MATH104a Module Notes

These notes do not repeat material presented in lectures, so reading them is not a substitute for attending lectures, or for taking proper notes.

There is one section of the notes for each of the five chapters of the module. Each section starts with a list of new terms introduced within the chapter, and a list of 'things to remember', which summarizes the most important points of the chapter. You may find these useful in your revision, and it is also a good idea to read them through before starting on a problem sheet: if you don't understand any of the 'things to remember', you should look them up in your lecture notes before proceeding. Both of the lists are designed as quick-reference tools, and are not necessarily comprehensible without your lecture notes.

The remainder of each section is organised under the same headings as your lecture notes, and contains additional remarks and examples which you may find helpful if you're having difficulty understanding particular sections of the module. Some of the additional examples are at the same level as those in lectures and some are more advanced. *Unless otherwise stated, only the lectured material is examinable: additional material in the module notes is for background only.* Almost all of the additional material, however, has been designed to help your understanding of the topics covered in lectures.

1 The language of mathematics

Mathematicians are like Frenchmen: whatever you say to them they translate into their own language, and forthwith it is something entirely different.
Johann Wolfgang von Goethe (1749 – 1832)

Terms Introduced[1]

Statement A (mathematical) statement is a sentence which is either true or false, once its free variables have been assigned values.

Free variable The free variables of a statement P are the objects (e.g. numbers) which must be given a value before the statement is unambiguously true or false.

Connective A connective combines two statements into a single statement. For example, the connective 'and' combines two statements P, Q into the single statement

$$P \text{ and } Q.$$

Negation The negation not(P) of a statement P is *the statement that P is false.* Thus not(P) is true if P is false, and false if P is true.

Set A set is a well defined collection of objects (e.g. numbers), called the *elements* of the set.

Things to remember

1. Be aware of what the symbols $=$ and $\implies$ mean, and avoid using them casually.
2. Identifying free variables is *not* just a matter of listing the different symbols in the statement. See the examples in Section 1.2.
3. In mathematics 'or' always means *inclusive* or. That is,

$$P \text{ or } Q$$

is true if P is true, or Q is true, *or both are true.*

[1]These are not formal definitions. Some of these terms ('Statement', 'Free variable', and 'Set') have technical definitions which are more complicated than the explanations given here. The alert reader will notice that the 'definitions' of 'statement' and 'free variable' are circular.

4. The symbol $\pm$ introduces an implicit 'or'[2]. For example, $x = \pm 1$ is a shorthand for
$$x = 1 \text{ or } x = -1.$$
It is important to bear this in mind when negating statements involving $\pm$.

5. The statement
$$P \implies Q$$
says that *if* P is true *then* Q is true. It *doesn't* claim that P actually is true, or that if P is false then Q must be false.

6. Remember that $P \implies Q$ and $Q \implies P$ are **not the same**.

7. The negation of 'P and Q' is 'not(P) **or** not(Q)'.
The negation of 'P or Q' is 'not(P) **and** not(Q)'.

8. Take special care when negating a statement involving $\implies$.

9. Mathematicians disagree about whether or not the natural numbers $\mathbb{N}$ include 0. In this module we will consider 0 to be a natural number (so $\mathbb{N} = \{0, 1, 2, \ldots\}$), and write $\mathbb{Z}^+$ for the set $\{1, 2, 3, \ldots\}$ of positive integers.

10. Distinguish between the similar-looking *Conditional* and *Constructive* descriptions of a set.

1.1 Writing Mathematics

We start with a couple of additional points about good mathematical writing style, and then present the Greek alphabet.

Distinguish between 'Let' and 'Then'

Remember that when you write mathematics, you're trying to communicate with someone (even if it's only a marker). Make it as easy as possible for them to understand what you're doing.

You should avoid writing statements like '$n < 3$', '$f(x) = \sin x$', or '$x \in X$' in isolation, since they leave the reader asking 'are you *assuming* that $n < 3$, or telling me that $n < 3$ *follows* from what went before?'.

[2] On the left of an $=$ sign, it can introduce an 'and' instead. For example, $f(x \pm y) = 0$ is shorthand for '$f(x + y) = 0$ and $f(x - y) = 0$'.

If it's an assumption, then you should write something like 'Let $n < 3$' or 'Suppose $n < 3$'. If the fact that $n < 3$ follows from what you've just written, you should write 'Then $n < 3$ because...', 'So $n < 3$', or 'Thus $n < 3$'.

Distinguish between 'Multiply' and 'Times'

This is really a point about spoken rather than written mathematics. Many people say things like 'we take these two numbers and times them together'. This is bad English: 'multiply' is a verb, whereas 'times' is (I think) a preposition.

The same comment applies to the other three basic arithmetic operations, $+$, $-$, and $\div$. The following table sums it up:

Operation	Verb	Preposition	Noun
$+$	Add	Plus	Sum
$-$	Subtract	Minus	Difference
$\times$	Multiply	Times	Product
$\div$	Divide	Divided by	Quotient

Thus you should say:

'Let's *add* 3 and 4. 3 *plus* 4 equals 7. So the *sum* of 3 and 4 is 7.'

'Now we'll *multiply* $(x+y)$ and $(x-y)$. We find that $(x+y)$ *times* $(x-y)$ equals x^2-y^2. That is, the *product* of $(x+y)$ and $(x-y)$ is x^2-y^2.'

The Greek Alphabet

Letters from the Greek alphabet are widely used in mathematical writing, sometimes in contexts specific to the letter (e.g. θ for an angle, ϵ for a small number, π), and sometimes simply because there aren't enough ordinary (Roman) letters.

The alphabet is shown in Table 1 on the following page. As with the Roman alphabet, each letter has a lower case ('small') and upper case ('capital') version. The table also indicates how you might write the lower case versions of the letters. I don't claim to be an expert in writing Greek (my ξ is just a squiggle), and you don't need to be either: the important thing is to be able to write each letter in such a way that it can be distinguished from other Greek and Roman ones.

All of the lower case letters except omicron are used in mathematical writing. Fewer of the upper case letters are used, mainly because many of them look exactly the same as upper case Roman letters. However, Γ, Δ, Θ, Λ, Ξ, Π, Σ, Φ, Ψ, and Ω are all frequently used.

It's well worth learning the names of the letters: that way, when a lecturer writes a formula like

$$\frac{\alpha - \beta}{\epsilon} + \eta\delta^3$$

and then starts talking about 'eta', you know which symbol is being referred to.

The Greek alphabet may be tested in the exam. If it is, the question would be similar to:

What are the names of the following Greek letters: δ; σ? Write the lower-case Greek gamma, and the upper-case omega.

You will not be tested on upper-case letters other than the ones which are used in mathematical writing (see list above).

1.2 Statements

Examples of identifying free variables

a) If $x > R$ then $f(x) < \epsilon$.

There are four objects involved in this statement: x, R, ϵ, and the function $f(x)$. Of these, R, ϵ, and $f(x)$ are free variables, since the statement is not unambiguously true or false until we have said what they are. For example, if we take $R = 10$, $f(x) = \frac{1}{x^2}$, and $\epsilon = 0.01$ we get

$$\text{If } x > 10 \text{ then } \frac{1}{x^2} < 0.01,$$

and it is then possible to decide whether or not the statement is true (it is). If we leave any of R, ϵ, and $f(x)$ undefined, then it cannot be decided whether or not the statement is true[3].

The key to noticing that x is not a free variable is the 'if' which precedes it. The point of the statement is that it's saying something about a whole range of values of x, and therefore it isn't appropriate to fix a particular value of x. Other words and phrases which indicate a non-free variable include 'For all/each/every', 'There exists/is', and

[3] In fact this isn't quite the case. Suppose we take $f(x) = -x^2$ and $\epsilon = 1$. The statement then reads 'If $x > R$ then $-x^2 < 1$'. Assuming (as we have been doing) that x is a real number, it is clear that this statement must be true whatever the value of R, since *any* x has $-x^2 \leq 0 < 1$. Our approach to such subtleties is to ignore them.

Name	Lower	Upper	Equivalent	Common uses
alpha	α	A	a	
beta	β	B	b	
gamma	γ	Γ	g	
delta	δ	Δ	d	Small (+ve) number
epsilon	ϵ, ε	E	ĕ	Small (+ve) number
zeta	ζ	Z	z	
eta	η	H	ē	
theta	θ, ϑ	Θ	th	Angle
iota	ι	I	i	
kappa	κ	K	k	
lambda	λ	Λ	l	Eigenvalue
mu	μ	M	m	
nu	ν	N	n	
xi	ξ	Ξ	x	
omicron	o	O	ŏ	
pi	π	Π	p	Circumference/Diameter
rho	ρ	P	r	
sigma	σ	Σ	s	Standard deviation
tau	τ	T	t	
upsilon	υ	Υ	u	
phi	ϕ, φ	Φ	ph	Angle
chi	χ	X	ch	
psi	ψ	Ψ	ps	Angle
omega	ω	Ω	ō	Angular velocity

Table 1: The Greek alphabet

'Whenever'. Likewise, the left hand side of a $\implies$ usually contains a non-free variable: the statement we're considering could have been written

$$x > R \implies f(x) < \epsilon.$$

However, it is unwise to rely solely on such rules: clear thought about each given example is preferable. In tricky cases, try experimenting by giving values to different combinations of objects in the statement, and deciding whether what remains is unambiguously true or false.

b) For every $\epsilon > 0$, there is some $\delta > 0$ such that $f(x) < \epsilon$ whenever $0 < x < \delta$.

Here there is only one free variable, the function $f(x)$. ϵ, δ, and x are not free variables: note the key phrases 'for every' before ϵ, 'there is' before δ, and 'whenever' before x. Note that the statement could equivalently have been written

$$\text{For every } \epsilon > 0, \text{ there is some } \delta > 0 \text{ such that } 0 < x < \delta \implies f(x) < \epsilon.$$

Now the fact that x is on the left of $\implies$ suggests that it isn't a free variable.

c) $f(x)$ is an odd function.

This example illustrates a different point. Clearly we can't decide whether or not the statement is true until we know what the function $f(x)$ is, so this function is a free variable. However, x itself is not a free variable: saying that $f(x)$ is odd is a statement about the function as a whole (namely, that *for all* x, $f(-x) = -f(x)$), not about some particular value of x.

For this and similar reasons, it's common to drop the '(x)' when talking about functions. Thus we'd just write

$$f \text{ is an odd function.}$$

The extra clarity which this brings is very valuable in more advanced or abstract areas of mathematics.

Statements with more than one 'and' or 'or'

In the lectures, we only considered statements containing either a single 'and', or a single 'or'. However, statements involving a combination of 'and' and 'or' are common in maths – for example, after analysing the solutions of an equation, we might decide that

$$x = 0 \quad \text{or} \quad x > 2 \text{ and } y = z.$$

It is important to realise that *this statement is ambiguous as written.* The way that it has been spaced suggests that what is meant is

$$x = 0 \quad \text{or} \quad (x > 2 \text{ and } y = z),$$

and this is quite different from

$$(x = 0 \text{ or } x > 2) \quad \text{and} \quad y = z.$$

For example, if $x = 0$, $y = 1$, and $z = 2$, then the first statement is true (since $x = 0$), but the second is false (since $y \neq z$). It is always advisable to include brackets to indicate which of the two possibilities is meant.

The rule when negating such compound statements is: *Negate each substatement, change each 'and' to 'or' and vice-versa, and keep the brackets where they are.* To see why this works, we negate the above example carefully in steps. Suppose P is the statement

$$P: \quad x = 0 \quad \text{or} \quad (x > 2 \text{ and } y = z).$$

To negate it, we take two steps, first dealing with the 'or' and then with the 'and':

$$\text{not}(P): \quad x \neq 0 \quad \text{and} \quad \text{not}(x > 2 \text{ and } y = z).$$

This is just the standard rule for negating an 'or'. Next, we apply the standard rule for negating an 'and' to give that not($x > 2$ and $y = z$) is the same as ($x \leq 2$ or $y \neq z$), so

$$\text{not}(P): \quad x \neq 0 \quad \text{and} \quad (x \leq 2 \text{ or } y \neq z).$$

If you brood on it for long enough, you'll agree that this is saying precisely that P isn't true.

1.3 Negation

Negation of an implication

As explained in lectures, negating a statement which involves $\implies$ (or, equivalently, which involves 'if. . . then') requires careful thought: however, once you've done a few examples, it begins to become more natural. Since $P \implies Q$ means that *if P is true then Q is true*, its negation states that *it is possible for P to be true and Q to be false.* Consider, for example, the statement

$$R: \qquad x > 0 \implies f(x) > 0.$$

(so P is '$x > 0$' and Q is '$f(x) > 0$'). This is a statement about a function $f(x)$: it says that *if* $x > 0$ *then* $f(x) > 0$. In other words, the statement claims that the portion of the graph of $f(x)$ to the right of the y-axis lies entirely above the x-axis.

Following the discussion above, the negation of R is: it is possible for P to be true and Q to be false. That is

$$\text{not}(R): \qquad \text{there is some } x \text{ with } x > 0 \text{ and } f(x) \leq 0.$$

That is, the negation says that the portion of the graph of $f(x)$ to the right of the y-axis does *not* lie entirely above the x-axis: there is at least one point $x > 0$ for which $f(x) \leq 0$, i.e. the graph touches or is below the y-axis.

A more mechanical approach to negating this sort of statement will be introduced in Chapter 5.

1.4 Set notation

Further examples of Conditional and Constructive Descriptions of sets

Here are some additional straightforward examples, similar to those of question 4 on problem sheet 2.

a) Give a statement $P(n)$ such that

$$\{\ldots, -4, -3, -2, -1, 0, 17, 19, 21, 23, 25, \ldots\} = \{n \in \mathbb{Z} \mid P(n)\}.$$

In this problem, we're asked to give a conditional description of a set which has two types of elements: first, all integers which are ≤ 0, and second, all odd integers which are ≥ 17. Having identified the elements of the set in this way, we can write down $P(n)$ almost immediately:

$$P(n): \; n \leq 0 \quad \text{or} \quad (n \geq 17 \text{ and } n \text{ is odd}).$$

Note the use of brackets to make the meaning of this statement unambiguous (see the discussion on page 7). Note also that there are many different ways of writing a correct answer: for example, instead of '$n \leq 0$' we could have written '$n < 1$', or 'n is not positive'.

b) Give a function $f(n)$ such that

$$\{3, -2, -7, -12, -17, \ldots\} = \{f(n) \mid n \in \mathbb{N}\}.$$

In this problem we're asked to give a constructive description. The obvious thing to try is a function $f(n)$ with

$$\begin{aligned} f(0) &= 3 \\ f(1) &= -2 \\ f(2) &= -7 \end{aligned}$$

and so on. The fact that each value is 5 less than the previous one suggests that $f(n) = C - 5n$ for some constant C, and since $f(0) = 3$ it follows that we must have $C = 3$. Thus $f(n) = 3 - 5n$: you can check that this gives the correct values when we take $n = 0, 1, 2, 3, \ldots$.

If you're stuck on question 4 b) f) on problem sheet 2, try reading the next section.

Advanced topic: Countability

The discussion which follows introduces the fascinating concept of countable and uncountable sets. It is definitely 'for interest only'. This subject is treated in more detail in MATH241.

The exercise on constructive description of sets on problem sheet 2 asks you, for various choices of set S, to find a function $f(n)$ such that

$$S = \{f(n) \mid n \in \mathbb{N}\}.$$

One might reasonably ask whether this is possible for *any* set S (perhaps with an extremely complicated function $f(n)$).

Since

$$\{f(n) \mid n \in \mathbb{N}\} = \{f(0), f(1), f(2), f(3), \ldots\},$$

it looks at first sight as though we can only describe S in this way if it is no bigger than $\mathbb{N}$, because there can only be one element of S for each element $0, 1, 2, 3, \ldots$ of $\mathbb{N}$. However, our intuitive ideas about the 'size' of a set can go wrong when we're talking about infinite sets. For example, it certainly looks at first sight as though $\mathbb{Z}$ is a 'bigger' set than $\mathbb{N}$, since it contains all of $\mathbb{N}$ and all the negative integers too. But it is possible to find a function $f(n)$ such that

$$\mathbb{Z} = \{f(n) \,|\, n \in \mathbb{N}\} :$$

to do it, we take $f(0) = 0$, $f(1) = 1$, $f(2) = -1$, $f(3) = 2$, $f(4) = -2$, $f(5) = 3$, and so on. With a little bit of thought, we can find an explicit formula for this function:

$$f(n) = \begin{cases} -\frac{n}{2} & \text{if } n \text{ is even} \\ \frac{n+1}{2} & \text{if } n \text{ is odd,} \end{cases}$$

or even (if we want to be really fancy and do our best to confuse the unfortunate reader)

$$f(n) = \frac{(-1)^{n+1}(2n+1)+1}{4}.$$

Since every integer appears in the list $0, 1, -1, 2, -2, 3, -3, \ldots$, we do indeed have

$$\mathbb{Z} = \{f(n) \,|\, n \in \mathbb{N}\}.$$

The set $\mathbb{Q}$ of all rational numbers (fractions) appears to be bigger still. However, it too can be described constructively from the natural numbers. Following the approach for $\mathbb{Z}$, the key is to find a list $q_0, q_1, q_2, q_3, \ldots$ (analogous to $0, 1, -1, 2, -2, 3, -3, \ldots$) which contains all of the rationals m/n: we can then take $f(0) = q_0$, $f(1) = q_1$, $f(2) = q_2$ and so on.

Notice first that the *positive* rationals can be listed like this:

$$\frac{1}{1}, \quad \frac{1}{2}, \frac{2}{1}, \quad \frac{1}{3}, \frac{2}{2}, \frac{3}{1}, \quad \frac{1}{4}, \frac{2}{3}, \frac{3}{2}, \frac{4}{1}, \ldots$$

We first list all the fractions whose numerator and denominator add up to 2 (there's only one of them), then those whose numerator and denominator add up to 3 (two of them), then 4 (three of them) and so on. Within each list, we arrange them in order of increasing numerator. Every positive rational m/n appears in this list (namely in the sublist of fractions whose numerator and denominator add up to $m + n$). To get a list of *all* rationals, we play the same trick that we did with $\mathbb{Z}$, interleaving positive and negative values:

$$0, \quad \frac{1}{1}, \frac{-1}{1} \quad \frac{1}{2}, \frac{-1}{2}, \frac{2}{1}, \frac{-2}{1}, \quad \frac{1}{3}, \frac{-1}{3}, \frac{2}{2}, \frac{-2}{2}, \frac{3}{1}, \frac{-3}{1}, \quad \frac{1}{4}, \frac{-1}{4}, \ldots$$

It would be possible, though a lot of work, to write an explicit formula for a function $f(n)$ such that $f(0) = 0$, $f(1) = 1$, $f(2) = -1$, $f(3) = 1/2$, $f(4) = -1/2$, and so on.

However, we don't have to. Provided we've described exactly what the list looks like (and we have), we can just say

$$f(n) = \text{the } (n+1)^{\text{st}} \text{ entry in the list},$$

and with this $f(n)$ we have

$$\mathbb{Q} = \{f(n) \mid n \in \mathbb{N}\}.$$

Having seen these examples, one might be tempted to think that indeed *any* set S can be described in this way. However, this is not the case. In 1874, the Russian-born Mathematician Georg Cantor proved that

$$\text{There is no function } f(n) \text{ such that } \mathbb{R} = \{f(n) \mid n \in \mathbb{N}\}.$$

This was the first step in a theory dividing infinite sets into different 'sizes'. Sets which can be described as

$$S = \{f(n) \mid n \in \mathbb{N}\}$$

are called *countable*, while those that can't (not very surprisingly) are called *uncountable*. Thus $\mathbb{Z}$ and $\mathbb{Q}$ are countable, and what Cantor showed is that $\mathbb{R}$ is uncountable. Informally, $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{Q}$ are all infinite sets of the 'same size', but $\mathbb{R}$ is 'bigger' than them.

A famous problem which was much studied following Cantor's work is whether or not there are infinite sets S which are *intermediate* in size between $\mathbb{N}$ and $\mathbb{R}$. Such a set S would be 'bigger' than $\mathbb{N}$ (so couldn't be described constructively from $\mathbb{N}$), but 'smaller' than $\mathbb{R}$ (so $\mathbb{R}$ couldn't be described constructively from S). It was eventually shown in 1963 that this question is *undecidable* in standard mathematics: that is, it is impossible within standard mathematics either to prove that there is such a set S, or to prove that there isn't!

2 Definitions

Mathematics is the art of giving the same name to different things.
J. Henri Poincaré (1854 – 1912)

Terms Introduced

Divides Let m and n be integers. Then m *divides* n (written $m|n$) if there exists an integer k such that $n = km$.

Even/Odd Let n be an integer. Then n is *even* if $2|n$, and n is *odd* otherwise.

Prime Let n be an integer. Then n is *prime* if $n \geq 2$, and there is no integer m with $1 < m < n$ such that $m|n$.

Injective Let $f(x)$ be a function. Then $f(x)$ is *injective* if for all $x, y \in \mathbb{R}$,

$$f(x) = f(y) \implies x = y.$$

Closed under addition Let S be a subset of $\mathbb{Z}$. Then S is *closed under addition* if for all $m, n \in S$, $m + n$ is also an element of S.

Relation Let X be a set. A *relation* R on X is something such that, for all $x, y \in X$,

$$x \, R \, y$$

is either true or false. (You could think of R as a statement $R(x, y)$ with exactly two free variables x and y which take values from the set X.)

Equivalence relation Let R be a relation on a set X. Then R is an *equivalence relation* if for all $x, y, z \in X$,

a) $x \, R \, x$ (reflexive),

b) If $x \, R \, y$ then $y \, R \, x$ (symmetric),

c) If $x \, R \, y$ and $y \, R \, z$ then $x \, R \, z$ (transitive).

Things to remember

1. **THE MANTRA**. Showing that a definition is satisfied, and showing that it is not satisfied, are usually quite different processes. Typically, one requires an *argument*, while the other only requires an *example*.

2. When faced with a definition, identify the *key phrases* such as 'there exists/there is', 'there does not exist/there is no', 'for all/for every/whenever'. Using these, decide what needs to be done to show that the definition is satisfied, and what needs to be done to show that it isn't.

3. When a definition is complicated, try to get an intuitive feeling for what it 'really' means (e.g. when you see *injective* you should think 'the graph touches each horizontal line at most once'). Use this intuition to have 'private thoughts' or do 'private work' to decide whether or not the definition is satisfied in some particular case. Then translate your private work into the language of the definition.

4. In definitions, *if* almost always really means *if and only if*.

Motivation

This discussion summarizes the motivation for definitions that I gave in lectures, but didn't write on the board.

In mathematics, laziness can be a virtue. We first meet constructive laziness when we do algebra: instead of observing that

$$\begin{aligned} 3^2 - 1 &= 2 \times 4, \\ 10^2 - 1 &= 9 \times 11, \\ 38^2 - 1 &= 37 \times 39, \text{ and} \\ 2.5^2 - 1 &= 1.5 \times 3.5, \end{aligned}$$

we just write

$$x^2 - 1 = (x-1)(x+1).$$

By giving the same name x to all real numbers, we can do infinitely many calculations at once, and so get longer to spend in bed on a Sunday morning. Indeed, x needn't even be a real number: it could be a complex number, a square matrix, or a polynomial.

Good mathematical definitions have the same benefits as using symbols to denote arbitrary numbers in algebra. By means of a definition, we give the same name to all mathematical 'objects' which have certain properties. If we can then do calculations or deduce consequences using only these properties, they apply to all the different objects: we don't end up repeating essentially the same work over and over again.

A second reason for the importance of definitions is precision. In maths, we can't afford the ambiguities which so enrich everyday language. It is essential, therefore, that every technical term be properly defined, and if possible agreed on by all mathematicians everywhere. Where there is no common agreement (for example, in the definition of $\mathbb{N}$), we need to state clearly what definition we're using.

Of course, it isn't just in maths that precision is vital. Here's an example of definitions taken from another field:

Definition: A player is in an *offside position* if

a) He is nearer to his opponents' goal line than the second last opponent, and

b) He is nearer to his opponents' goal line than the ball, and

c) He is not in his own half of the field of play.

Definition: A player commits the *offside offence* if, at the moment the ball is played by one of his team

a) He is in an offside position, and

b) He is involved in active play, by

   i) Interfering with play, or

   ii) Interfering with an opponent, or

   iii) Gaining an advantage from his position.

This illustrates two points. First, definitions can be complex, but someone (such as a referee) who uses them frequently can learn to apply them quickly and (we hope) accurately to decide whether or not an offside offence has been committed. Second, definitions are often chained together: in order to understand what the *offside offence* is, you have to have understood the definition of *offside position*. In mathematics it's common to have extremely long chains of definitions.

2.1 Definitions of Terms

This section contains two examples of definitions not presented in lectures, with a discussion of how we might show whether or not they're satisfied in different cases. The first is a relatively simple one (along the lines of *divides*), while the second is more complicated (along the lines of *injective*). At the end of the section is a summary of the argument I gave in lectures (but didn't write on the board) for rejecting an alternative definition of *divides*.

Example: contains a square

Definition: Let $n \in \mathbb{Z}$. Then n *contains a square* if there is an integer $m > 1$ such that n is divisible by m^2.

Informally, n contains a square if it's a multiple of one of $4, 9, 16, 25, \ldots$.

The key phrase is 'if there is an integer $m > 1$'.

Thus to show that n *does* contain a square, we only need an *example* of such an m. To show that n *doesn't* contain a square, we need some sort of *argument*.

Example: 180 contains a square. For $180 = 4 \times 45$, so 180 is divisible by 4, and $4 = 2^2$.

(In fact 180 is also divisible by $9 = 3^2$, but we've already shown it contains a square, so there's no need to mention this.)

The second example is of an integer which doesn't contain a square. Since we can't possibly check every integer $m > 1$ and show that n isn't divisible by m^2, we need some sort of *argument*. In this case it's a simple one, which just says that we only need to consider a few small values of m. Nevertheless, it's clearly more than we had to do in the first example.

Example: 10 doesn't contain a square. For suppose $m > 1$ is any integer. If $m \geq 4$ then $m^2 \geq 16 > 10$, so 10 certainly can't be divisible by m^2. Hence we only need to consider $m = 2$ and $m = 3$. As in the lecture notes, we can check that 10 is not divisible by $2^2 = 4$ or by $3^2 = 9$, and hence 10 doesn't contain a square.

Example: Perron-Frobenius

The definition in this section is more complicated, but it has the advantage that you don't need to worry over questions about what you are and aren't allowed to assume about integers. You do, however, need to be able to multiply matrices...

Definition: Let M be an square matrix with non-negative integer entries. Then M is *Perron-Frobenius* if there is an integer $k \geq 1$ such that all of the entries of M^k are positive.

This definition is about square matrices containing only whole numbers bigger than or equal to 0, e.g.

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \qquad \text{or} \qquad \begin{pmatrix} 1 & 0 & 3 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

Such a matrix is Perron-Frobenius if some power of it doesn't contain any 0s. Perron-Frobenius matrices have lots of nice properties (which don't concern us here): it's therefore important to be able to decide whether or not a given matrix is Perron-Frobenius – if it is, then all the nice properties come for free.

The key phrase in the definition is 'if there is an integer $k \geq 1$'.

Thus to show that a matrix *is* Perron-Frobenius, we only need an *example* of such an integer k. To show that it *isn't* Perron-Frobenius, we need an *argument* saying that *whatever* k is, M^k contains some 0s.

It normally isn't 'obvious' whether or not a matrix M is Perron-Frobenius: one of the two examples above is, and the other isn't, but can you tell which is which just by looking at them?

Examples

a) $M = \begin{pmatrix} 1 & 0 & 3 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$.

Private work:

$$M^2 = \begin{pmatrix} 1 & 3 & 6 \\ 1 & 0 & 3 \\ 1 & 1 & 1 \end{pmatrix}, \quad M^3 = \begin{pmatrix} 4 & 6 & 9 \\ 1 & 3 & 6 \\ 2 & 1 & 4 \end{pmatrix}.$$

We're done!

Public work: Since

$$M^3 = \begin{pmatrix} 4 & 6 & 9 \\ 1 & 3 & 6 \\ 2 & 1 & 4 \end{pmatrix}$$

has all positive entries, M is a Perron-Frobenius matrix.

b) $M = \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix}$.

Private work:

$$M^2 = \begin{pmatrix} 1 & 0 \\ 3 & 4 \end{pmatrix}, \quad M^3 = \begin{pmatrix} 1 & 0 \\ 7 & 8 \end{pmatrix}, \quad M^4 = \begin{pmatrix} 1 & 0 \\ 15 & 16 \end{pmatrix}.$$

It looks as though the top row of M^k is always $1 \quad 0$. If we can show this, then M is certainly not Perron-Frobenius, since M^k will always contain a 0. How can we show it? Let's take $N = \begin{pmatrix} 1 & 0 \\ a & b \end{pmatrix}$ to be any matrix with a top row of this form. Then

$$MN = \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ a & b \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 2a+1 & 2b \end{pmatrix}.$$

So each time we multiply by M, the top row remains $1 \quad 0$.

Public work: M is not Perron-Frobenius, since the top row of M^k is $1 \quad 0$ for *any* integer k. To see why this is so, notice that when we multiply any matrix with top row $1 \quad 0$ by M, the top row remains $1 \quad 0$:

$$\begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ a & b \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 2a+1 & 2b \end{pmatrix}.$$

If you didn't follow the details of this argument it's not so important. What is important is the general principle: *If a definition says 'there exists something with a certain property', then to show the definition is satisfied we only need an example of something with that property; to show that it isn't satisfied, we need an argument.*

Incidentally, the argument in example b) could be better expressed using *induction*, which is taught in MATH142.

Remarks on an alternative definition of *divides*

The definition of *divides* could also have been given like this:

Definition: Let m and n be integers. Then m *divides* n if $n = 0$, or if $m \neq 0$ and n/m is an integer.

This is certainly easier to handle if you want to check whether or not m divides n. Since there isn't a 'there exists' clause, you never have to provide an argument: just divide n by m and see whether or not the result is an integer. For example, 2 doesn't divide 5, since $5/2 = 2.5$ is not an integer. However, this definition is not generally used: here are three good reasons why (in increasing order of importance).

a) Having to deal separately with the cases when m or n are 0 makes the definition less clear.

b) The definition takes us outside the number system which it pertains to. This definition is about *integers*, and in its original form didn't require us to know about anything else. The new definition requires us to be able to divide any integer by any other (non-zero) integer, for which we need rational numbers.

c) The original definition is easier to *generalize* to other situations. For example

   Definition: Let M and N be 2×2 matrices with integer entries. Then M *divides* N if there is a 2×2 integer matrix K such that $N = KM$.

   Definition: let $f(x)$ and $g(x)$ be polynomials with integer coefficients. Then $f(x)$ *divides* $g(x)$ if there is a polynomial $h(x)$ with integer coefficients such that $g(x) = h(x)f(x)$.

   It isn't always possible to divide one matrix by another (i.e. to work out N/M), so we can't use the second form of the definition of 'divides'.

   Having the different definitions look exactly the same is more than just aesthetically pleasing. It's likely that arguments about divisibility of integers will carry over without change to arguments about divisibility of matrices and polynomials. If there's any chance of being lazy, we should take it.

Of course, keeping the first definition of *divides* shouldn't prevent us from using the second to check whether or not m divides n, *provided* we're convinced that the two definitions really are just different ways of saying the same thing.

2.2 Definitions of structures

We start with a couple of additional examples of checking whether or not a relation is an equivalence relation. Then a new example of a 'structural' definition, that of a *metric space* is presented: the emphasis is again on the 'key phrase' in the definition, and the different strategies for showing that it is or isn't satisfied. Finally, we fill out the details in the definition of a *ring*, mentioned in lectures.

Equivalence relations: additional examples

a) $X = \mathbb{Z}$, $x\,R\,y$ if $x|y$.

   Private work:

   Reflexive? $x|x$*? Yes, every number is divisible by itself.*

   Symmetric? If $x|y$*, must* $y|x$*? No. e.g.* $1|2$ *but* $2 \nmid 1$.

   Public work: R is not an equivalence relation. For $1|2$ but $2 \nmid 1$, so symmetry fails.

b) $X = \mathbb{Z}$, $x\,R\,y$ if $x|y$ and $y|x$.

Private work:

Reflexive? Yes, this just says '$x|x$ and $x|x$'.

Symmetric? If $x\,R\,y$ (i.e. $x|y$ and $y|x$), is it true that $y\,R\,x$ (i.e. $y|x$ and $x|y$)? Yes, since these two statements are just different ways of saying the same thing.

Transitive? Suppose $x\,R\,y$ and $y\,R\,z$ (i.e. $x|y$, $y|x$, $y|z$, and $z|y$). Is it true that $x\,R\,z$ (i.e. $x|z$ and $z|x$). Yes. Since $x|y$ and $y|z$, z is divisible by y and y is divisible by x, so z must be divisible by x, i.e. $x|z$. Similarly, $y|x$ and $z|y$ tells us that $z|x$.

Public work: R is an equivalence relation. For let x, y, z be any elements of $\mathbb{Z}$. Then

Reflexive $x\,R\,x$ since $x|x$ and $x|x$ (any integer divides itself).

Symmetric If $x\,R\,y$ then $y\,R\,x$, since both of these say exactly that $x|y$ and $y|x$.

Transitive Suppose $x\,R\,y$ and $y\,R\,z$. That is, i) $x|y$; ii) $y|x$; iii) $y|z$; and iv) $z|y$. i) and iii) give $x|z$, while ii) and iv) give $z|x$. Hence $x\,R\,z$.

Example: metric spaces

The notion of *distance* is a common and useful one. We can talk about the distance between two points on a line, along a curve, in the plane, on the surface of a sphere, in three-dimensional space; and we can talk about the distance between two functions $f(x)$ and $g(x)$ (perhaps defined as the greatest value of $|f(x) - g(x)|$), the distance between two matrices, etc. In general, to describe the distance between elements of a set X, we have a function $d(x, y)$ which tells us the distance from x to y.

In order to conform with our intuitive notion of what distance means, certain properties should hold:

a) The distance between any two different points should be > 0 (and the distance from a point to itself should be 0).

b) The distance from x to y should be the same as the distance from y to x.

c) Going from x to y via z should be at least as far as going directly from x to y. That is, the distance from x to y should be no greater than the distance from x to z plus the distance from z to y.

These properties are the ones used in the definition of a metric space:

Definition: Let X be a set, and $d(x,y)$ be a function (with $x,y \in X$). Then (X,d) is a *metric space* if for all $x,y,z \in X$,

a) $d(x,x) = 0$, and if $x \neq y$ then $d(x,y) > 0$.

b) $d(x,y) = d(y,x)$.

c) $d(x,y) \leq d(x,z) + d(z,y)$.

You should think of the notation (X,d) as meaning 'X and d together'. Metric space theory starts only from the assumption that these three properties are true: it is a large and far-reaching theory, and its conclusions apply to the examples mentioned above and to many others.

The key phrase is 'for all $x,y,z \in X$'.

To show that (X,d) *isn't* a metric space, all we need is to find an *example* of x, y, and z such that a *single* one of the conditions a), b), and c) fails. To show that (X,d) *is* a metric space, we need an *argument* showing that for *any* choice of x, y, and z, *all* of a), b), and c) hold. This can be a lot of work...

Example: Let $X = \mathbb{R}$, and $d(x,y) = x + y$.

Private work: adding two numbers together doesn't look like a sensible way of defining a distance between them, but let's see.

a) Is $d(x,x) = x + x$ always equal to 0? No, for example if $x = 1$.

Public work: (X,d) is not a metric space. For if $x = 1$ then $d(x,x) = 1 + 1 = 2 \neq 0$, so condition a) fails.

Example: Let $X = \mathbb{R}$, and $d(x,y) = |x - y|$.

This is the 'usual' notion of the distance between two real numbers x and y: we subtract the two numbers, and if the answer is negative we change its sign. We should therefore hope that (X,d) is a metric space. Here's an *argument* saying that it is.

Public work: (X,d) is a metric space. For let x,y,z be any real numbers. Then

a) $d(x,x) = |x - x| = 0$. If $x \neq y$ then $x - y \neq 0$, so $|x - y| > 0$. Hence $d(x,y) > 0$.

b) $d(x,y) = |x - y| = |-(x - y)| = |y - x| = d(y,x)$.

c) is harder. One (tedious) way to do it is to consider each of the six possible orderings of x, y, and z separately. These are: $x \leq y \leq z$, $x \leq z \leq y$, $y \leq x \leq z$, $y \leq z \leq x$, $z \leq x \leq y$, and $z \leq y \leq x$. Let's take, for example, $y \leq x \leq z$. Then $d(x, y) = x - y \leq z - y = d(z, y)$, so certainly $d(x, y) \leq d(x, z) + d(z, y)$. As another example, if $y \leq z \leq x$, then $d(x, y) = x - y = (x - z) + (z - y) = d(x, z) + d(z, y)$, so again $d(x, y) \leq d(x, z) + d(z, y)$. The other four possibilities can be treated similarly.

Example: Let $X = \mathbb{R}$, and define $d(x, y) = 1$ if $x \neq y$, $d(x, y) = 0$ if $x = y$.

Private work: Any two different numbers are distance 1 apart! Let's see...

a) $d(x, x) = 0$ *and if* $x \neq y$ *then* $d(x, y) = 1 > 0$. *Good.*

b) Both $d(x, y)$ *and* $d(y, x)$ *are* 1 *if* x *and* y *are different, and* 0 *if they're the same. So* $d(x, y) = d(y, x)$.

c) How could it be possible that $d(x, y) > d(x, z) + d(z, y)$*? Since each of the terms is either* 0 *or* 1*, this could only happen if* $d(x, y) = 1$ *and both* $d(x, z)$ *and* $d(z, y)$ *are* 0*. But this is impossible, since if* $d(x, z)$ *and* $d(z, y)$ *are both* 0*, then* $x = z$ *and* $z = y$*, so* $x = y$ *which gives* $d(x, y) = 0$.

Public work: (X, d) is a metric space. For let x, y, z be any real numbers. Then

a) $d(x, x) = 0$, and if $x \neq y$ then $d(x, y) = 1 > 0$.

b) If $x = y$ then $d(x, y) = d(y, x) = 0$. If $x \neq y$ then $d(x, y) = d(y, x) = 1$.

c) If x, y, and z are all equal then $d(x, y) = d(x, z) = d(z, y) = 0$, and so

$$0 = d(x, y) \leq d(x, z) + d(z, y) = 0.$$

If they're not all equal, then either $d(x, z) = 1$ or $d(z, y) = 1$. Hence

$$d(x, y) \leq 1 \leq d(x, z) + d(z, y).$$

Example: Rings

In the lectures, we used the idea of a ring to motivate structural definitions. However, the actual definition is too complicated (or at least too long) to treat in lectures. It is given here for interest. Note that this definition isn't meant to be 'obvious': rather than popping out of some clever person's head, it took many years of experimentation to formulate.

Definition: Let R be a set such that any two elements x, y can be added to give an element $x+y$ of R, and multiplied to give an element xy of R. Then R is a *Ring* if:

Properties of Addition

a) For all $x, y \in R$, $\quad x+y=y+x$.

b) For all $x, y, z \in R$, $\quad x+(y+z)=(x+y)+z$.

c) There is an element 0 of R such that for all $x \in R$, $\quad x+0=x$.

d) For all $x \in R$ there is an element w of R such that $\quad x+w=0$.

Property of multiplication

e) For all $x, y, z \in R$, $\quad x(yz)=(xy)z$.

Mixed property

f) For all $x, y, z \in R$, $\quad x(y+z)=xy+xz \quad$ and $\quad (x+y)z=xz+yz$.

The key phrases in the definition are the many occurences of 'for all'.

To show that a set R *is* a ring, we need an *argument* showing that *all* of these properties hold for *all* choices of x, y, z. To show that R *isn't* a ring, we only need an *example* of a *single* property in a) − f) which fails for a *single* choice of x, y, z.

Thus, for example, $\mathbb{N}$ is not a ring. For property d) fails: if we take $x=1 \in \mathbb{N}$, there is no element w of $\mathbb{N}$ with $1+w=0$ (since -1 does not belong to $\mathbb{N}$). This is all that is required: whether or not $\mathbb{N}$ satisfies the other properties (it does) is irrelevant.

As mentioned in lectures, there are many examples of rings: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, the set of square matrices of a given size with integer entries, the set of (real) functions, the set of polynomials with integer coefficients, the set of integers mod 15 (or mod anything else), and so on. To show that each of these is a ring requires a long and tedious argument, verifying each of a) − f) separately for all possible choices of x, y, z. However, the work is well worth while. Anything that we can show to be true using only properties a) − f) above applies to all of these different examples. By giving all the sets the same name, 'Ring', we can work with all of them at the same time.

Notice, by the way, that the definition makes no mention of subtraction. The key to this is property d), which says that for every x there's some w with $x+w=0$. We'd normally give w the name '$-x$'. Then we can define subtraction by saying that $y-x$ means exactly the same as $y+(-x)$.

Appendix: Assumptions made in simple definitions

One of the problems with treating very simple and familiar examples like *odd*, *even*, *divisible*, and *prime* as examples of definitions is that it can leave you unsure about what you are and are not allowed to assume about numbers: after all, if we aren't allowed to assume that we know 37 is odd just by looking at it, why should we be allowed to assume (for example) that if we add 1 to a number then it gets bigger?

Here is a list of what we will take for granted (in this module) when dealing with such simple definitions about integers:

- That we know what the integers are, and how to add, subtract, and multiply them. (But *not* divide: after all, that needs rational numbers.)
- That all the 'usual rules' of arithmetic hold: e.g. that $m+n = n+m$, that $m(n+p) = mn+mp$, etc. (More precisely, that the integers are a *ring* (see above), and also satisfy $mn = nm$ for all m, n.)
- That we know the meaning of $<$, $\leq$, $>$, and $\geq$.
- That the 'usual rules' for manipulating inequalities hold: e.g. that if $m < n$ then $m + p < n + p$ for any p; that if $m < n$ and $p > 0$ then $mp < np$, etc.

3 Theorems

Terms Introduced

Theorem A theorem is a true statement. Psychologically, the word 'theorem' suggests that the statement is important and not obvious.

If ... Then theorem An *if ... then* theorem is a true statement of the form 'if P then Q', where P and Q are statements.

Hypothesis/Conclusion [4] The *hypothesis* of an if ... then theorem 'if P then Q' is the statement P. The *conclusion* is the statement Q.

Context The *context* of an if ... then theorem is the part of the theorem statement which is required in order for each of the hypothesis and conclusion to make sense in isolation.

Converse The *converse* of an if ... then theorem 'if P then Q' is the statement 'if Q then P'. *It is not necessarily true.*

Contrapositive The *contrapositive* of an if ... then theorem 'if P then Q' is the statement 'if not(Q) then not(P)'. *It is just another way of stating the theorem, and so is always true.*

Things to remember

1. **THE MANTRA**. The converse of a theorem is not necessarily true. The contrapositive is always true.

2. When faced with an if ... then theorem, especially when you are to apply it to some particular problem, start by identifying the context, hypothesis, and conclusion; and by writing down the contrapositive.

3.1 Examples of If ... Then theorems

This section contains two further examples of analyzing an if ... then theorem: the first is an 'obvious' theorem, and the second is deliberately chosen to be meaningless at present.

[4]The terms *hypothesis conclusion*, and *context* aren't well defined. Theorems can usually be stated in many different (equivalent) ways, each of which gives different 'obvious' identifications of context, hypothesis, and conclusion.

Note that in order to formulate the contrapositive of a theorem, it is necessary to be able to negate statements accurately. If you're unsure about this, you should review your notes on negation.

Example:

Theorem 1 *Let m and n be integers. If m is even or n is even, then mn is even.*

Context $m, n \in \mathbb{Z}$.

Hypothesis m is even or n is even.

Conclusion mn is even.

Since the negation of 'k is even' is 'k is odd'; and the negation of 'P or Q' is 'not(P) and not(Q)', the hypothesis has negation 'm is odd and n is odd'. (Note that this is precisely saying that it is not true that 'm is even or n is even'.) Hence

Contrapositive

Let m and n be integers. If mn is odd then m is odd and n is odd.

Since the contrapositive is just another way of stating the theorem, it is necessarily true.

Converse

Let m and n be integers. If mn is even then m is even or n is even.

In this case, the converse is true: however, you should remember (see the example in your lecture notes) that this is not always the case.

Example:

Theorem 2 *Let X be a T_2 space. If X is first countable and X is countably compact, then X is T_3.*

This theorem includes the terms 'T_2 space', 'first countable', 'countably compact' and 'T_3' which aren't familiar to us. However, this is no obstacle to analysing it.

Context X is a T_2 space.

Hypothesis X is first countable and X is countably compact.

Conclusion X is T_3.

To formulate the contrapositive, remember the rule for negating a statement involving 'and'. We get

Contrapositive

Let X be a T_2 space. If X is not T_3, then either X is not first countable, or X is not countably compact.

Even though we have no idea what this means, we know that it is true. The same is not true of the converse:

Converse

Let X be a T_2 space. If X is T_3 then X is first countable and X is countably compact.

Since *the converse of a theorem need not be true*, we have no idea whether or not this is a true statement without understanding what the terms mean. (In fact, it is false.)

3.3 Applying theorems

In many modules, you're presented with a number of theorems which constitute the 'main content' of the module (even if they're not called 'theorems': remember, a theorem is nothing more than a 'true statement', or a 'fact'). You are then asked to apply these theorems to particular problems.

Much of the time this is just common sense, but it can nevertheless require careful thought to avoid applying them wrongly (most commonly, by taking them to say more than they actually do say). For example, with an if . . . then theorem, you should

- Check that the problem you're working on agrees with the context of the theorem (for example, if the theorem is about real numbers, then it isn't going to help you directly if you're working with complex numbers).
- Identify the hypothesis and conclusion, and check that the hypothesis is satisfied for the particular example you're working with. (If so, you know the conclusion must be true.)
- Resist the temptation to assume that the converse is true (unless you know this to be the case).
- Remember that it may be useful to work from the contrapositive rather than the theorem itself.

In lectures, an example was given in which the theorem took the form 'If P and Q then R'. The example here is of a theorem of the form 'If P then Q or R'. The example in the lecture notes was deliberately chosen so that the terms used were unfamiliar: this illustrates that applying a theorem in this way can be an entirely logical process, which doesn't require understanding what the theorem actually means. The example presented here, by contrast, uses familiar terms and should be 'obvious'. The disadvantage of such an example is that it requires discipline to draw our conclusions solely from the theorem, and not from all the other things we know about real numbers.

Theorem 3 *Let a, b, and c be real numbers. If $ab > ac$ then $a < 0$ or $b > c$.*

Context $a, b, c \in \mathbb{R}$.

Hypothesis $ab > ac$.

Conclusion $a < 0$ or $b > c$.

To write down the contrapositive, recall that the negation of '$a < 0$ or $b > c$' is '$a \geq 0$ **and** $b \leq c$'. Since the negation of '$ab > ac$' is $ab \leq ac$, we have:

Contrapositive

Let a, b, and c be real numbers. If $a \geq 0$ and $b \leq c$ then $ab \leq ac$.

The contrapositive is just another way of stating the theorem, so it must be true.

What, if anything, does the theorem tell us about real numbers a, b, and c when

a) $ab > ac$?

b) $a < 0$ or $b > c$?

c) $ab > ac$ and $b < c$?

d) $a \geq 0$ and $ab > ac$?

e) $ab \leq ac$?

To answer these questions, we use the statements of the theorem (or its contrapositive, if that's easier – the two are just different ways of writing the same thing).

a) It tells us that $a < 0$ or $b > c$ (this is just the statement of the theorem).

b) It tells us nothing: this situation doesn't fit the hypothesis of either the theorem or its contrapositive.

c) It tells us that $a < 0$. Using the theorem, the fact that $ab > ac$ tells us that either $a < 0$ or $b > c$; since we're told that $b < c$, it must be the case that $a < 0$.

d) It tells us that $b > c$. As in c), the fact that $ab > ac$ tells us that either $a < 0$ or $b > c$; since we're told $a \geq 0$, it must be the case that $b > c$.

e) It tells us nothing: this situation doesn't fit the hypothesis of either the theorem or its contrapositive.

Note that the converse of this theorem is false:

Converse

Let a, b, and c be real numbers. If $a < 0$ or $b > c$ then $ab > ac$

This is false: for if $a = 0$, $b = 2$, and $c = 1$ then the hypothesis is satisfied (since $b > c$), but $ab = ac = 0$, so it is not true that $ab > ac$.

The converse of a theorem is not necessarily true.

3.4 Some words

You will often see alternative words used instead of 'theorem': the most common examples are 'lemma', 'corollary', and 'proposition'. Remember that a theorem is nothing more than a 'true statement', or a 'fact' – a writer (or lecturer) chooses between these words to help the reader (or student) understand how that fact fits into the grand scheme of things. Roughly speaking, the different terms have the following connotations:

Theorem A fact of some significance, not immediately 'obvious', likely to be useful in a wide variety of contexts.

Lemma A fact which is temporarily useful (perhaps in proving a particular theorem, or in carrying out calculations in some restricted context), but which doesn't usually have the wide relevance of a theorem. It may be 'obvious', but need not be. (It comes from a Greek word, meaning 'something taken for granted'.)

Corollary A fact normally of the same significance and relevance as a theorem, but which follows easily from a theorem or lemma which has already been shown to be true. (It comes from the Latin word *corollarium*, meaning 'tip': an additional bonus payment for the work you've done.)

Proposition In logic, the word 'proposition' means a statement with no free variables (i.e. one which is either true or false, but *not necessarily true*). Some mathematicians, however, use it to mean much the same as 'theorem'.

4 Proofs

When you have eliminated the impossible, whatever remains, however improbable, must be the truth.
Arthur Conan Doyle (1859 – 1930)

Things to remember

1. Proving things is difficult. The aim of this chapter is to help you to understand the logic of different types of proof, so that when you come across them in other modules you can follow the *idea* of what it is that the lecturer is trying to do, even if the details are obscure. In order to achieve this, you are asked to construct short proofs of your own.

2. Many people object that they don't know where to start when asked to prove a statement. Start by identifying the *givens* (the context and hypothesis in the case of an if . . . then theorem) and the *goal* (the conclusion of an if . . . then theorem). The aim is then to work from the givens towards the goal.

3. A good technique when the goal contains 'or' is to negate one part of the 'or' statement and move it into the givens. This depends on the fact that
$$P \text{ or } Q$$
means exactly the same as
$$\text{if not}(P) \text{ then } Q.$$

4. Sometimes, especially when the goal is more complicated than the givens, the easiest way to see how to prove a statement is to *work backwards:* start with the goal and work towards the givens. When you write down the final proof, however, you should always work from givens to goal.

5. *Proof by contradiction* works by assuming the theorem to be false, and arriving at a statement you know to be false (a contradiction). Move the negation of the goal into the givens column, and write 'Contradiction' in the goal column.

4.1 Direct Proof

This section contains two more examples of direct proofs. As in lectures, the results proved will be 'obvious'. The disadvantage with such examples is that they can lead to confusion about what you can and can't assume to be true. For instance, can you assume that $x + 1 > x$? That if you add two even numbers you get an even number? That every positive integer can be factorized into primes in just one way? Most proofs you see in other modules would take it for granted that all of these things are true, but in this module (particularly when dealing with 'obvious' examples), we will normally only assume the first. As a guide, if a theorem is about even numbers or divisibility (for example), you should work from the definitions of these terms rather than assuming the things we all know about them to be true. For a more complete answer, see the appendix on 'Assumptions made in simple definitions' in Chapter 2 of these notes.

Example: This example shows a direct proof which is a little more complicated than the one in lectures.

Theorem 1 *Let* $m, n \in \mathbb{Z}$. *If* $m|n$ *and* $n|m$ *then* $n = \pm m$.

Given	**Goal**
$m, n \in \mathbb{Z}$	$n = \pm m$
$m\|n$	
$n\|m$	

As discussed above, the fact that this 'obvious' result is about divisibility indicates that we should work from the definition of that term. Recall that '$m|n$' means that there is an integer k with $n = km$; similarly, '$n|m$' means that there is an integer ℓ with $m = \ell n$.

Given	**Goal**
$m, n \in \mathbb{Z}$	$n = \pm m$
There is an integer k with $n = km$	
There is an integer ℓ with $m = \ell n$	

Now we can see how the proof should work. If $n = km$ and $m = \ell n$ then $n = k(\ell n)$, i.e. $n = (k\ell)n$, so *either* $n = 0$ (in which case $m = \ell n = 0$, so $n = m$), *or* $k\ell = 1$ (in which case $k = \pm 1$, giving $n = km = \pm m$).

Proof. Let $m, n \in \mathbb{Z}$, and suppose that $m|n$ and $n|m$: thus there are integers k and ℓ such that $n = km$ and $m = \ell n$. It follows that $n = (k\ell)n$. There are now two possibilities.

i) If $n = 0$ then $m = \ell n = 0$, and so $m = n$ as required.

ii) If $n \neq 0$ then $k\ell = 1$. This means that $k \neq 0$ and $\ell \neq 0$, so that $|k| \geq 1$ and $|\ell| \geq 1$. Since $|\ell| \geq 1$ we have $|k\ell| \geq |k| \geq 1$. However $|k\ell| = |1| = 1$, so $1 \geq |k| \geq 1$, i.e. $|k| = 1$. Thus $k = \pm 1$, giving $n = km = \pm m$ as required.

∎

Notice that a little care is necessary to be sure we've considered all the possible cases. In particular *if you're going to cancel something from both sides of an equation (such as $n = (k\ell)n$), you need to consider the possibility that that something (in this case n) could be* 0.

Example: This is another example of how to deal with an 'or' in the goal.

Theorem 2 *Let $x \in \mathbb{R}$. If $x^2 > x$ then $x < 0$ or $x > 1$.*

Given	**Goal**
$x \in \mathbb{R}$	$x < 0$ or $x > 1$
$x^2 > x$	

Remember that '$x < 0$ or $x > 1$' means exactly the same as 'if not($x < 0$) then $x > 1$', i.e. 'if $x \geq 0$ then $x > 1$'. That is, we negate '$x < 0$' and move it into the givens:

Given	**Goal**
$x \in \mathbb{R}$	$x > 1$
$x \geq 0$	
$x^2 > x$	

We'd like to divide both sides of $x^2 > x$ by x to give $x > 1$. If $x > 0$ then there's no problem with this, but we're only given that $x \geq 0$. However, since we're also given that $x^2 > x$, it isn't possible to have $x = 0$.

Proof. Let $x \in \mathbb{R}$ with $x^2 > x$. Suppose it is not true that $x < 0$: since $x^2 > x$, this means that $x > 0$. Then we can divide both sides of the inequality $x^2 > x$ by x to give $x > 1$. Hence either $x < 0$ or $x > 1$ as required. ∎

You'll often see proofs presented like this, and it can be hard to understand the logic to start with: we *suppose* that $x < 0$ is false, and use this to show that $x > 1$. Hence *either* $x < 0$, *or* $x \not< 0$, from which it follows that $x > 1$.

4.2 Proof by contradiction

In the lectures, a famous proof was given showing that $\sqrt{2}$ is not a rational number: there is no $a/b \in \mathbb{Q}$ with $(a/b)^2 = 2$. In this section, it will be shown how essentially the same argument can be used to prove that $\sqrt[3]{2}$ and $\sqrt{3}$ are also not rational. The arguments are very good examples of the logic of proof by contradiction: Question 2 on Example Sheet 5 is based on them.

In the lectures, we took it for granted that if n is an integer and n^2 is even then n is also even. This isn't hard to show, but the proof isn't very instructive. (However, the *idea* of the proof by contradiction is instructive. If n weren't even then it would be odd, but then n^2 would also be odd, which is the required contradiction. Hence n must be even.) In this section, we'll take a little bit more for granted:

Lemma 3 *Let n and k be positive integers, and p be a prime number. If n^k is divisible by p, then n is also divisible by p.*

The fact we used in lectures comes from taking $p = 2$ and $k = 2$. This lemma is surprisingly difficult to prove without making any initial assumptions. However, you can convince yourself that it is true from the fact that every positive integer can be factored into primes in just one way: the prime factorization of n^k must just consist of all the prime factors of n repeated k times, so if p is one of the prime factors of n^k it must also be one of the prime factors of n.

Theorem 4 ($\sqrt[3]{2}$ is irrational) *Let $\frac{a}{b} \in \mathbb{Q}$. Then $\left(\frac{a}{b}\right)^3 \neq 2$.*

Given	**Goal**
$\frac{a}{b} \in \mathbb{Q}$	$\left(\frac{a}{b}\right)^3 \neq 2$

For a proof by contradiction, we negate the goal and move it in with the givens:

Given	**Goal**
$\frac{a}{b} \in \mathbb{Q}$ $\left(\frac{a}{b}\right)^3 = 2$	Contradiction

Proof. Let $\frac{a}{b} \in \mathbb{Q}$, and assume for a contradiction that $\left(\frac{a}{b}\right)^3 = 2$. We can also assume that at least one of a and b is odd (if they're both even, we can cancel 2 from the top and bottom of the fraction).

Thus $\frac{a^3}{b^3} = 2$, or $a^3 = 2b^3$.

So a^3 is divisible by 2, and by Lemma 3 (with $p = 2$ and $k = 3$) it follows that a is also divisible by 2: that is, $a = 2k$ for some integer k.

Now the equation $a^3 = 2b^3$ gives $(2k)^3 = 2b^3$, or $8k^3 = 2b^3$, i.e. $4k^3 = b^3$.

Thus b^3 is divisible by 2, and by Lemma 3 it follows that b is also divisible by 2. Hence both a and b are even. This is the required contradiction. ∎

Theorem 5 ($\sqrt{3}$ is irrational) *Let* $\frac{a}{b} \in \mathbb{Q}$. *then* $\left(\frac{a}{b}\right)^2 \neq 3$.

Given	**Goal**
$\frac{a}{b} \in \mathbb{Q}$ $\left(\frac{a}{b}\right)^2 = 3$	Contradiction

The proof is almost exactly the same, except now we're interested in divisibility by 3 rather than divisibility by 2 (i.e. evenness/oddness).

Proof. Let $\frac{a}{b} \in \mathbb{Q}$, and assume for a contradiction that $\left(\frac{a}{b}\right)^2 = 3$. We can also assume that a and b are not both divisible by 3 (if they are, we can cancel 3 from the top and bottom of the fraction).

Thus $\frac{a^2}{b^2} = 3$, or $a^2 = 3b^2$.

So a^2 is divisible by 3, and by Lemma 3 (with $p = 3$ and $k = 2$) it follows that a is also divisible by 3: that is, $a = 3k$ for some integer k.

Now the equation $a^2 = 3b^2$ gives $(3k)^2 = 3b^2$, or $9k^2 = 3b^2$, i.e. $3k^2 = b^2$.

Thus b^2 is divisible by 3, and by Lemma 3 it follows that b is also divisible by 3. Hence both a and b are divisible by 3. This is the required contradiction. ∎

The three proofs dealing with $\sqrt{2}$, $\sqrt[3]{2}$, and $\sqrt{3}$ are very similar: question 2 on Example Sheet 5 asks you to extend the argument to the most general result that you can. It is worthwhile asking yourself what would go wrong with the argument if you tried to use it to show that $\sqrt{4}$ is irrational (which it clearly isn't!).

Note, by the way, that we have only shown that $\sqrt{2}$, $\sqrt[3]{2}$, and $\sqrt{3}$ are not rational numbers: we have not shown (for example) that there is a *real* number x with $x^2 = 2$. This seemingly obvious fact can only be shown to be true with a much better appreciation of what the real numbers 'really' are than our mental picture of 'all the numbers making up the whole line'. This topic is treated in MATH241 next year.

5 Quantifiers

For every action there exists an equal and opposite reaction.
Isaac Newton (1642 – 1727)

Terms Introduced

Universal Quantifier The *universal quantifier* $\forall$ means "For all".

Existential Quantifier The *existential quantifier* $\exists$ means "There exists".

Things to remember

1. **THE MANTRA**. The order of quantifiers matters.

2. To negate a statement with quantifiers,

   i) Switch each $\forall$ to $\exists$ and vice-versa.

   ii) Negate the final part of the statement.

3. When trying to decide (and prove) whether a statement with quantifiers is true or false, it can be helpful to imagine playing the quantifier game. The enemy picks $\forall$s, and you pick $\exists$s.

4. i) To prove that a statement starting "$\forall x \in S$" is true, you need an *argument* dealing with all possible values of x. To prove that it's false, you only need an *example* of a bad value of x.

   ii) To prove that a statement starting "$\exists x \in S$" is true, you only need an *example* of a suitable x. To prove that it's false, you need an *argument* showing that there is no suitable value of x.

5. $\exists$ implicitly includes "such that", so you should write

$$\exists n \in \mathbb{Z},\, n^2 = 4$$

   rather than

$$\exists n \in \mathbb{Z} \text{ such that } n^2 = 4.$$

5.1 Simple use of quantifiers

Here are a few more examples of statements with a single quantifier. It's important to be able to understand quickly what these mean, before going on to more advanced examples with two or more quantifiers.

a) $\exists n \in \mathbb{Z}$, $n^2 = 5$.

"There exists an integer n such that $n^2 = 5$." This statement is false: $\sqrt{5}$ is not an integer.

b) $\forall x \in \mathbb{R}$, $\cos x < 2$.

"For all real numbers x, $\cos x < 2$." This statement is true: $\cos x$ is between -1 and 1 for all real numbers x.

c) $\forall x \in \mathbb{R}$, $f(x) \geq 0$.

"For all real numbers x, $f(x) \geq 0$." This statement has the function $f(x)$ as a free variable: we can't say whether it's true or false until we know what $f(x)$ is. For example, it's true if $f(x) = x^2$ or $f(x) = e^x$, but false if $f(x) = \sin x$ or $f(x) = x^3$.

d) $\exists x \in \mathbb{R}$, $f(x) = -2$.

"There exists a real number x such that $f(x) = -2$." Once again, $f(x)$ is a free variable. The statement is true if $f(x) = x$ or $f(x) = \log x$, but is false if $f(x) = x^2$ or $f(x) = \cos x$.

5.3 Statements with two or more quantifiers

This section contains some more relatively straightforward examples of the 'quantifier game'.

a) $\forall n \in \mathbb{Z}$, $\exists m \in \mathbb{Z}$, $mn > 0$.

The game:

i) The enemy picks an integer n.

ii) You try to pick an integer m with $mn > 0$.

If you can always win, then the statement is true. If the enemy can win (by a clever choice of n), then the statement is false.

Enemy $n = 3$.

You $m = 1$. ($mn = 3 > 0$.)

Enemy $n = -5$.

You $m = -1$. ($mn = 5 > 0$.)

Enemy (Aha!) $n = 0$.

You Surrender.

If the enemy picks $n = 0$, any value of m you choose will give $mn = 0 \not> 0$. Hence the enemy can win, and the statement is false.

Theorem 1 *The statement*

$$\forall n \in \mathbb{Z}, \exists m \in \mathbb{Z}, mn > 0$$

is false.

Proof. Let $n = 0 \in \mathbb{Z}$. Then for any $m \in \mathbb{Z}$ we have $mn = 0 \not> 0$. ∎

Notice that the proof says exactly that the negation of the statement:

$$\exists n \in \mathbb{Z}, \forall m \in \mathbb{Z}, mn \leq 0$$

is true. There exists an integer n (namely $n = 0$) such that for any $m \in \mathbb{Z}$ it is not true that $mn > 0$.

b) $\forall n \in \mathbb{Z}, \exists m \in \mathbb{Z}, m + n > 100$.

The game:

i) The enemy picks an integer n.

ii) You try to pick an integer m with $m + n > 100$.

If you can always win, the statement is true. If the enemy can win (by a clever choice of n), then the statement is false.

Enemy $n = 1$.

You $m = 100$. ($m + n = 101 > 100$.)

Enemy $n = -50$.

You $m = 151$. ($m + n = 101 > 100$.)

Enemy $n = -10000$.

You $n = 10101$. $(m + n = 101 > 100.)$

Enemy Surrender.

To *prove* that the statement is true, we need a strategy telling us how to respond to any enemy n. The above plays suggest a good one: pick $m = 101 - n$ so $m + n = 101 > 100$.

Theorem 2

$$\forall n \in \mathbb{Z}, \exists m \in \mathbb{Z}, m + n > 100.$$

Proof. Let n be any integer, and set $m = 101 - n$. Then $m + n = 101 > 100$. ∎

c) $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, x < y^3$.

(Compare this with the example in lectures where $x < y^3$ was replaced by $x < y^2$.)

The game:

i) You pick a real number x.

ii) The enemy tries to pick a real number y with $x \geq y^3$.

If you can win (by a clever choice of x), the statement is true. If the enemy can always win, then the statement is false.

You $x = 1$.

Enemy $y = 1$. $(1 \geq 1^3 = 1.)$

You $x = 0$.

Enemy $y = 0$. $(0 \geq 0^3 = 0.)$

You $x = -1$.

Enemy $y = -1$. $(-1 \geq (-1)^3 = -1.)$

You $x = -10$.

Enemy $y = \sqrt[3]{-10}$. $(-10 \geq (\sqrt[3]{-10})^3 = -10.)$

You (Now I see her evil strategy) Surrender.

To prove the statement is false, you have to give the enemy strategy for responding to any x you come up with. It's fiendishly simple: she just says $y = \sqrt[3]{x}$.

Theorem 3 *The statement*

$$\exists x \in \mathbb{R},\ \forall y \in \mathbb{R},\ x < y^3$$

is false.

Proof. Let x be any real number and take $y = \sqrt[3]{x}$. Then $y^3 = x$, so it is not true that $x < y^3$. ∎

Notice that the proof says exactly that the negation of the statement:

$$\forall x \in \mathbb{R},\ \exists y \in \mathbb{R},\ x \geq y^3$$

is true. For *any* real number x, there exists a real number y (namely $y = \sqrt[3]{x}$) such that $x < y^3$ is false. The difference with the example treated in lectures is that any real number x has a real cube root, but negative numbers x don't have a real square root.

5.4 Negating statements with quantifiers

As described in lectures, there's a general rule for negating a statement with quantifiers, which means you don't even need to try to understand the statement before you negate it: just switch every $\exists$ with $\forall$ and vice-versa, and negate the final part of the statement. Two examples have already been included in Section 5.3 above: here are two more.

a) P : $\forall x \in \mathbb{R},\ \exists y \in \mathbb{R},\ f(y) = x.$

not(P) : $\exists x \in \mathbb{R},\ \forall y \in \mathbb{R},\ f(y) \neq x.$

(For those doing MATH142, P says exactly that the (real) function $f(x)$ is *surjective*: every real number x is $f(y)$ for some real number y. Hence not(P) says exactly that $f(x)$ is *not* surjective: there is a real number x which is not equal to $f(y)$ for *any* value of y.)

b) P : $\forall \epsilon > 0,\ \exists N \in \mathbb{N},\ \forall n \geq N,\ \forall x \in \mathbb{R},\ |f_n(x) - f(x)| < \epsilon.$

not(P) : $\exists \epsilon > 0,\ \forall N \in \mathbb{N},\ \exists n \geq N,\ \exists x \in \mathbb{R},\ |f_n(x) - f(x)| \geq \epsilon.$

P is a very complicated statement (in fact it's the definition of what it means for a sequence $(f_n(x))$ of functions to converge uniformly to a function $f(x)$), but we don't need to understand it in order to negate it. The only point to bear in mind is that we don't change $\epsilon > 0$ to $\epsilon \leq 0$ or $n \geq N$ to $n < N$: only the final part of the statement is negated.

5.5 A 'real-life' example

This section of the notes contains details of the discussion in lectures motivating a definition, using quantifiers, of a sequence (x_n) tending to a limit L.

A (real-valued) sequence (x_n) is just a list of (real) numbers $x_1, x_2, x_3, x_4, \ldots$ going on for ever. For example, we could have

$$x_n = \frac{1}{n}$$

(so the sequence is $x_1 = 1$, $x_2 = \frac{1}{2}$, $x_3 = \frac{1}{3}$, $x_4 = \frac{1}{4}$, ...), or something more complicated like

$$x_n = \left(1 + \frac{1}{n}\right)^n.$$

Intuitively, a sequence (x_n) *tends to a limit L as $n \to \infty$* if x_n *gets as close as we like to L as n gets bigger and bigger.* For example, the sequence $\left(\frac{1}{n}\right)$ clearly tends to 0, since as n gets larger, $\frac{1}{n}$ gets closer and closer to 0.

This is a good way to think about it, since it's relatively easy to understand. However, for many purposes it isn't precise enough: for example, if x_n tends to L as $n \to \infty$ and y_n tends to $M \neq 0$ as $n \to \infty$, we might want to be sure that $\frac{x_n}{y_n} \to \frac{L}{M}$ as $n \to \infty$. Using an intuitive idea of what it means for a sequence to tend to a limit, it's impossible to argue carefully that this must be true. We therefore unpack our intuitive idea step by step to try to arrive at a precise mathematical definition.

a) What do we mean by 'as close as we like'? What we mean is that the enemy can specify *any* degree of closeness, and we have to be able to satisfy her that eventually x_n is that close to L. More precisely, for any $\epsilon > 0$ the enemy picks, no matter how small, we must be able to show that x_n is eventually within ϵ of L.

   (x_n) tends to L as $n \to \infty$ if

   $$\forall \epsilon > 0,\ x_n \text{ is eventually within } \epsilon \text{ of } L.$$

b) What does it mean for x_n to be 'eventually' within ϵ of L? If the enemy chooses ϵ to be very small, we'll have to go a long way down the sequence before we're that close to L, but eventually we should get there. Thus it means that *there exists* some (big) number N such that $x_N, x_{N+1}, x_{N+2}, \ldots$ are all within ϵ of L.

   (x_n) tends to L as $n \to \infty$ if

   $$\forall \epsilon > 0,\ \exists N \in \mathbb{N},\ x_N, x_{N+1}, x_{N+2}, \ldots \text{ are all within } \epsilon \text{ of } L.$$

   Note that the enemy has to choose ϵ before we choose N, so our N can *depend* on her ϵ.

c) Of course, there's a better way of saying that $x_N, x_{N+1}, x_{N+2}, \ldots$ are *all* within ϵ of L: that *for all* $n \geq N$, x_n is within ϵ of L.

   (x_n) tends to L as $n \to \infty$ if

$$\forall \epsilon > 0,\ \exists N \in \mathbb{N},\ \forall n \geq N,\ x_n \text{ is within } \epsilon \text{ of } L.$$

d) Finally, what does it mean for x_n to be 'within ϵ' of L? It means that x_n is between $L - \epsilon$ and $L + \epsilon$, or, more concisely, that $|x_n - L| < \epsilon$ ("the distance between x_n and L is less than ϵ").

   (x_n) tends to L as $n \to \infty$ if

$$\forall \epsilon > 0,\ \exists N \in \mathbb{N},\ \forall n \geq N,\ |x_n - L| < \epsilon.$$

This is the standard mathematical definition of what it means for a sequence to tend to a limit. It's quite incomprehensible when you're just presented with the definition, but easier to understand if you go through the steps of working out the definition for yourself. If you still find it hard to understand, take heart: it took many years for the mathematical community to arrive at and agree on this definition.

One of the nice things about the definition is that it generalizes easily. For example, x_n and L could just as well be complex numbers; and, if you read Section 2.2 of these notes (on metric spaces), x_n and L could belong to any metric space (X, d) provided we replace $|x_n - L|$ (the distance between x_n and L) with $d(x_n, L)$.

Armed with our general rule, negating the statement is easy. Since the negation of "$|x_n - L| < \epsilon$" is "$|x_n - L| \geq \epsilon$", we get

$$\exists \epsilon > 0,\ \forall N \in \mathbb{N},\ \exists n \geq N,\ |x_n - L| \geq \epsilon.$$

(We've just switched each $\forall$ with $\exists$ and each $\exists$ with $\forall$.) This is precisely the statement that x_n *doesn't tend to L as $n \to \infty$*. Unpacking it, it says that there's some $\epsilon > 0$ (which the enemy could choose) such that, whatever N we pick, there's some $n \geq N$ such that x_n isn't within ϵ of L. By picking this ϵ, the enemy could therefore win the quantifier game.

Examples

a) First, let's show that the sequence $\left(x_n = \frac{1}{n}\right)$ does indeed tend to 0 as $n \to \infty$. We'll start by playing the quantifier game to see why this should be true.

   i) The enemy picks any value of $\epsilon > 0$.

ii) You have to find an integer N such that $x_N, x_{N+1}, x_{N+2}, \ldots$ are all within ϵ of 0 (i.e. between $-\epsilon$ and ϵ).

If the enemy can win by a clever choice of ϵ, then it isn't true that x_n tends to 0 as $n \to \infty$. If you can always win, then it is true.

Enemy $\epsilon = 1$.

You $N = 2$. (1/2, 1/3, 1/4, ... are all within 1 of 0.)

Enemy $\epsilon = 1/2$.

You $N = 3$. (1/3, 1/4, 1/5, ... are all within 1/2 of 0.)

Enemy (in desperation) $\epsilon = 1/100000$.

You $N = 100001$. (1/100001, 1/100002, 1/100003, ... are all within 1/100000 of 0.)

In order to *prove* that x_n tends to 0 as $n \to \infty$, we need a *strategy* for dealing with any enemy choice of ϵ. The plays above suggest the strategy: we choose an integer N which is bigger than $1/\epsilon$, so that $1/N$, $1/(N+1)$, ... are all smaller than ϵ, and hence are within ϵ of 0.

Theorem 4 *The sequence* $\left(\frac{1}{n}\right)$ *tends to* 0 *as* $n \to \infty$.

Proof. Given any number $\epsilon > 0$, let $N \in \mathbb{N}$ be any integer with $N > 1/\epsilon$. Then $1/N < \epsilon$, and hence $0 < 1/n < \epsilon$ for all $n \geq N$. That is,

$$\forall n \geq N, \left|\frac{1}{n} - 0\right| < \epsilon$$

as required. ∎

b) In this (rather silly) example, we'll show that the sequence (x_n) with

$$x_n = \frac{n+1}{n}$$

doesn't tend to 0 as $n \to \infty$. Since the sequence is

$$2, \frac{3}{2}, \frac{4}{3}, \frac{5}{4}, \ldots$$

this is obvious from our intuitive idea of what it means to tend to a limit.

This time when we play the quantifier game the enemy can win:

Enemy $\epsilon = 2$.

You $N = 2$. ($\frac{3}{2}, \frac{4}{3}, \frac{5}{4}, \ldots$ are all within 2 of 0.)

Enemy $\epsilon = 1$.

You Surrender. (All the numbers x_n are bigger than 1, so no matter how far down we go we don't get within 1 of 0.)

To *prove* that x_n doesn't tend to 0 as $n \to \infty$, all we need is this single example of a winning enemy ϵ:

Theorem 5 *The sequence* $\left(\frac{n+1}{n}\right)$ *doesn't tend to* 0 *as* $n \to \infty$.

Proof. Let $\epsilon = 1 > 0$. Then for any integer $N \in \mathbb{N}$, $\frac{N+1}{N}$ is greater than 1, and hence

$$\left|\frac{N+1}{N} - 0\right| \geq \epsilon.$$

∎

Notice the connection with the *negation* of the definition of a sequence tending to a limit: *there exists* an $\epsilon > 0$ (namely $\epsilon = 1$) such that *for any* integer $N \in \mathbb{N}$, *there exists* $n \geq N$ (namely $n = N$) such that $|x_n - L| \geq \epsilon$.