give you an idea of how to structure your argument. Note the amount of *words* used!

Theorem 10.3. *Let A, B and C be sets. Then*

(a) $A \subseteq A$

(b) If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof. (a) Start by choosing an arbitrary element $a \in A$ (we mean A on the left hand side of "$A \subseteq A$"). Then it follows that $a \in A$ (A on the left right side).
We chose a arbitrarily, hence the argument holds for all $a \in A$. So by the definition of a subset, $A \subseteq A$.

(b) Let $a \in A$. Then, since $A \subseteq B$, it follows that $a \in B$. Since $B \subseteq C$, we have that $a \in C$.
So $a \in A$ implies $a \in C$. Therefore $A \subseteq C$. □

If A is a subset of B but it they are not equal, then we say that A is a **proper subset** of B and write it $A \subset B$ (or $A \subsetneq B$ or $A \subsetneqq B$).

To show that A is a *proper* subset of B, you need to show that $A \subseteq B$ and find at least *one* element of B which is not an element of A.

Example 10.4.

$$\{a, b, c\} \subset \{a, b, c, d\},$$
$$\{1, 2, 3\} \not\subset \{1, 2, 3\} \textit{ but } \{1, 2, 3\} \subseteq \{1, 2, 3\}.$$

Definition 10.3. The **power set** of a set A consists of all subsets of A and is usually denoted by $\mathcal{P}(A)$ (some writers use 2^A).

The power set of $A = \{x, y, \emptyset\}$ is $\mathcal{P}(A) = \{\{x\}, \{y\}, \{\emptyset\}, \{x, y\}, \{x, \emptyset\}, \{y, \emptyset\}, \{x, y, \emptyset\}, \emptyset\}$.

10.3 Cardinality and equality

Definition 10.4. In mathematics, the **cardinality** of a set A ($card(A)$ or $|A|$) is a measure of the "number of the elements of the set"[5].

Example 10.5. *If* $A = \{a, b, c\}$, *then* $|A| = 3$.

Example 10.6. *Important to notice:*

$$|\{\emptyset\}| = 1, \textit{ while } |\emptyset| = 0.$$
$$|\{0\}| \neq 0, \textit{ but } |\{0\}| = 1.$$

Notice that the repetitions are ignored when we are counting the members of the set. The convention is to list each element only once, however as you see in the Example 4.1. the same number can be written in different forms.

$$F = \{-1, 0, 1, \cos\pi\} = \{-1, 0, 1\}, \text{ as } \cos\pi = -1. \text{ Hence, } |F| = 3.$$

Definition 10.5. Two sets A and B are **equal** when they have exactly the same elements, i.e. every element of A is an element of B and every element of B is an element of A. So

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

Example 10.7.

$$\{-1, 0, 1\} = \{-1, 0, 1, \cos\pi\},$$
$$\{2, 3, 3, 3, 3, 2, 3, 2, 2\} = \{2, 3\},$$
$$\{2, 3, 4\} = \{4, 2, 3\}.$$

[5]This works for finite sets - see section 4.6. for the cardinality of the infinite sets

To show that two sets A and B are equal, pick an arbitrary $x \in A$ and show that $x \in B$ and vice versa.

Exercise 10.8. Let $A = \{1, 2, 3, 4\}$ and $B = \{x : x \in \mathbb{N}, x^2 < 17\}$, where $\mathbb{N}$ is the set of natural numbers. Show that $A = B$.

Answer. To prove the equality of the sets, we must show that for every x,

$$x \in B \Rightarrow x \in A \ (B \subseteq A)$$

and

$$x \in A \Rightarrow x \in B \ (A \subseteq B).$$

So if $x \in B$, then $x^2 < 17$, which implies $x < \sqrt{17}$. Therefore $x \leq 4$. Since x is a positive integer, therefore for every $x \in B$ we have that $0 < x \leq 4$. Hence, $x \in B \Rightarrow x \in A$.

Now assume $x \in A$, so $x \in \{1, 2, 3, 4\}$. To prove that $x \in B$, it suffices to show that the *largest* element $x \in A$ satisfies $x^2 < 17$. Then it is also true for the smaller values since they all belong to $\mathbb{N}$.

Since $\forall x \in A, x^2 \leq 4^2 \leq 16 < 17$, we have that $x \in A \Rightarrow x \in B$.

Exercise 10.9. Show that $\{(\cos t, \sin t) : t \in \mathbb{R}\} = \{(x, y) : x^2 + y^2 = 1\}$.

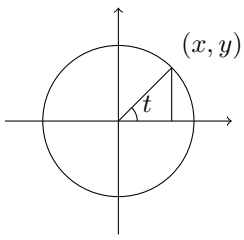
Answer. Let $A = \{(\cos t, \sin t) : t \in \mathbb{R}\}$ and $B = \{(x, y) : x^2 + y^2 = 1\}$. Now, to show that $A = B$ we need to show that $A \subseteq B$ and $B \subseteq A$.

Let $x = \cos t$ and $y = \sin t$. Then

$$x^2 + y^2 = \cos^2 t + \sin^2 t = 1$$

because $\cos^2 t + \sin^2 t = 1$ is a known identity. Hence we have that $A \subseteq B$.

Now, to show that $B \subseteq A$ we appeal to geometry. Let $(x, y) \in B$, hence $x^2 + y^2 = 1$. So (x, y) lies on the unit circle.



Therefore, we have that $\cos t = x$ and $\sin t$=y. As $x^2 + y^2 = 1$, substituting in for x and y gives

$$\cos^2 t + \sin^2 t = 1$$

and hence we have shown that $B \subseteq A$ and so $A = B$.

10.4 Common sets of numbers

The commonly used sets of numbers are:

- The set of natural numbers, $\mathbb{N} = \{1, 2, 3, 4...\}$. Careful! Some mathematicians include 0 in $\mathbb{N}$,

the others do not. Your lecturers will usually tell you at the beginning which version do they mean by writing $\mathbb{N}$;

- The set of integers, $\mathbb{Z} = \{-3, -2, -1, 0, 1, 2, 3, 4, ...\}$;
- The set of rational numbers $\mathbb{Q} = \{\frac{m}{n} : m, n \in \mathbb{Z}, n > 0\}$;
- The set of real numbers $\mathbb{R}$, which is the union[6] of both rational $\mathbb{Q}$ and irrational numbers (which cannot be expressed as a fraction, for example $\log 2, \sqrt{2}, \pi, e$).

Notice that one set is a subset of another, in the following order: $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.

10.5 How to describe a set?

As mentioned before, we write the elements of a set inside curly brackets. The elements should be defined clearly, for example

$$\{x \in \mathbb{R} : 2 < x < 3\}.$$

Notice that it is often tempting to write just $\{2 < x < 3\}$, but it is meaningless! Naturally, x being a natural number rather than a real number makes a big difference! Hence, make sure that you define your sets properly. It may give rise to a very long and scary looking sentence with lots of notation, but there will be no room for ambiguity.

We can represent the intervals on the real number line using set notation. Let $a, b \in \mathbb{R}$ be any two numbers with $a < b$. Then we can define the following:

closed interval	$[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$
open interval	$(a, b) = \{x \in \mathbb{R} : a < x < b\}$
half open intervals	$[a, b) = \{x \in \mathbb{R} : a \leq x < b\}$
	$(a, b] = \{x \in \mathbb{R} : a < x \leq b\}$
infinite intervals	$[a, \infty) = \{x \in \mathbb{R} : a \leq x\}$
	$(a, \infty) = \{x \in \mathbb{R} : a < x\}$
	$(-\infty, b] = \{x \in \mathbb{R} : x \leq b\}$
	$(-\infty, b) = \{x \in \mathbb{R} : x < b\}$
	$\mathbb{R} = (-\infty, \infty)$

It is important to understand that ∞ is *not* a real number! It is a symbol to represent the fact that the interval goes on forever, hence infinity is a concept rather than a big numerical value. Notice that no interval is closed at ∞ or $-\infty$, as there is no *number* there to be included in the real line.

10.6 More on cardinality

We have seen earlier the definition, stating that the **cardinality** of a set is a measure of the "number of the elements of the set". This is indeed the case when the sets, say A and B, are **finite**, i.e. they consist of a finite number of elements. Then the notion $|A| = |B|$ means the equality of integers. Do not confuse it with $A = B$, which means that not just a *number* of the elements is the same, but *elements* themselves are equal.

The problem arises when we consider the infinite sets. The number of their elements is not finite and so we cannot count them and arrive at finite number. In this case we say that two sets A and B have the same cardinality whenever we can match, or pair off, the elements of the set A with the elements of the set B. Put more exactly, two sets A and B have the same cardinality whenever there is a bijection[7] between A and B.

[6] See section 10.7

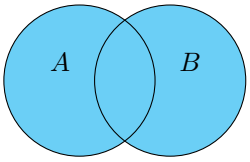
[7] One-to-one correspondence or bijection - see section 11

For example, given set $A = \{1, 2, 3\}$, its cardinality equals 3 ($card(A) = 3$). It is more complicated to talk about the cardinalities of the sets of, say, real or natural numbers. It automatically brings up the interesting discussion about infinity and its different sizes (!). One of the most striking theorems of set theory was proved in 1878 by George Cantor, who stated that $card(\mathbb{R}) = card(\mathbb{R}^2)$. The proof to this powerful statement is quite simple (see appendix), but who would have thought that a straight line has *as many* points as the plane?

10.7 Operations on sets

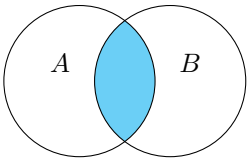
Below we present the basic operations on sets, which can be nicely presented on the Venn diagrams.

- Unions



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

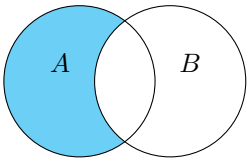
- Intersections



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

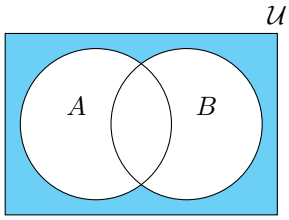
note: when $A \cap B = \emptyset$, then A and B are said to be **disjoint**.

- Complements



$A \backslash B = \{x \in A : x \notin B\}$

The above notation is sometimes called a **relative complement of B in A**. We also distinguish the **universal complement** or simply a **complement**, $\mathcal{U} \backslash A$ (denoted by A' or A^c).



$A^c = \{x : x \notin A\}$

Here $\mathcal{U}$ is the **universal set**, which contains all objects, including itself. Notice that $\mathcal{U}$ must be specified (which is very often omitted) for A^c to be well-defined[8].

[8] well-defined means that the expression is unambiguous, so it has a unique value or interpretation assigned to it

- Cartesian Product
$$A \times B = \{(a, b) : a \in A \text{ and } b \in B\}$$
Note, that here (a, b) is not an open interval , but an **ordered pair**, which is a pair of elements written in a particular order. This means that (x, y) and (y, x) represent different ordered pairs, unless $x = y$. Sometimes x and y are called coordinates, with x being the first one and y the second.

10.8 Theorems

In this section we will present statements and proofs of simple theorems, which are a good warm-up to the more complicated material on the set theory.

Theorem 10.10. *For any sets A, B and C, the following statements are true:*

i. $A \cup A = A$,

ii. $A \cup B = B \cup A$, *(commutative law)*

iii. $A \cup (B \cup C) = (A \cup B) \cup C$, *(associative law)*

iv. $A \subset A \cup B$ *and* $B \subset A \cup B$,

v. $A \cup \emptyset = A$.

Proof. i. Take any x in A. But then the statement "$x \in A$ or $x \in A$ is also trivially true ($\forall x,\ x \in A \Leftrightarrow (x \in A \text{ or } x \in A)$). Therefore the statement holds.

ii. $(x \in A \text{ or } x \in B) \Leftrightarrow (x \in B \text{ or } x \in A)$. Trivially, the statements are equivalent, hence *(ii)* is true.

iii. We will start from the left hand side of the statement to arrive at the right hand side, using definitions of the union of sets.

$\forall x,\ (x \in A \cup (B \cup C)) \Leftrightarrow (x \in A \text{ or } x \in (B \cup C)) \Leftrightarrow (x \in A \text{ or } (x \in B \text{ or } x \in C)) \Leftrightarrow ((x \in A \text{ or } x \in B) \text{ or } x \in C) \Leftrightarrow (x \in (A \cup B) \text{ or } C) \Leftrightarrow (x \in (A \cup B) \cup C)$.

iv. This follows from the definition of the union of the sets: $x \in A \cup B$ means $x \in A$ or $x \in B$. Hence, $A \subset A \cup B$ and $B \subset A \cup B$.

v. $x \in A \cup \emptyset \Leftrightarrow x \in A$ or $x \in \emptyset$. But $\emptyset$ does not contain any elements, hence $x \in A \cup \emptyset \Leftrightarrow x \in A$. □

The next theorem is similar to the previous one, but it deals with the intersections of the sets. The proofs are not provided and the reader is strongly encouraged to mimic the above arguments to prove the following statements.

Theorem 10.11. *For any sets A, B and C, the following statements hold:*

i. $A \cap A = A$,

ii. $A \cap B = B \cap A$, *(commutative law)*

iii. $A \cap (B \cap C) = (A \cap B) \cap C$, *(associative law)*

iv. $A \cap B \subset A$, $A \cap B \subset B$,

v. $A \cap \emptyset = \emptyset$. □

The next result provides the rules when taking the unions and intersections with three different sets.

Theorem 10.12 (Distributive laws for sets)**.** *For any three sets A, B and C,*

i. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$,

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

When working with sets, it is a good idea to picture the statement first, using Venn diagrams, to see that the theorem is in fact true. Remember that the diagrams are **not** proofs and the formal argument needs to follow.

Draw separate pictures, one for the left hand side and the other for the right hand side of the statement. You should get exactly the same graphs, which can reassure you that the theorem is correct. Then you can start your formal proof.

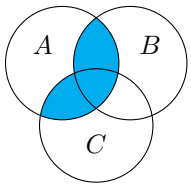


Figure 3: $A \cap (B \cup C)$

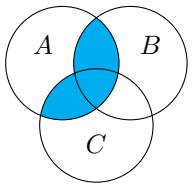


Figure 4: $(A \cap B) \cup (A \cap C)$

Proof. i.

$$\begin{aligned} x \in (A \cap (B \cup C)) &\Leftrightarrow x \in A \text{ and } x \in (B \cup C) \\ &\Leftrightarrow x \in A \text{ and } (x \in B \text{ or } x \in C) \\ &\Leftrightarrow (x \in A \text{ and } x \in B) \text{ or } (x \in A \text{ and } x \in C) \\ &\Leftrightarrow x \in (A \cap B) \text{ or } x \in (A \cap C) \\ &\Leftrightarrow x \in (A \cap B) \cup (A \cap C). \end{aligned}$$

ii. This part is left to the reader as an exercise. □

Three of the earlier described operations on sets (intersection, union and complement) have been related to each other in the 19th century by the British mathematician Augustus De Morgan. We present his theorem below.

Theorem 10.13 (De Morgan's Laws)**.** *Let A and B be sets. Then the following statements are true:*

i. $(A \cap B)' = A' \cup B'$,

ii. $(A \cup B)' = A' \cap B'$

The proof is not provided, but is an excellent exercise so the reader is strongly encouraged to try writing it.

11 Functions

A function can be defined by specifying three elements: set of inputs (called **domain**), set of outputs plus possibly extra elements[9] (called **codomain**) and a **rule** assigning each element from the domain to a unique member of the codomain. Formally, functions can be defined in many ways, for example in terms of sets, like below.

Definition 11.1 (Function)**.** Let A and B be sets. A **function** (also called a **map**) f from A to B, $f : A \to B$ is a subset $F \subseteq A \times B$ such that for each $a \in A$ there is one and only one pair of the form (a, b) in F.

For example, we may have the set of real numbers $\mathbb{R}$ as a domain and the codomain and the rule $f(x) = x^2$. In this case, we define the function in the following way:

$$\text{let } f : \mathbb{R} \to \mathbb{R} \text{ be given by } f(x) = x^2.$$

Writing just $f(x) = x^2$ on its own does not describe the function fully; it is tempting to state "$f(x) = x^2$ is a function", but you need to specify the domain and codomain as well. Notice that they are a really important part of our definition of a function. Imagine that we changed the codomain from $\mathbb{R}$ to $\mathbb{Z}$; the resulting function is completely different! The functions are equal only if all three elements are the same.

Many authors of the mathematical books, like for example D. Bloch [1], will point out the difference between f and $f(x)$. This is one of those things that are often assumed as "unimportant" by students and needs to be pointed out at the beginning, since it may lead to misunderstandings in the future. Informally, you may still find people referring to "the function x^2", but this is really an abuse of notation. Notice how we defined the function above; "$f : \mathbb{R} \to \mathbb{R}$" suggests that the name of the function is f and NOT $f(x)$.

11.1 Image and preimage

There is an important difference between the codomain and the **image**, sometimes also called **range**. It is common to mix these two terms and interchange them when describing the functions. You can think of a codomain as the "target set" of a function, which all the outputs are constrained to fall into. It may however include the elements which are not the outputs of the function for any of the elements of the domain. The image of the function, however, is a set of values that the function can produce. The formal definition is given below.

Definition 11.2 (Image)**.** *Let $f : A \to B$ be a function from set A to B and let X be a subset of A. The image of a subset $X \subseteq A$ under f is the subset $f(X) \subseteq B$ defined by*

$$f(X) = \{b \in B | b = f(a) \text{ for some } a \in X\}.$$

*The image $f(A)$ of the entire domain is called the **image of f**.*

We also use the term "image" when talking about a single element of a set. Letting $f : A \to B$ to be a function from the set A to B, we can find the image of any element $a \in A$ under f. The function $f(a) = b$ gives us the "output", i.e. the element of the codomain B, which is our required image of a point a.

So far, we have only looked at the function as the process of inputting the values and receiving the output values. We can also reverse this operation.

Definition 11.3 (Inverse image, pre-image)**.** *Let f be a function from A to B. The **pre-image** or **inverse image** of a set $Y \subseteq B$ under f is the subset of A defined by*

$$f^{-1}(Y) = \{\, a \in A \,|\, f(a) \in Y\}.$$

[9] see the difference between the codomain and the range

In various mathematical books you may find a slightly different notation for the image and pre-image of the function; for the image of the function $f : A \to B$, some authors use $f_*(A)$ instead of our $f(A)$, and the pre-image is denoted by $f^*(B)$ instead of $f^{-1}(B)$. Although the notation used by the author of this paper is more common and should be sufficient for students, Bloch [1] in his book calls such writing style an "abuse of notation, which is a technically incorrect way of writing something that everyone understands what it means anyway, and tends not to cause problems". He argues that the notation $f^{-1}(B)$ does not imply that the function f^{-1} exists, which sends us to the topic of inverse functions, discussed later in this document.

Examples

Let us give some examples on what we have discussed so far.

- The first, classical example when talking about the images and preimages is the function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$. Notice that the image of 3 is 9, but the preimage of 9 is {-3,3}.
- Given the function $g : \{1, 2, 3, 4\} \to$ {red,white,blue} defined by

$$g(x) = \begin{cases} red & \text{if } x = 1, 2, \\ white & \text{otherwise.} \end{cases}$$

  Then the image of the function is the set $\{red, white\}$. The preimage of red is $g^{-1}(\{red\}) = \{1, 2\}$ and $g^{-1}(\{red, blue\}) = \{1, 2\}$ as well. Notice that $g^{-1}(\{blue\}) = \emptyset$.
- Let $h : \mathbb{R} \to \mathbb{R}, h(x) = e^x$. Here the codomain is defined to be $\mathbb{R}$, but the image of the function is the set $(0, \infty)$.

11.2 Composition of the functions

We can combine the functions in many different ways using the **composition of the functions**.

Definition 11.4. *Let $f : A \to B$ and $g : B \to C$ be functions. The **composition** of f and g is the function $g \circ f : A \to C$ defined by*

$$(g \circ f)(x) = g(f(x)) \text{ for all } x \in A.$$

This means that for any element of the domain ($a \in A$), we can apply the function f and then the function g, to get an output ($(g \circ f)(a) \in C$) of the function $g \circ f$. To be able to combine two functions, we must have that the codomain of the first one is equal to the domain of the second one.

Be careful not to mix the order of applying the functions, as the commutativity does not hold in this case. The following example illustrates this fact.

Example 11.1. *Let $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}$ be functions given by $f(x) = x^3$ and $g(x) = x + 5$.*
Then $(g \circ f)(2) = g(f(2)) = g(2^3) = g(8) = 13$,
but $(f \circ g)(2) = f(g(2)) = f(2 + 5) = f(7) = 7^3 = 243$.

Notice that in the above example we are able to form both $g \circ f$ and $f \circ g$, since the domains and codomains are equal. In the situation when

$$f : A \to B, g : B \to C,$$

it is impossible to construct $f \circ g$, unless $A = C$!

11.3 Special functions

Among many different functions we can distinguish a special function, which will always return the same value that was used as an input. We call such function the **identity function** defined by $f : A \to A$ such that $f(x) = x$ and usually denoted by id_A.

A **constant function** is another specific function. It is of the form $f(x) = c$, where c is the constant returned from the function, regardless of the input value.

11.4 Injectivity, surjectivity, bijectivity

Definition 11.5 (Injectivity, one-to-one function)**.** This is a function that maps distinct points of the domain to distinct points of the codomain.

Let f be a function whose domain is D. If f is injective, then $\forall\ a, b \in D,\ a \neq b \Leftrightarrow f(a) \neq f(b)$.

You can often judge whether the function is injective or not by just looking by its graph. We should see that *every* element from the domain is assigned to *exactly one* member of the codomain. Remember that although the picture is a helpful tool, it does not replace the formal argument!

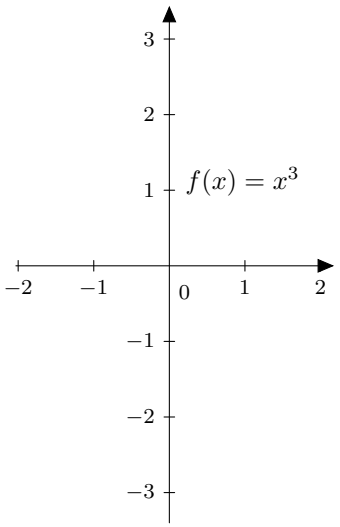


Figure 5: Injective

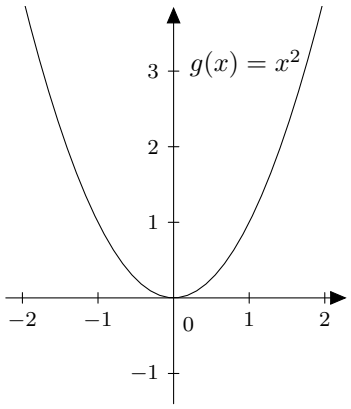


Figure 6: Not injective

To show the injectivity (or non-injectivity) of a function f, we use the definition. We let $x_1, x_2 \in \mathbb{R}$ and start by assuming that $f(x_1) = f(x_2)$. If the function is injective, we should arrive at the statement "$x_1 = x_2$". Otherwise, the it is not injective.

Let $f : \mathbb{R} \to \mathbb{R}, f(x) = x^3$,

Assume that $f(x_1) = f(x_2)$

$$\begin{aligned}
&\implies x_1^3 = x_2^3 \\
&\implies x_1^3 - x_2^3 = 0 \\
&\implies (x_1 - x_2)\underbrace{(x_1 + x_1x_2 + x_2^2)}_{\text{always} > 0} = 0 \\
&\implies x_1 = x_2
\end{aligned}$$

Hence this function is injective.

Let $g(x) : \mathbb{R} \to \mathbb{R}, g(x) = x^2$

Assume that $g(x_1) = g(x_2)$

$$\begin{aligned}
&\implies x_1^2 = x_2^2 \\
&\implies x_1^2 - x_2^2 = 0 \\
&\implies (x_1 - x_2)(x_1 + x_2) = 0 \\
&\implies x_1 = \pm x_2
\end{aligned}$$

Hence g is **not** injective.

Note that it is possible to get $g(x) = x^2$ injective, by restricting the domain to $\mathbb{R}^+$ (positive real numbers).

Definition 11.6 (Surjectivity, onto function)**.** Let f be a function $f : A \to B$. Then f is surjective $\Leftrightarrow$ for any element $b \in B$, there exists an element $a \in A$ such that $f(a) = b$.

Note that f may send more than one element from A to the same element in B.

The image of the surjective function is equal to its codomain, so *every* element of B has *at least one* element of A assigned to it. From Figure 5 we can see that the function $f(x) = x^3$ is surjective, however $g(x) = x^2$ is not. To make g surjective, we need to change the codomain to $\mathbb{R}^+$.

Definition 11.7 (Bijectivity, one-to-one correspondence[10])**.** A bijective function $f : A \to B$ is mapping between two sets A and B, which is both injective and surjective. Each element from the set A is paired with exactly one element from set B and each element from set B is paired with exactly one element from set A.

Exercise 11.2. *Study the examples below. Decide whether they are surjective, injective or bijective. If not, how can you restrict domain or codomain to make them bijective?*

1. $f : \mathbb{R} \Rightarrow \mathbb{R},\ f(x) = \sin x,$
2. $g : \mathbb{Z} \to \mathbb{Z},\ g(x) = e^x,$
3. $h : \mathbb{R}^+ \to \mathbb{R},\ h(x) = x^2 - 5.$

11.5 Inverse function

For any bijective function f, we can find an **inverse function** (f^{-1}), which reverses the process. While the function f takes an input x and returns the output $f(x) = y$, the inverse function will take y back to x, i.e.

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

Notice also that the composition of the function with its inverse gives the identity function[11],

$$f^{-1}(f(x)) = x = f(f^{-1}(x)).$$

Notice that the function $f(x) = x^2$, will have an inverse (or not) depending on the domain (will need to be restricted so that f is bijective).

11.6 Even and odd functions

Definition 11.8. The function $f : X \to Y$ is **even** if it is true that

- if $x \in X$, then $-x \in X$, and
- $f(x) = f(-x)$ for all $x \in X$.

[10] Note that the *one-to-one function* and *one-to-one correspondence* are two different concepts and should not be confused.

[11] See the theorem at the end of the chapter

Even functions are **symmetric with respect to the $y-$axis**. You can check that the function $g(x) = x^2$ (fig.6) is an even function, but $f(x) = x^3$ (fig.5) is not.

Definition 11.9. The function $f : X \to Y$ is **odd** if it is true that

- if $x \in X, \text{then } -x \in X$, and
- $f(-x) = -f(x)$ for all $x \in X$.

The odd functions are **symmetric with respect to the origin**, which means that they remain unchanged when reflected across both $x-$ and $y-$axis. From the graph you can see that the function in fig.5 is odd, but the one in fig.6 is not.

11.7 Exercises

Theorem 11.3. Let $f : A \to B, g : B \to C$ and $h : C \to D$ be functions.

1. If f has an inverse, then the inverse is unique;
2. If f and g are injective, then $g \circ f$ is also injective;
3. If f and g are surjective, then $g \circ f$ is also surjective;
4. If f and g are bijective, then $g \circ f$ is also bijective;
5. $(h \circ g) \circ f = h \circ (g \circ f)$ (Associative Law);
6. $f \circ id_A = f$ and $id_B \circ f = f$ (Identity Law).

The above statements are a good exercise to practise proofs on functions and are left for the reader to try.

References

[1] Ethan D. Bloch, *"Proofs and Fundamentals. A First Course in Abstract Mathematics"*, Birkhäuser, Boston, 2000.

[2] Kevin Houston, *"How to Think Like a Mathematician. A Companion to Undergraduate Mathematics"*, Cambridge University Press, Cambridge, 2009.

[3] Martin Liebeck, *"A Concise Introduction to Pure Mathematics"*, CRC Press, Taylor & Francis Group, Boca Raton, 2011.

[4] Richard Bornat, *"Proof and Disproof in Formal Logic"*, Oxford University Press, New York, 2005.

[5] Kam-Tim Leung, Doris Lai-Chue Chen, *"Elementary Set Theory"*, Hong Kong University Press, Hong Kong, 1967.

[6] Martin Aigner, Günter M. Ziegler, *"Proofs from THE BOOK"*, Springer-Verlag, Berlin, 2001.

12 Appendix

Theorem 12.1. *card($\mathbb{R}$)= card($\mathbb{R}^2$)*

Notes. Here the question is: how is it actually possible to correspond an element from the real line to an element on the plane? We will present the idea of the proof, considering an interval $\mathcal{I} = [0, 1]$ and the unit square $\mathcal{Q} = [0, 1]^2$ instead of the whole real line and the plane.

Proof. Consider a point in the unit sqare $(x, y) \in \mathcal{Q}$ and write the decimal expansion of x and y,

$$x = 0.\, x_1\, x_2\, x_3\, x_4\, x_5 ...$$

and

$$y = 0.\, y_1\, y_2\, y_3\, y_4\, y_5 ...$$

Now, to find a point on $\mathcal{I}$ corresponding to (x, y), we use the above expansion of x and y, creating a point z, as shown below.

$$z = 0.\, x_1\, y_1\, x_2\, y_2\, x_3\, y_3 ...$$

Note, that this approach would work well if not for the fact that $0.a\,b\,c\,0\,9\,9\,9... = 0.a\,b\,c\,1\,0\,0\,0....$ So we can represent the point $(x, y) \in \mathcal{Q}$ using two different decimal expansions of x and y, which would result in getting two distinct points z and z' $(z, z' \in \mathcal{I})$. Hence the mapping is not one-to-one. To avoid this situation, we do not allow the decimal expansions with the infinite number of nines, (for example 0.04999... is forbidden).

Now we can be sure that the point $z \in \mathcal{I}$ is unique for each pair (x, y). □

Theorem 12.2. *Suppose that $\{v_1, v_2, v_3\}$ is the linearly independent set of vectors. Then $\{v_1, v_3\}$ is also linearly independent set.*

> *Notes. The proof is not complete and the reader is encouraged to fill in the gaps. First, recall that finitely many vectors $v_1, v_2, \dots v_r$ are **linearly dependent** if there exist scalars (not all zero) such that $a_1v_1 + a_2v_2 + \cdots + a_rv_r = 0$. If the vectors are not linearly dependent, then we say they are **linearly independent**.*
> *Now, the statement is fairly simple but how to prove it? If we remember the relation $(A \Rightarrow B) \equiv (\text{not } B \Rightarrow \text{not } A)$, then the second one is easy to show.*

Click here to see a video example

Proof. Assume that $\{v_1, v_3\}$ are ...

(assume the opposite)

So we can write

$$\dots v_1 + \dots v_3 = \dots$$

for some scalars $\dots, \dots \in \mathbb{R}$.

(fill in the dots using your knowledge about the dependent vectors)

Now notice that

$$\dots v_1 + \dots v_2 + \dots v_3 = 0,$$

hence we have that v_1, v_2 and v_3 are ....

So we proved that...

(write the conclusion)

hence by contrapositive we have that .... □

Theorem 12.3. $\ln x \leq x - 1$ *for* $x > 0$.

Proof. We will use the expansion of the exponential function (proof of the expansion is not provided, as it is commonly used in the first year of studies):

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \dots \qquad (*)$$

We first show that $e^x \geq 1 + x$ for all $x \in \mathbb{R}$.

From the expansion above (*), this is clear for $x \geq 0$.

Also from (*), if $0 \leq x < 1$,

$$\begin{aligned} e^x &= 1 + x + \frac{x^2}{2} + \frac{x^3}{3!} + \dots \\ &\leq 1 + x + x^2 + x^3 + \dots \\ &= \frac{1}{1-x} \end{aligned}$$

Therefore if $-1 < x < 0$,

$$e^x \leq \frac{1}{1-(-x)} = \frac{1}{1+x}$$

and so $e^x \geq 1 + x$ for $-1 < x < 0$.

Finally, for $x \leq -1$, e^x is positive and $1 + x$ is negative. So $e^x \geq 1 + x$ for $x \leq 1$.

Therefore, $e^x \geq 1 + x$ for all $x \in \mathbb{R}$.

Now, let $x = \ln u$ (where $u > 0$). Then

$$\begin{aligned} e^{\ln u} &\geq 1 + \ln u \\ \therefore u &\geq 1 + \ln u \end{aligned}$$

So $\ln u \leq 1 - u$ for all $n > 0$.

□

UNIVERSITY OF BIRMINGHAM

UNIVERSITY OF BIRMINGHAM
Mathematics
Support Centre
PART OF THE ACADEMIC SKILLS CENTRE