MA102
Mathematical Proof and Analysis

and

MA103
Introduction to Abstract Mathematics

Autumn Term

Lecture Notes

These lecture notes were compiled by Peter Allen in 2024. However much of the content comes from Martin Anthony, Graham Brightwell, Michele Harvey, Jan van den Heuvel and Amol Sasane.

Contents

1 Introduction

This chapter is intended to tell you what 'abstract mathematics' and 'proof' mean, and why you should care about studying them.

1.1 'Thinking like a mathematician'

You probably know that Maths students (and other students who do a decent amount of maths, for example who do this course) typically go on to interesting and well paid jobs. However, you also know that a fair bit of the maths you have learned at school, and what you will go on to study here, is not likely to be practically useful in most jobs.

Employers, of course, are not stupid. They are not interested in hiring people who don't know how to do useful things. So why are mathematicians useful?

The answer is that at the end of your degree course—assuming you study well—you will no longer think the same way you do today. In fact, a lot of that change to your thinking will happen this year, in this course: though the more you practice, the better you will get at thinking like a mathematician. To a large extent, that's what your future boss wants.

Changing the way you think is not going to be an easy process; there will likely be some points in the course where it is painful. It may well be tempting to try to leave some parts of the course 'for later' and concentrate on your other courses. However, if you do this you will not be thinking like a mathematician when the exam comes, and you will likely fail it. This is especially true of the first three weeks of the course.

I should add that naturally there are other possibilities to develop a mathematical way of thinking: but probably the easiest route available is to take this course.

If you talk to a psychologist, they will tell you about all of the crazy things that the human brain does. Everyone grows up with a large collection of cognitive biases and short-cuts that 'usually work'. When we believe X is true, and we notice that if X is true then Y should happen, and we see Y actually does happen, then we think this is evidence for X. When we design something, we think about how it will work when expected events occur. In general, we do a lot of things which do not actually make any logical sense.

Mathematicians are definitely not immune to these biases. However, we can, when we are paying attention, think logically. What are all the other reasons for Y, and is one of those maybe a better explanation than X? Are there any weird events that might make our design go wrong, how likely are they, and what can we do about them? Of course, if I ask you these kinds of questions, you'll be able to answer them. The point is that to work effectively in the good jobs you would like to get, you need to be constantly thinking like this, automatically questioning whether reality really is as you thought, and whether there might be holes in your plan.

Another thing that most people do is give up too easily when faced with a difficult problem. If you read a question with a couple of technical words in that you don't know, the first thing that likely comes to mind as an answer is 'I don't know'. If you're asked to calculate something, and you don't know a method for it, you might well reply 'I can't'.

This is a perfectly reasonable reaction. Most of the time, there's something else you could be doing instead of trying to solve hard problems which will get you better rewards. If it's an A-level paper, in your limited time it probably was a better idea to do all the questions you did know how to do. However, it's the wrong reaction if you want to end up in a good job.

If you have experience with Maths Olympiad or STEP style questions, you probably feel you know how to deal with difficult problems. You certainly have some advantage over everyone else, but be cautious: the advantage is much less than you might think. These questions are still designed to be done quickly, they still expect you to use the 'right method', and the solution will generally be a fairly short and linear chain of ideas.

A mathematician's response to a question with unfamiliar words is to start working on understanding what the question is actually asking, then start trying things. If there happens to be a 'right method' that gets to a neat solution, we might find it eventually, but we are also prepared to deal with a more realistic problem which simply is not so neat: solve bits at a time, try to patch the bits together, find the holes that are still left and fix them. That might not be the 'textbook' solution—maybe there is no 'textbook' solution—but provided it is guaranteed to work, then it will be what the future job needs.

Again, it might not sound so hard to do that. But what do you do if you've tried for a couple of hours and you don't know if anything you have done will be useful? The answer, usually, is keep trying—or be very confident that you've really tried everything you know and ask your boss for help—but it's actually quite difficult to keep really trying things as opposed to just repeating things you already know don't work, and to keep looking for holes in the current solution, especially as hours turn into days and weeks.

We'll only begin developing your ability to do this kind of serious problem solving in this course. We'll get to the point where you (should) automatically start trying to understand what the problem is asking, rather than just giving up at the first unfamiliar word, and where you will be used to trying things for an hour or two before you get anywhere. We won't get to the point of days and weeks developing a complicated solution (though if you seriously attempt the starred exercises you'll get a lot further down this path). Still, the hardest bit is getting started; the rest is just practice and work.

One standard response to this is: why should I? I was quite comfortable with all the A-level methods, I just want to learn more of those, why are you not teaching me methods?

Well, this is not a methods course. Though, there *will* be some methods, at least methods to get started, and you will need to learn and use them. But more to the point, anything I can teach you to do without thinking too much, I can also program into a computer, and the computer is cheaper, faster, and more reliable. And by the time you graduate, ChatGPT 5.0 will be able to learn them for itself and apply them too, and it too will be cheaper than you, and faster, even if maybe *not* more reliable. There is not likely to be a job market for 'I know the words and I can do the methods, but I don't really understand so I can't do anything genuinely new'. LLMs can already do that reasonably well, and they will only get better. You should be aiming to be at the level where you can do things that 'AI' in three years cannot do, or at the least where you can understand what the output is supposed to do, so that you know when you've been given a good solution versus when it needs fixing.

A last point you should notice is that though in this course 'problems' will be mathematical, in your future 'problems' could be a lot broader: software engineering, public policy, consultancy, banking... the mathematical way of thinking will still help.

1.2 What is this course about?

There are two main concepts in this course, and they are the two main concepts you will learn, use, and re-use throughout your degree. After you have finished your degree, you might never again use some of the mathematics you learn: but the ways of thinking which you will be shown, will practice, and will steadily improve through your time here will stay with you. These ways of thinking are what in the end prepare you for your future career. These concepts are *abstraction* and *proof*.

You probably saw before at least some idea of what a mathematical proof is (but it is fine if you did not—we will cover it!), and you probably do not know what 'abstraction' should be (which is also fine). So I will begin by giving an example of abstraction which you met long ago. Choose a number, multiply it by itself, then add your chosen number four times, and finally add four. For example:

$$\begin{aligned}
&1\times 1+1+1+1+1+4=9 &&=3\times 3=(1+2)\times(1+2)\\
&2\times 2+2+2+2+2+4=16 &&=4\times 4=(2+2)\times(2+2)\\
&3\times 3+3+3+3+3+4=25 &&=5\times 5=(3+2)\times(3+2)\quad\text{and so on}\ldots
\end{aligned}$$

These are *concrete examples*. You probably see that there is a pattern to the answers we get. We can write it more generally:

$$x\times x+4\times x+4=(x+2)\times(x+2)\,.$$

This is a *mathematical statement*. It's something which is either true or false (depending on what x is). It means the same as the following English:

Choose a number, multiply it by itself, then add your chosen number four times, and finally add four. You will get the same answer as if you add two to your chosen number to get a new number, then multiply the new number by itself.

Writing x in an equation, rather than 'your chosen number' in an English phrase, is an example of a (simple) abstraction. Here the purpose is to simplify the presentation. There is no *need* to write equations with xs in them; you could do it all in words—and indeed long ago that is what people did. Of course, it's hard to get anything done like that. If you show the equation to a small child, it won't mean anything to them, while they can read and understand the sentence. But once you understand what the symbols in the equation mean, then it's much quicker and easier to read or write.

Now we come to proof. Is the statement above (however it's written) *true* for some other values of x than the three we checked by calculation? And if so, why? The purpose of a proof is *not* just to be certain that a statement is true. It also explains *why* a statement is true. As you probably know, the statement we wrote is true for all integers. Here is a proof.

Proof.

$$\begin{aligned}
&(x+2)\times(x+2) &&\\
=&(x+2)\times x+(x+2)\times 2 &&\text{(multiplication distributes over addition)}\\
=&x\times x+2\times x+(x+2)\times 2 &&\text{(multiplication distributes over addition)}\\
=&x\times x+2\times x+x\times 2+2\times 2 &&\text{(multiplication distributes over addition)}\\
=&x\times x+2\times x+x\times 2+4 &&(2\times 2=4)\\
=&x\times x+2\times x+2\times x+4 &&\text{(multiplication is commutative)}\\
=&x\times x+(2+2)\times x+4 &&\text{(multiplication distributes over addition)}\\
=&x\times x+4\times x+4 &&(2+2=4)
\end{aligned}$$

We can see that each line is equal to the previous one, for any integer x, because of the reason given on the right. Most of the reasons are *axioms*—statements which we are assuming to be true—and a couple are little calculations which you should check. So in particular the first and last lines are equal for any integer x, in other words the statement

$$(x+2)\times(x+2) = x\times x + 4\times x + 4$$

is true for any integer x. That's what we wanted to prove. □

Of course, you will never want to write down a proof in this kind of detail. You would much rather write at most a couple of lines of algebra expanding out the brackets, just as you would have done in school, or simply write 'it is obvious that $(x+2)\times(x+2) = x\times x+4\times x+4$'. This is fine (unless a question explicitly asks you to prove something from axioms). You just need to be aware that when you write 'it is obvious...' that you are promising that if someone really wants to see the details, you would be able to write out the details as above.

Let's go back to *abstraction*. These *axioms* we wrote down above (multiplication distributes over addition, multiplication is commutative) are statements which you presumably agree are true for the integers. Of course, they are also true for other numbers—they are true for real numbers, or complex numbers. That means that the proof we wrote down works equally well for real numbers, or complex numbers. So you know, for instance, that

$$(4.5+6i+2)\times(4.5+6i+2) = (4.5+6i)\times(4.5+6i)+4\times(4.5+6i)+4$$

is a true statement. This is a second reason abstraction is important: it is a time- and memory-saving device. You can prove something once—or remember one fact—in an abstract setting and use it in many different concrete examples.

Later on, you will see examples of mathematical structures which *are not* just numbers. For some of these structures, the two axioms we mentioned above will be true, and (if you can find a reasonable way of saying what '2' and '4' are!) the above proof still works. For other structures, one or both of these axioms might not be true, so the proof will not work. That *doesn't* mean the statement is automatically false, but at least you should be suspicious.

Actually, you probably already know an example (or, at least, by the time you come to revision you will know it). We can look at 2-by-2 matrices. Here, it's reasonable to say that '2' should mean the matrix $\begin{pmatrix}2&0\\0&2\end{pmatrix}$, and '4' should be $\begin{pmatrix}4&0\\0&4\end{pmatrix}$. Assuming you know how to add and multiply 2-by-2 matrices, you can make sense of the statement '$(x+2)\times(x+2) = x\times x+4\times x+4$' now when x is a 2-by-2 matrix. Does the proof we gave still work, and is the statement true?

Well, multiplication of matrices does still distribute over addition, and the two small calculations do still work. But matrix multiplication is *not* commutative; you can find pairs of matrices where the order you multiply them makes a difference to the answer. So the proof does not work.

But it happens (luckily!) to be the case that multiplication of any 2-by-2 matrix by $\begin{pmatrix}2&0\\0&2\end{pmatrix}$ *does* commute (think about why!) and since the only place we used commutativity of multiplication in our proof above was to say $2\times x = x\times 2$, we can make our proof work by changing the reason 'multiplication is commutative' to 'multiplication by $\begin{pmatrix}2&0\\0&2\end{pmatrix}$ is commutative'. Phew! The statement is still true for 2-by-2 matrices, and we can prove it.

However, you should be a bit careful with matrices. Is it true that

$$\left(\begin{pmatrix}0&1\\0&0\end{pmatrix}+\begin{pmatrix}0&0\\1&0\end{pmatrix}\right)^2 = \begin{pmatrix}0&1\\0&0\end{pmatrix}^2 + 2\cdot\begin{pmatrix}0&1\\0&0\end{pmatrix}\cdot\begin{pmatrix}0&0\\1&0\end{pmatrix}+\begin{pmatrix}0&0\\1&0\end{pmatrix}^2 ?$$

This looks like the same 'expanding out the brackets' that we just did, but (if you try to mimic the proof above) you'll see that there is a step where you would like to say that $\begin{pmatrix}0&1\\0&0\end{pmatrix}\cdot\begin{pmatrix}0&0\\1&0\end{pmatrix}=\begin{pmatrix}0&0\\1&0\end{pmatrix}\cdot\begin{pmatrix}0&1\\0&0\end{pmatrix}$, i.e. that *these* two matrices commute. They don't, and this is where the calculation goes wrong.

Next term, we'll give axiomatic definitions of a *group* and a *vector space*, and start proving theorems about abstract groups (and vector spaces). Here 'abstract' means we don't assume anything about the group except the axioms. This will seem painful and useless at first: you'll (by then) know a few concrete examples of groups and of vector spaces. It will usually be easier to see how to prove the theorems for the concrete examples. Usually you will have some idea already why the theorems should be true in the examples, while you won't have much intuition for how abstract groups behave. The natural response will be that you don't want to study abstract groups, you want to work with the concrete examples you know. But this is the **wrong reaction**. The reason is that you will then *only* learn about the concrete examples you already know, and you will suffer as soon as in future courses you see new examples of groups and are expected to immediately know a bunch of facts about them (and also in the exam, where we will likely test your ability to work with a new example of an abstract structure).

Finally, let's return to *proof*. Why should you care that you can mathematically prove a statement, when it's obviously true (like the one above) or when you can check lots of cases and become convinced?

First, we will not generally be interested in proving obvious statements, we will rather be trying to prove statements which aren't obvious. We will discuss later what exactly that word 'obvious' means, and we will see lots of examples of statements where you don't immediately see whether it is true or false, or how to decide which.

Second, what do you learn from checking cases? If you are trying to find out whether a claim is true or false, it's a good idea to start checking cases. That might give you an idea why the claim is true, or find out if it is complete nonsense. But what if the statement is true for most cases, but there are some special cases where it goes wrong? You most likely won't find them. Similarly, if you're writing a computer program (a likely part of your future career!) and your program works most of the time, but you don't consider some special cases ('edge cases' is the jargon), you might end up writing a program which causes a disaster—not at the level of say crashing a plane, because such programs are checked in detail, but you could easily find your automated trading program has lost your bank a lot of money and you your job. To avoid that, you need to learn how to keep an overview of a complicated problem: which parts have I checked, and what is still left that could go wrong? Learning to write formal proofs is a good way to train.

In this course, we need to work with *precise definitions* and *statements*, and you will need to know these. Not only will you need to know these, but you will have to understand them, and be able (through the use of them) to demonstrate that you understand them. Simply learning the definitions without understanding what they mean is not going to be adequate. I hope that these words of warning don't discourage you, but I think it's important to make it clear that this is a subject at a higher conceptual level than most of the mathematics you are likely to have studied before. This does not mean it is incredibly hard and you will struggle. It is not incredibly hard, and you are quite capable of doing well in this course (or you would not be here). It does mean, though, that if you are used to getting through school courses by memorising material without understanding it, then now is the time to change that (and, by the way, no-one will hire you for your memorisation ability—a computer does that better!).

One of the standard problems students have in this course is around what it means to 'know precise definitions'. We will be using English language—not, for the most part, logical symbols—to define various concepts. If you know the string of words as it appears here by heart, then, yes, you know the precise definition. But most likely I will not be completely consistent, and certainly your textbooks and other courses will use slightly different strings of words for the same concept. What will be changed will turn out to be things that do not alter the meaning of the concept—you're completely used to the idea that there are words one can change without changing the intent of a sentence in English. Mathematical English is, however, a bit more picky than the usual spoken English; there are some words which you cannot change, and in particular the order of words is often important. I'll highlight this when it gets relevant in the course. For now, if you're not sure whether two sentences mean the same thing, that tells you you don't understand either of them and you need to think a bit more and look at the examples.

1.2.1 How to get the most out of this course (and all the other maths courses)

There are two theories about mathematical ability (and intelligence in general). One theory says that you have what you are born with. The other says that (just like strength or stamina) it's something you develop by practice. Various studies have shown that broadly similar number of students believe each theory, but the ones who believe ability is something you develop are consistently the ones who do better—and almost all academic mathematicians believe ability is something you learn and train.

Some people are faster than others, but speed is in the end not all that useful: no matter how fast you are, if you switch off and coast for a while, you will have trouble catching up with people who pay attention and work on understanding their courses. In particular—and this is different to school maths—we will always assume you understood the previous lectures and courses, and we will use things from those previous lectures and courses all the time. If you do understand the previous material—even if you are not so fast—you'll understand a good deal of the current lecture (maybe all of it, maybe not quite) in real time, and you won't need to spend much time after the lecture going over the material. If you don't really understand the previous material, you won't have a chance to understand large parts of the lecture and you'll have to do even more work afterwards to catch up.

In this course, all the theory will be introduced in the lectures, together with some examples. There will be extra examples sessions (which don't exist in most courses—don't expect them!), which you do not have to attend but which may well be useful.

In the lectures and examples sessions, you should be trying to understand what is going on. Don't waste time copying things down which will appear on Moodle (which is essentially everything). Certainly don't waste time with a newspaper or games on your phone, which annoys me and distracts your classmates. No-one is taking attendance in the lectures; if you're not going to pay attention, go to a café instead. If you do not understand something I said or wrote, then probably either I didn't explain it properly or I made a mistake, so you should **ask questions** (louder, or put your hand up, if I don't hear). When I ask a question, **I really want an answer**. Probably you need to think about the question to answer it, so I will wait until someone does answer.

For many of you there will be some point in the lectures where you do not immediately understand what I say, and when you ask a question the answer is still not very useful. You should keep asking me to explain better in such a situation. It is possible that I will eventually say that I want to move on and you should think about it after the lecture. That doesn't mean I think you are stupid, it generally means I am failing to understand what exactly you don't understand, or maybe I do understand but cannot think of a good way to explain it on the spot. In either case, if you try to formulate clearly exactly what it is that you do not like (which will take time, which is why you should do it after the lecture), you will probably find that doing so also helps you figure out what is going on; once you understand something deeply in this way you will not forget it. But it would still be useful to tell me about it after the lecture, so that I can improve the lectures for next year (and if possible give some more explanation on Moodle directly).

There will also be problems set every week, some online (for which you'll see results immediately) and some which you will solve and hand in to your class teacher, who will mark them and discuss in the next class. *The class work will be marked, and in addition it will contribute 10% to your eventual course grade.*

The purpose of the problems is for you to practice and check you really know what is going on. If you get stuck, hand in half a solution with 'I don't know what to do next' and your class teacher will tell you (either written on the work, or maybe many people were stuck in the same place and the class teacher will go over it in class; usually then there will be a short comment like 'Will discuss in class'). Then you learn something. If you don't hand anything in, or you only hand in the problems you could solve, you don't learn anything. The written comments on your work, and the explanations in class, are the most important piece of feedback you get—but you only get it if you show us something on which we can give feedback. On that note—please do not copy work from someone else (or from last year's solutions). Doing this is a waste of your time and ours, and it is plagiarism which can potentially land you in serious trouble. Your mark for each week will reflect how well your class teacher feels you did on the exercises.

The contribution to the course grade is different. Each week, your work will be either judged as acceptable or not—this is a binary system, you don't get extra points for amazing work—and to get all of the 10% course grade, you need sufficiently many acceptable pieces of work, handed in on time, over the term.

There are two ways in which a piece of work can be judged acceptable. One is if you have a 50% or better grade. The other is if you do not have such a grade, *but* you have made a serious attempt at all the questions. This is defined to mean: you have written down all the definitions (often there will be only one, but there can be more than one) that you need in order to understand the question.

The intention of this contribution to the course grade is to reward students who keep up with the course and make some effort to learn actively. If you know how to do most exercises, you're guaranteed to get the 'acceptable'. If you don't, then the first thing you should do is to write down the definitions, not just because this will guarantee you your 'acceptable', but also (and mainly) because the most common reason why students cannot do exercises is that they do not know what the exercise is actually asking—writing down the definitions will often give you an idea of how to get on with the solution.

The only way to fail to get the 10% for coursework is for you to decide that it is not worth your time to make any serious attempt at the classwork. In recent years we noticed students increasingly doing this, usually then telling us that they are 'a bit behind and need to catch up', or that they will 'do all the questions in revision'. Usually, these students failed their exams; we hope that if you are thinking of studying 'school style', even if you believe that you personally will be able to make it work, you will at least recognise that throwing away 10%—an entire class grade—is a bad move.

Finally, there are office hours and the Maths Support Centre. If you don't understand something, you should first try to figure it out for yourself—if you manage, then you won't forget it (and you should be happy with yourself). But if you get stuck, then you should not wait and hope that it magically gets clear. It probably will not, and you will suffer because you don't understand something I am assuming you do understand in my lectures. So go to office hours or the Support Centre and ask questions. You have already paid for those office hours; use them. You can also try talking with your friends on the course and seeing if you can figure out what's going on—group work can be fun and productive.

Finally finally, some weeks I will set a 'starred question' on the exercise sheet. You will usually be given 2 weeks for these questions instead of 1, and there will be a separate hand-in box on Moodle. I'll mark these pieces of work, not your class teacher. I will try to do this in reasonable time, but sometimes it'll take a while. When I mark, I'll usually just give all the work 1 point (because Gradescope needs to see a point given) but I will try to write helpful comments—so look at the comments not the mark.

These starred questions are *not* compulsory, and in fact if you are finding the course difficult and struggling to do the weekly work, *please don't do them*, rather put your energy into understanding the course. They are there for those who are enjoying the course and doing well, who would like to know more, try out new things, and see what mathematics research might be like. In particular, if you're thinking that the distant future might hold going on to a PhD in a quantitative discipline—whether Maths, Stats, Economics or something else—then the starred questions are your first taste of what that might be like.

1.2.2 Topics covered (MA102, first half of MA103)

Descriptions of topics to be covered appear in the relevant chapters. However, it is useful to give a brief overview at this stage. These notes are for the ten weeks of MA102, which is the first half of MA103.

We are concerned primarily with proof and logic. We will first investigate how precise mathematical statements can be formulated, and here we will use the language and symbols of mathematical logic. We will then study how one can prove or disprove mathematical statements, and introduce some important basic structures and concepts. This will occupy the first (roughly) five weeks, at something like one week per topic. In each new topic, we will begin from scratch, and the way you need to think about each topic will be different.

After this, we will spend the next five weeks concentrating on *Analysis*. This is one of the major branches of abstract mathematics. While these five weeks are split into three topics, the way you need to think about all three is very much the same.

Most of the material in these notes is intended to help you prepare for the rest of this course; all of it is intended to prepare you for the second-year and later mathematics courses. All of it is examinable, with the exception of sections which are clearly marked 'non-examinable'. Just to be clear—some of the non-examinable material will be useful for understanding the course (and I'll probably talk about it in lectures), some is background which you will not need to understand the course (but which you might find interesting, and which I will probably not talk about in lectures). The way I choose what material is examinable and what is not, is I try to come up with a good exam question; if I can't, then I'll mark it as non-examinable. That means, anything in the course marked as examinable is material which I know how to test in an exam.

1.3 Moodle

All information and materials for this course are on Moodle:

`http://moodle.lse.ac.uk/course/view.php?id=1989`

On the course Moodle page, you will find assignments, solutions, lecture notes, and so on.

1.4 Reading

These notes are intended to be a comprehensive treatment. That means, I think you should not need to buy or borrow any textbooks for this course.

However, you might disagree. If you don't like my writing style, or you want to understand a particular topic better, try looking at a textbook. If you want more exercises, and you are actually going to do the exercises, look at a textbook. If you want more exercises in order to read the solutions, you're wasting your time!

There are many books that would be useful for this subject, since abstract mathematics is a component of all university-level mathematics degree programmes I know of. That said, some options which are definitely suitable are to be found on the course Moodle page, under 'Study Material — Autumn Term', where you found these notes.

1.5 Activities and sample exercises

Throughout the chapters of these notes, you'll find 'activities'. These are things for you to do or think about as you read, just to reaffirm that you've understood the material.

At the end of each chapter of these notes you will find some sample exercises together with solutions. These are not the exercises that will be assigned for classes, but are *additional* to those. They are a very useful resource. You should try them once you think you have mastered a particular chapter. Really try them: don't just simply read the solutions provided. Make a serious attempt before consulting the solutions. Note that the solutions are often just sketch solutions, to indicate to you how to answer the questions.

2 Mathematical statements, proof, and logic

In this chapter we go over the basics which one needs in order to start doing abstract mathematics and proof, namely statements and logic. This will go by fairly quickly—there is nothing hard here.

However, this chapter and the next are also the most important in the course. You need to be completely on top of the material here—especially basic logic and quantification—otherwise the rest of the course will not make much sense and you will fail the exam.

The material in this chapter is also covered in:

- Biggs, N.L. *Discrete Mathematics.* Chapters 1–3.
- Eccles, P.J. *An Introduction to Mathematical Reasoning.* Chapters 1–4 and 6.

2.1 Introduction

In this course, we want to make precise mathematical statements and establish whether they are true or not—we want to *prove* things. But for that, we have to first understand what a proof is. We will look at fairly simple types of mathematical statement, in order to emphasise techniques of proof. Some of these statements are going to be interesting, others are not so interesting—bear in mind that what you are doing in this part of the course is learning the rules of the game: the play (and more of the fun) comes later.

In later chapters (such as those on numbers, analysis and algebra) we will use these proof techniques extensively. You might think that some of the things we prove in this chapter are very obvious and hardly merit proving, but proving even ‘obvious’ statements can be quite tricky sometimes, and it is good preparation for proving more complicated things later.

As I’ve said, this is not a methods course. However, we will begin to see some *standard strategies* as term goes on: things that you can try, that will help you understand a problem, or get started, or move you along when you get stuck. Occasionally (for example, on some exam questions) they will turn out to be all you need to solve a problem, more often they will just be options you can try. If at the end of the course you can use all these strategies reliably and you understand what they are doing, then you will get at least a 2:1 in the exam and you will be well prepared for future courses. Now, all of these standard strategies require that you understand basic logic as in this chapter: if you can’t reliably write down for example the contrapositive of an implication, or negate a statement, then you will not be able to use them. So: ideally you should learn and understand all the basic logic in this chapter. If you don’t feel you really understand, at least learn and practice it: with enough practice the understanding will come.

2.2 Mathematical statements and proof

To introduce the topics of mathematical statement and proof, we start by giving some explicit examples. Later in the chapter we give some general theory and principles. Our discussion of the general theory is limited because this is not a course in logic. We need enough logic to understand what mathematical statements mean and how we might prove or disprove them. We don't need to start talking about things like which statements are provable and which statements are true (and whether those are the same or not). There are interesting mathematical things to say there (and interesting philosophical things), but you don't need to know them in order to do mathematics. The things you must know (in this chapter and in future) will be highlighted as critical. As promised, there will be quite a lot in this chapter and the next, but only a few after that.

2.2.1 Examples of Mathematical Statements

Consider the following statements (in which you should recall that the natural numbers are the positive integers):

(a) 20 is divisible by 4.

(b) 21 is not divisible by 7.

(c) 21 is divisible by 4.

(d) 21 is divisible by 3 or 5.

(e) 50 is divisible by 2 and 5.

(f) n^2 is even.

(g) For every natural number n, the number $n^2 + n$ is even.

(h) There is a natural number n such that $2n = 2^n$.

(i) If n is even, then n^2 is even.

(j) For all odd numbers n, the number n^2 is odd.

(k) For natural numbers n, the number n^2 is even if and only if n is even.

(l) There are no natural numbers m and n such that $\sqrt{2} = m/n$.

These are all mathematical statements, of different sorts (all of which will be discussed in more detail in the remainder of this chapter).

Statements (a) to (e) are straightforward *propositions* about certain numbers, and these are either true or false. Statements (d) and (e) are examples of *compound statements.* Statement (d) is true precisely when *either one (or both)* of the statements '21 is divisible by 3' and '21 is divisible by 5' is true. Statement (e) is true precisely when *both* of the statements '50 is divisible by 2' and '50 is divisible by 5' are true.

Statement (f) is different, because the number n is not specified and whether the statement is true or false will depend on the value of the so-called *free variable n.* Such a statement is known as a *predicate.*

Statement (g) makes an assertion about *all* natural numbers and is an example of a *universal statement.*

Statement (h) asserts the existence of a particular number and is an example of an *existential* statement.

Statement (i) can be considered as an assertion about all even numbers, and so it is a universal statement, where the 'universe' is all even numbers. But it can also be considered as an *implication*, asserting that *if* n happens to be even, *then* n^2 is even.

Statement (j) is a universal statement about all odd numbers. It can also be thought of (or rephrased) as an implication, for it says precisely the same as 'if n is odd, then n^2 is odd'.

Statement (k) is an 'if and only if' statement: what it says is that n^2 is even, for a natural number n, *precisely when* n is even. But this means two things: namely that n^2 is even if n is even, and n is even if n^2 is even. Equivalently, it means that n^2 is even if n is even and that n^2 is odd if n is odd. So statement (k) will be true precisely if (i) is true for all natural numbers, and (j) is true.

Statement (l) asserts the non-existence of a certain pair of numbers (m, n). Another way of thinking about this statement is that it says that for all choices of (m, n), it is *not* the case that $m/n = \sqrt{2}$. (This is an example of the general rule that a non-existence statement can be thought of as a universal statement, something to be discussed later in more detail.)

It's probably worth giving some examples of things that are *not* proper mathematical statements.

'6 is a nice number' is not a mathematical statement. This is because 'nice number' has no mathematical meaning. However, if, beforehand, we had *defined* 'nice number' in some way, then this would not be a problem. For example, suppose we said:

> Let us say that a number is *nice* if it is the sum of all the positive numbers that divide it and are less than it.

Then '6 is a nice number' would be a proper mathematical statement, and it would be true, because 6 has positive divisors $1, 2, 3, 6$ and $6 = 1 + 2 + 3$. But without defining what 'nice' means, it's not a mathematical statement. Definitions are important[1].

'$n^2 + n$' is not a mathematical statement, because it does not say anything about $n^2 + n$. It is not a mathematical statement in the same way that 'Liz Truss' is not a sentence: it makes no assertion about what Liz Truss did or did not do to get thrown out. However, '$n^2 + n > 0$' is an example of a *predicate* with free variable n and, for a particular value of n, this is a mathematical statement. Likewise, 'for all natural numbers n, $n^2 + n > 0$' is a mathematical statement.

Finally, anything which does not make sense as an English sentence is not a mathematical statement. We will use lots of symbols—some you know, like =, some you don't yet, like ∀—which all mean some English word or words. It's easy to write something with symbols that, when you read it out, doesn't make sense. If when you read your work out, you are saying something like 'five is true' or 'for every integer n we have $n = 2$', something is wrong. Figure out what you meant to write, then write that.

[1] Usually we say that a natural number which is equal to the sum of all smaller positive numbers which divide it is *perfect*. The reason for using 'nice' in the text is because that term is not commonly defined!

2.2.2 Introduction to proving statements

We've seen, above, various types of mathematical statement, and such statements are either true or false. But how would we establish the truth or falsity of these?

We can, even at this early stage, prove (by which we mean establish the truth of) or disprove (by which we mean establish the falsity of) most of the statements given above. Before we do this, we need to be sure that we really know precisely what all the statements mean. We already said what we mean by the 'natural numbers', and I assume you know what the algebra means (i.e. that n^2 means n multiplied by n, and so on). We haven't formally defined 'divisible', though, and you might not have seen this in school. So we need to do that:

Let us say that a natural number n is *divisible* by a natural number d if we can write $n = d \cdot k$ for some natural number k. We say that a natural number is *even* if it is divisible by 2, and *odd* if it is not.

Note that saying n is divisible by d is the same thing as saying that if we try to divide n by d we get no remainder. This definition is probably what you thought 'divisible' meant when you read the statements in the previous section—now you know you were right, and you know everyone else will (by definition!) agree with you. For the rest of your degree, we'll assume you know what 'divisible' means, and the meaning will not be changed. We might say 'divisible means when we try to divide we get no remainder', or some other phrase which has the same mathematical meaning: the precise words aren't important. What is important is that the mathematical meaning is now fixed.

Now that we're all clear on exactly what the statements mean, let's see which ones are true and prove them.

(a) 20 is divisible by 4.

This statement is true. Since $20 = 5 \times 4$, we see that (by the definition) 20 is divisible by 4. And that's a proof! It's utterly convincing, watertight, and not open to debate. Nobody can argue with it, not even a sociologist! Isn't this fun? Well, maybe it's not that impressive in such a simple situation, but we will certainly prove more impressive results later.

(b) 21 is not divisible by 7.

This is false. It's false because 21 *is* divisible by 7, because $21 = 3 \times 7$.

(c) 21 is divisible by 4.

This is false, as can be established in a number of ways. First, we note that if the natural number m satisfies $m \leq 5$, then $m \times 4$ will be no more than 20. And if $m \geq 6$ then $m \times 4$ will be at least 24. Well, any natural number m is either at most 5 or at least 6 so, for all possible m, we do not have $m \times 4 = 21$ and hence there is no natural number m for which $m \times 4 = 21$. In other words, 21 is not divisible by 4. Another argument (which is perhaps more straightforward, but which relies on properties of rational numbers rather than just simple properties of natural numbers) is to note that $21/4 = 5.25$, and this is not a natural number, so 21 is not divisible by 4. (This second approach is the same as showing that 21 has remainder 1, not 0, when we divide by 4.)

Most of you are probably completely happy with these proofs. Maybe one or two of you would like to know things like: why is there no natural number between 5 and 6? Do we need to prove it? We won't get into fundamentals to that extent: it takes too long to get anywhere and you do not gain much. If you are interested, if is called Foundations of Mathematics.

(d) 21 is divisible by 3 or 5.

As we noted above, this is a compound statement. It is true precisely if one (or both) of the following statements is true:

(i) 21 is divisible by 3

(ii) 21 is divisible by 5.

Statement (i) is true, because $21 = 7 \times 3$. Statement (ii) is false. Because at least one of these two statements is true, statement (d) is true.

(e) 50 is divisible by 2 and 5.

This is true. Again, this is a compound statement and it is true precisely if *both* of the following statements are true:

(i) 50 is divisible by 2

(ii) 50 is divisible by 5.

Statements (i) and (ii) are indeed true because $50 = 25 \times 2$ and $50 = 10 \times 5$. So statement (e) is true.

(f) n^2 is even

As mentioned above, whether this is true or false depends on the value of n. For example, if $n = 2$ then $n^2 = 4$ is even, but if $n = 3$ then $n^2 = 9$ is odd. So, unlike the other statements (which are *propositions*), this is a *predicate* $P(n)$. The predicate will become a proposition when we assign a particular value to n to it, and the truth or falsity of the proposition can then be established. You probably implicitly assume that n has to be a natural number, but there isn't actually anything in the statement to tell you that—maybe n is a matrix, in which case it's not even clear what 'even' should mean for a matrix (we only defined 'even' for natural numbers). If we assume n is a natural number, then (i) and (j) cover all the possibilities.

(g) For every natural number n, the number $n^2 + n$ is even.

Here's our first non-immediate, non-trivial, proof. How on earth can we prove this, if it is true, or disprove it, if it is false? Suppose it was false. How would you convince someone of that? Well, the statement says that *for every* natural number n, $n^2 + n$ is even. So if you managed (somehow!) to find a particular N for which $N^2 + N$ happened to be odd, you could prove the statement false by simply observing that 'When $n = N$, it is *not* the case that $n^2 + n$ is even.' And that would be the end of it. So, in other words, if a universal statement about natural numbers is false, you can prove it is false by showing that its conclusion is false for *some particular* value of n. But suppose the statement is true. How could you prove it. Well, you could prove it for $n = 1$, then $n = 2$, then $n = 3$, and so on, but at some point you would expire and there would still be numbers n that you hadn't yet proved it for. And that simply wouldn't do, because if you proved it true for the first 9999 numbers, it might be false when $n = 10000$. So what you need is a more sophisticated, *general* argument that shows the statement is true for any *arbitrary* n.

Now, it turns out that this statement is true. So we need a nice general argument to establish this. Well, here's one approach. We can note that $n^2 + n = n(n + 1)$. The numbers n and $n + 1$ are consecutive natural numbers. So one of them is odd and one of them is even. When you multiply any odd number and any even number together, you get an even number, so $n^2 + n$

is even. Are you convinced? Maybe not? We really should be more explicit. Suppose n is even. What that means is that, for some integer k, $n = 2k$. Then $n + 1 = 2k + 1$ and hence

$$n(n + 1) = 2k(2k + 1) = 2 (k(2k + 1)) .$$

Because $k(2k + 1)$ is an integer, this shows that $n^2 + n = n(n + 1)$ is divisible by 2; that is, it is even. We supposed here that n was even. But it might be odd, in which case we would have $n = 2k + 1$ for some integer k. Then

$$n(n + 1) = (2k + 1)(2k + 2) = 2 ((2k + 1)(k + 1)) ,$$

which is, again, even, because $(2k + 1)(k + 1)$ is an integer.

Right, we're really proving things now. This is a very general statement, asserting something about *all* natural numbers, and we have managed to prove it. I find that quite satisfying, don't you?

(h) There is a natural number n such that $2n = 2^n$.

This is an *existential statement*, asserting that *there exists* n with $2n = 2^n$. Before diving in, let's pause for a moment and think about how we might deal with such statements. If an existential statement like this is true we would need only to show that its conclusion (which in this case is $2n = 2^n$) holds for some particular n. That is, we need only find an n that works. If the statement is false, we have a lot more work to do in order to prove that it is false. For, to show that it is false, we would need to show that, for *no* value of n does the conclusion holds. Equivalently, for *every* n, the conclusion fails. So we'd need to prove a universal statement and, as we saw in the previous example, that would require us to come up with a suitably general argument.

In fact, this statement is true. This is because when $n = 1$ we have $2n = 2 = 2^1 = 2^n$; we're done.

We could also use $n = 2$ to prove this statement is true: we have $2n = 2 \cdot 2 = 4 = 2^2 = 2^n$. But to prove an existential statement to be true, it's enough to find one example; once we saw $n = 1$ is such an example, we don't need to care that $n = 2$ is also an example.

(i) If n is even, then n^2 is even

This is again a predicate, officially: it doesn't have a truth value until you say what n is. However, it's true for every integer n. The most straightforward way to prove this is to assume that n is some (that is, *any*) even number and then show that n^2 is even. So suppose n is even. Then $n = 2k$ for some integer k (by definition) and hence $n^2 = (2k)^2 = 4k^2$. This is even because it is $2(2k^2)$ and $2k^2$ is an integer.

(j) For all odd numbers n, n^2 is odd.

Just as with (i), this is a predicate but happens to be true for every integer n. The most straightforward way to prove this is to assume that n is *any* odd number and then show that n^2 is also odd. So suppose n is odd. Then $n = 2k + 1$ for some integer k and hence $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1$. To establish that this is odd, we need to show that it can be written in the form $2K + 1$ for some integer K. Well, $4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. This is indeed of the form $2K + 1$, where K is the integer $2k^2 + 2k$. Hence n^2 is odd.

Another way to prove this result is to prove that if n^2 is even then n must be even. We won't do that right now, because to do it properly requires a result we meet later concerning the factorisation of numbers into prime numbers. But think about the strategy for a moment. Suppose we were able to prove the following statement, which we'll call Q:

Q: for all integers n, *if* n^2 is even *then* n is even.

Why would that establish what we want (namely that for all integers n, if n is odd then n^2 is odd)? Well, one way is to observe that Q is what's called the *contrapositive* of statement (j) that we're trying to prove, and the contrapositive is *logically equivalent* to the initial statement. (This is a bit of formal logic, and we will discuss this more later). But there's another way of thinking about it, which is perhaps easier to understand at this stage. Suppose we have proved statement Q and suppose that n is odd. Then it must be the case that n^2 is odd. For, if n^2 was not odd, it would be even and then Q would tell us that this means n is even. But we have assumed n is odd. It cannot be both even and odd, so we have reached a contradiction. By assuming that the opposite conclusion holds (n^2 even) we have shown that something impossible happens. This type of argument is known as a *proof by contradiction* and it is often very powerful. We will see more about this later.

(k) For all natural numbers n, the number n^2 is even if and only if n is even.

This is true. What we have shown in proving (i) and (j) is that if n is even then n^2 is even, and if n is odd then n^2 is odd. The first, (statement (i)) establishes that *if* n is even, then n^2 is even. The second of these (statement (j)) establishes that n^2 is even *only if* n is even. This is because it shows that n^2 is odd if n is odd, from which it follows that if n^2 is even, n must not have been odd, and therefore must have been even. 'If and only if' statements if this type are very important. As we see here, the proof of such statements breaks down into the proof of two 'If-then' statements.

(l) There are no natural numbers m and n such that $\sqrt{2} = m/n$.

This is, in fact, true, though we defer the proof for now, until we know more about factorisation of numbers into prime numbers. We merely comment that the easiest way to prove the statement is to use a proof by contradiction.

These examples hopefully demonstrate that there are a wide range of statements and proof techniques, and in the rest of this chapter we will explore these further.

Right now, one thing I hope comes out very clearly from these examples is that to prove a mathematical statement, you need to know precisely what it means. Well, that sounds obvious, but you can see how detailed we had to be about the meanings (that is, the *definitions*) of the terms 'divisible', 'even' and 'odd'.

Something you can also notice is that we like to come up with special names to distinguish things even when it's 'unnecessary'. For example, we talked about 'propositions' and 'predicates' as being different types of statement; why bother with these two funny words? Right now, this no doubt feels like me inventing more words that you have to learn for no good reason. Nevertheless, I'm going to tell you that you must know these words, and also the difference between 'free variable' and 'bound variable'.

Critical

A *variable* just means a letter that we're using as a placeholder for something else—usually a number, but it could be any mathematical object.

When we have a logical statement with some variables inside it, these variables can be *free* or *bound*. The letter n in (f) is free. The same letter in (g) is bound. The difference is: a free variable is defined *outside* the statement; you can change it and it might change the truth value. A bound variable is defined *inside* the statement, often with 'for all' or 'there exists'; it doesn't make sense to 'change it'.

A *predicate* is a logical statement with at least one free variable. We normally give it a name like $Q(r,t)$ to indicate that the free variables are r and t.

A *proposition* has no free variables: it can have bound variables, as in (g).

You should usually be able to see instantly whether a variable is free or bound. If I ask you 'Is n^2 is even?' then you will stare at me and wonder why I am asking something so ridiculous. Of course you can't answer it, because you don't know what n I have in my head. And if I ask you 'Is p^2 even?' then I'm asking you a different question, for which you need to know some different variable p. This n is (and so is p) a free variable.

If on the other hand you can answer the question without needing to wonder what variable I have in my head—like if I ask 'Is it that for all natural numbers n the quantity $n^2 + n$ is even?'—and you can change the letter without it altering the question ('Is it that for all natural numbers r the quantity $r^2 + r$ is even?') then the variable is bound. Furthermore, it doesn't make sense to say 'For $r = 7$ for all natural numbers r the quantity $r^2 + r$ is even', so it doesn't make sense to talk about the proposition 'Is it that for all natural numbers r the quantity $r^2 + r$ is even?' for some specified r. You can say 'For $r = 7$ the quantity $r^2 + r$ is even', but this is a different statement we're working with (the predicate 'the quantity $r^2 + r$ is even').

I don't really care as such that you know these names. However, I care a lot that you do not get confused, and I've seen far too many students get confused here. For the next couple of chapters, we will only be doing fairly simple pieces of logic. You will be able to remember the details of everything that is going on even if you get sloppy with writing things down, and it will be tempting to do so, just as it's tempting to ignore a language's grammar when you only know a few words and your sentences are very short. However, after that we will start doing more complicated things. If you don't understand the mathematical grammar, you will not understand my lectures and no-one will understand your work. You will not be able to remember all the details, and because you're writing them down sloppily, you will end up confusing yourself. At this point, all you'll learn from the rest of the course is a few buzzwords. The same goes for the rest of the 'mathematical grammar' we'll see in this and the next chapter.

The kind of error that students make when they don't understand the differences here is to write something like 'f is continuous for $\varepsilon = 1$'. You don't need to know what the word 'continuous' means just yet: the point is that this is rather like writing '4 is even for $k = 17$'. f is either continuous or it isn't, it's a proposition and there is nothing more to it (even though ε does show up as a bound variable inside the definition as written in these notes). Similarly, 4 is either even or it isn't, what the value of some letter k might be has nothing to do with it (even though the letter k does appear in the definition up above in the notes).

You can believe that someone who writes a statement like '4 is even for $k = 17$' most likely doesn't understand what 'even' means, because they seem to think that $k = 17$ is important; they will likely go on to do some kind of calculation with k that they think is important but doesn't really mean anything. This is because you know what the word 'even' means. But you can catch this kind of mistake also for words like 'continuous' whose meaning you don't know (yet): the definition of 'even' has k as a bound variable inside it, so you can't use it outside, if you do something is wrong. Similarly, continuous has ε as a bound variable in the definition, so you can't use it outside and the statement must be nonsense. Any time something is wrong and you suspect you've written nonsense, first try to find what went wrong, but if you can't ask me or a class teacher for help.

2.3 Some basic logic

Mathematical statements can be true or false. Let's denote 'true' by T and 'false' by F. Given a statement, or a number of statements, it is possible to form other statements. This was indicated in some of the examples above (such as the compound statements). A technique known as the use of 'truth tables' enables us to define 'logical operations' on statements, and to determine when such statements are true. This is all a bit vague, so let's get down to some concrete examples.

2.3.1 Negation

The simplest way to take a statement and form another statement is to *negate* the statement. The *negation* of a statement P is the statement $\neg P$ (sometimes just denoted 'not P'), which is defined to be true exactly when P is false. This can be described in the very simple truth table, Table 2.1:

P	$\neg P$
T	F
F	T

Table 2.1: The truth table for 'negation' or 'not'

What does the table signify? Quite simply, it tells us that if P is true then $\neg P$ is false and if P is false then $\neg P$ is true.

Example 2.1. If P is '20 is divisible by 3' then $\neg P$ is '20 is not divisible by 3'. Here, P is false and $\neg P$ is true.

It has, I hope, been indicated in the examples earlier in this chapter, that to disprove a universal statement about natural numbers amounts to proving an existential statement. That is, if we want to disprove a statement of the form 'for all natural numbers n, property $p(n)$ holds' (where $p(n)$ is some predicate, such as 'n^2 is even') we need only produce some N for which $p(N)$ fails. Such an N is called a *counterexample*. Equally, to disprove an existential statement of the form 'there is some n such that property $p(n)$ holds', one would have to show that for *every* n, $p(n)$ fails. That is, to disprove an existential statement amounts to proving a universal one. But, now that we have the notion of the negation of a statement we can phrase this a little more formally. Proving that a statement P is false is equivalent to proving that the negation $\neg P$ is true. In the language of logic, therefore, we have the following:

Critical

- The negation of a universal statement is an existential statement.
- The negation of an existential statement is a universal statement.

More precisely,

- The negation of the universal statement 'for all n, property $p(n)$ holds' is the existential statement 'there is n such that property $p(n)$ does not hold'.
- The negation of the existential statement 'there is n such that property $p(n)$ holds' is the universal statement 'for all n, property $p(n)$ does not hold'.

We could be a little more formal about this, by defining the negation of a predicate $p(n)$ (which, recall, only has a definitive true or false value once n is specified) to be the predicate $\neg p(n)$ which is true (for any particular n) precisely when $p(n)$ is false. Then we might say that

- The negation of the universal statement 'for all n, the statement $p(n)$ is true' is the existential statement 'there is n such that $\neg p(n)$ is true'.
- The negation of the existential statement 'there is n such that $p(n)$ is true' is the universal statement 'for all n, the statement $\neg p(n)$ is true'.

Now, let's not get confused here. None of this is really difficult or new. We meet such logic in everyday life. If I say 'It rains every day in London' then either this statement is true or it is false. If it is false, it is because on (at least) one day it does not rain. The negation (or disproof) of the statement 'On every day, it rains in London' is simply 'There is a day on which it does not rain in London'. The former is a universal statement ('On every day, ...') and the latter is an existential statement ('there is a day ...'). Or, consider the statement 'There is a student who enjoys reading these lecture notes'. This is an existential statement ('There is ...'). This is false if 'No student enjoys reading these lecture notes'. Another way of phrasing this last statement is 'Every student reading these lecture notes does not enjoy it'. This is a more awkward expression, but it emphasises that the negation of the initial, existential statement, is a universal one ('Every student ...').

The former is an existential statement ('there is something I will write that ...') and the latter is a universal statement ('everything I write will ...). This second example is a little more complicated, but it serves to illustrate the point that much of logic is simple common sense.

2.3.2 Conjunction and disjunction

There are two very basic ways of combining propositions: through the use of 'and' (known as conjunction) and the use of 'or' (known as disjunction).

Suppose that P and Q are two mathematical statements. Then 'P and Q', also denoted $P \wedge Q$, and called the *conjunction* of P and Q, is the statement that is true precisely when *both* P and Q are true. For example, statement (e) above, which is

'50 is divisible by 2 and 5'

is the conjunction of the two statements

- 50 is divisible by 2
- 50 is divisible by 5.

Statement (e) is true because *both* of these two statements are true.

Table 2.2 gives the truth table for the conjunction P and Q:

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

Table 2.2: The truth table for 'and'

What Table 2.2 says is simply that $P \wedge Q$ is true precisely when *both* P and Q are true (and in no other circumstances).

Suppose that P and Q are two mathematical statements. Then 'P or Q', also denoted $P \vee Q$, and called the *disjunction* of P and Q, is the statement that is true precisely when P, or Q, or both, are true. For example, statement (d) above, which is

'21 is divisible by 3 or 5'

is the disjunction of the two statements

- 21 is divisible by 3
- 21 is divisible by 5.

Statement (d) is true because at least one (namely the first) of these two statements is true.

Note one important thing about the mathematical interpretation of the word 'or'. It is *always* used in the 'inclusive-or' sense. So $P \vee Q$ is true in the case when P is true, or Q is true, or *both*. In some ways, this use of the word 'or' contrasts with its use in normal everyday language, where it is often used to specify a choice between mutually exclusive alternatives. (For example 'You're either with us or against us'.) But if I say 'Tomorrow I will wear brown trousers or I will wear a yellow shirt' then, in the mathematical way in which the word 'or' is used, the statement would be true if I wore brown trousers and any shirt, any trousers and a yellow shirt, and also if I wore brown trousers and a yellow shirt. You might have your doubts about my dress sense in this last case, but, logically, it makes my statement true.

Table 2.3 gives the truth table for the disjunction P and Q:

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

Table 2.3: The truth table for 'or'

What Table 2.3 says is simply that $P \vee Q$ is true precisely when *at least one of* P and Q is true.

2.3.3 If-then statements

It is very important to understand the formal meaning of the word 'if' in mathematics. The word is often used rather sloppily in everyday life, but has a very precise mathematical meaning. Let me give you an example. Suppose I tell you 'If it rains, then I wear a raincoat', and suppose that this is a true statement. Well, then, suppose it rains. You can certainly conclude I will wear a raincoat. But what if it does not rain? Well, you can't conclude anything. My statement only tells you about what happens *if* it rains. If it does not, then I might, or I might not, wear a raincoat: and whether I do or not does not affect the truth of the statement I made. You have to be clear about this: an 'if-then' statement only tells you about what follows *if* something particular happens.

More formally, suppose P and Q are mathematical statements (each of which can therefore be either true or false). Then we can form the statement denoted $P \implies Q$ ('P implies Q' or, equivalently, 'if P, then Q'), which has as its truth table Table 2.3.3. (This type of statement is known as an *if-then* statement or an *implication*.)

Note that the statement $P \implies Q$ is false only when P is true but Q is false. To go back to the previous example, the statement 'If it rains, I wear a raincoat' is false precisely if it does rain but I do not wear a raincoat.

P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T
F	F	T

Table 2.4: The truth table for '$P \implies Q$'

Critical

Warning 2.2. Many students focus on the 'if the premise is true' first two lines of the truth table above, and forget the last two lines. We will need to use all four lines regularly, so do not do this. Yes, the mathematical $\implies$ is a bit different to the usual English 'implies', but this is something you simply need to get used to. For the next few months, every time you use $\implies$, think for a few seconds about whether you have really written what you wanted to write.

The statement $P \implies Q$ can also be written as $Q \impliedby P$. There are different ways of describing $P \implies Q$, such as:

- if P then Q
- P implies Q
- P is sufficient for Q
- Q if P
- P only if Q
- Q whenever P
- Q is necessary for P.

All these mean the same thing. The first two are the ones I will use most frequently.

2.3.4 If and only if statements; logical equivalence

If $P \implies Q$ and $Q \implies P$ then this means that Q will be true precisely when P is. That is Q is true *if and only if* P is. We use the single piece of notation $P \iff Q$ instead of the two separate $P \implies Q$ and $P \impliedby Q$. There are several phrases for describing what $P \iff Q$ means, such as:

- P if and only if Q (sometimes abbreviated to 'P iff Q')
- P is equivalent to Q
- P is necessary and sufficient for Q
- Q is necessary and sufficient for P.

The truth table is shown in Table 2.5, where we have also indicated the truth or falsity of $P \implies Q$ and $Q \implies P$ to emphasise that $P \iff Q$ is the same as the conjunction $(P \implies Q) \wedge (Q \implies P)$.

What the table shows is that $P \iff Q$ is true precisely when P and Q are either both true or both false.

P	Q	$P \implies Q$	$Q \implies P$	$P \iff Q$
T	**T**	T	T	**T**
T	**F**	F	T	**F**
F	**T**	T	F	**F**
F	**F**	T	T	**T**

Table 2.5: The truth table for '$P \iff Q$'

Activity 2.1. *Look carefully at the truth table and understand why the values for $P \iff Q$ are as they are. In particular, try to explain in words why the truth table is the way it is.*

So far in mathematics, most statements you have seen are 'if and only if' statements. In particular when you rearrange equations, you're (usually!) saying '*these* two things are equal if and only if *those* two things are equal'. In fact, most of the times that you have seen a 'genuine' $\implies$ (I mean, one where it would not be true to write $\iff$) it's been as a warning that something nasty might be around the corner: it's true that if $a = b$ then $a^2 = b^2$, but it's not always true that if $a^2 = b^2$ then $a = b$, so be careful.

That is **not** how things will be for most of the mathematics you will study, and you will get used to 'implies' being the normal thing. That shouldn't be surprising. There are usually several different possible causes for the same effect, so any one of these causes will imply the effect. If you stay inside, you won't get sunburnt; if you use sunscreen, you won't get sunburnt; if you wear a spacesuit, you won't get sunburnt. The converse is generally going to be false—it is not true that if you don't get sunburnt, then the reason is that you used sunscreen, and stayed inside, and wore a spacesuit.

Another piece of vocabulary we will sometimes use, when we are told $A \iff B$, is that A and B are *logically equivalent.* Spelling it out, we say A and B are logically equivalent if either they are both true, or they are both false. Generally, we will say things like 'P is true if and only if Q is true' when we need to look at what the statements P and Q actually are—as mathematical statements, maybe talking about integers—in order to see why the $\iff$ is the case. We will say that A and B are 'logically equivalent' if we do not need to understand the mathematical meaning of the statements at all, we only need to look at the logic. This is 'to help the reader'.

Example 2.3. The statements $\neg(P \vee Q)$ and $\neg P \wedge \neg Q$ are logically equivalent.

To see that this is true, we can draw out the truth tables:

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

Table 2.6: The truth tables for $\neg(P \vee Q)$ and $\neg P \wedge \neg Q$

We can see that the two bold lines are the same—these two statements are logically equivalent.

So I might say 'We know that the flobble is not either pretty or quick. It is logically equivalent to say that the flobble is not pretty, and the flobble is not quick.'—and I presumably want to go on for a few more lines of argument to tell you something interesting about the flobble. However what I've signalled here is that you do not need to know what a flobble is, nor what it should mean for one to be pretty or quick, in order to be happy with this particular line of argument.

If on the other hand, I say 'a graph is bipartite if and only if it contains no odd cycle' then I'm signalling that in order to be happy that this statement is true (it is) you will need to look up definitions of all the funny words in the sentence (don't do that now!) and do some 'real maths' not 'just logic'.

Critical

Activity 2.2. *Show that the statements* $\neg(P \wedge Q)$ *and* $\neg P \vee \neg Q$ *are logically equivalent.*

2.4 Implications and associated statements

Given an implication $P \implies Q$, there are three more 'associated' statements we can make by swapping P and Q for $\neg P$ and $\neg Q$, by reversing the implication, or both. One of these is important because it is logically equivalent to $P \implies Q$ (and this turns out to be very useful) and the other two are important because they are *not* logically equivalent to $P \implies Q$ (and this is a standard way to make mistakes).

2.4.1 Converse statements

The implication $Q \implies P$ is the *converse* of $P \implies Q$. Generally, there is no reason why the converse should be true just because the implication is. For example, consider the statement 'If it is Tuesday, then I buy the Guardian newspaper'. The converse is 'If I buy the Guardian newspaper, then it is Tuesday'. Well, I might buy that newspaper on other days too, in which case the implication can be true but the converse false.

We've seen, in fact, that if both $P \implies Q$ and $Q \implies P$ then we have a special notation, $P \iff Q$, for this situation. Generally, then, the truth or falsity of the converse $Q \implies P$ has to be determined separately from that of the implication $P \implies Q$.

Activity 2.3. *What is the converse of the statement 'if the natural number n divides 4 then n divides 12'? Is the converse true? Is the original statement true?*

2.4.2 Contrapositive statements

Critical

The *contrapositive* of an implication $P \implies Q$ is the statement $\neg Q \implies \neg P$. The contrapositive is logically equivalent to the implication.

This is shown in Table 2.7. (The columns highlighted in bold are identical.)

P	Q	$P \implies Q$	$\neg P$	$\neg Q$	$\neg Q \implies \neg P$
T	T	**T**	F	F	**T**
T	F	**F**	F	T	**F**
F	T	**T**	T	F	**T**
F	F	**T**	T	T	**T**

Table 2.7: The truth tables for $P \implies Q$ and $\neg Q \implies \neg P$.

If you think about it, the equivalence of the implication and its contrapositive makes sense. For, $\neg Q \implies \neg P$ says that if Q is false, P is false also. So, it tells us that we cannot have Q false and P true, which is precisely the same information as is given by $P \implies Q$.

So what's the point of this? Well, sometimes you might want to prove $P \implies Q$ and it will, in fact, be easier to prove instead the equivalent (contrapositive) statement $\neg Q \implies \neg P$. You will see many examples of this through your degree.

2.4.3 Converse of the contrapositive

Finally, $\neg P \implies \neg Q$ is the converse of the contrapositive of $P \implies Q$. As we've seen, this is logically equivalent to the converse, so *not* logically equivalent to $P \implies Q$, but all the 'not's floating around can make this hard to see, especially if P and Q are complicated statements with 'not's in themselves.

Warning 2.4. It is very easy to get tricked into believing that just because a statement is true, so is its converse (or the contrapositive of its converse). If you wear sunscreen, you will not get sunburnt. If you tell someone 'you are not wearing sunscreen, so you will get sunburnt' you might be right; on the other hand if it's midnight, you will probably get laughed at.

Mistake 1 (The theorem doesn't apply, so its conclusion is false)**.** *I've just finished (summer 2019) marking MA103 exams in which a large number of students wrote 'the conditions of Theorem A are not met, so the conclusion is false'. That is exactly the same error as the midnight sunscreen advocate: Theorem A is an 'if P then Q' statement, and it can perfectly well be that P is false but (for some other reason) Q is still true. So these answers received zero marks, and this paragraph has been added.*

Summer 2020: The same mistake again. I'll keep adding to this each year many students lose marks for this class of error in the exam.

Summer 2021: Well, there were less of these mistakes, but it made the difference between passing and failing for quite a few.

Summer 2022: We didn't have a question of this form this year.

Summer 2023: This was one way students failed to answer Q2c.

Summer 2024: Question 3c picked up some answers like 'the EVT doesn't apply so no maximum exists'—unfortunately, the maximum does exist.

2.5 What is a proof?

You should probably have some idea of what a proof is by now: you start with some statements you're assuming to be true (usually called *axioms*), from these statements you deduce others (using the rules of logic) and eventually you get to the statement you wanted to prove. If you are being very formal, you should write down every single step.

If you write down every single step, you're in a great position if someone wants to argue with your proof. If someone doesn't agree with your conclusion—the statement you're proving—it's their problem to find a mistake in your proof. That means they have to point at some statement in your proof and say that they do not believe it. Now there are two sorts of statements in your proof: ones which follow logically from earlier statements, and your axioms. If the doubter says they don't believe something which follows logically from earlier statements, then they have to point at one of these earlier statements and say they don't like that one either (or they tell you they don't believe in logic, in which case you can safely stop listening). Eventually they will either be convinced you were right all along, or they will get back to one of your axioms and say they disagree with that. Now, if you have some strange non-standard axiom, then there might even be a good reason to argue. But if you stick to standard axioms, like 'addition of natural numbers is commutative', then no-one is going to argue—which means you will convince everyone that what you claim is true. This is the gold standard of proof.

The problem with writing down every single step is that it takes a very long time to actually get anywhere. Look back to the proof on page 8—it takes eight lines to do a piece of algebra which you would normally write out in one line, and even that proof skips the steps of proving from axioms that $2 \times 2 = 2 + 2 = 4$. You don't want to spend the next three years taking pages and pages to write out simple algebra, so we need to agree on a way to write proofs which is shorter. There are two ways to do this, and we will use both.

The first way is that, as we go through the course (and the degree) we will make for ourselves a library of true statements—ones which we already proved—and we will not repeat the proofs every time we want to use them. So, for example, we already proved that for every natural number n, the number $n^2 + n$ is even (We didn't really write out every single step—if you don't like that, try doing it yourself). Next time we want to know that $n^2 + n$ is even for some natural number n, we won't need to prove it, we can just say 'proved in MA103'. There's nothing much anyone can object to here—it's clear that we could have written out a gold standard proof just by copying-and-pasting in the proof from MA103.

The second way we will save time is by *not* writing out every single step. When you need to do a piece of algebra, do it just as you did in school, and we will assume you do know how to justify all the steps by going back to the axioms (or at least that you know where to look in order to find out how). We will also sometimes save steps by saying that something is 'obvious', or 'clear'. When you (or I) write 'obvious' or 'clear' in a proof, it is there to tell the reader that there are some steps missing, that you (or I) know what those steps are, and that the reader should have no trouble figuring out what the missing steps are. What this also means is: **if you cannot explain why a statement is true, then you cannot write that it is 'obvious' in a proof**. You will need to make a judgement of how many steps it is OK to skip.

You will quickly get used to what is and what is not acceptable as a proof—assuming you do the weekly exercises—because your class teacher will correct you. What you should keep in mind is that whatever you write as a proof should be something which you could expand out to a gold standard proof if you were forced to, either from memory or because you know where to look for the missing pieces and previously proved statements.

As we go on, those 'missing pieces and previously proved statements' will get pretty long: there will be proofs you write later this year in a page or two which might take a hundred or more pages to write out in 'gold standard' style. For an example (which you shouldn't expect to understand when you read this the first time; but it will make sense when you're revising) think about how to prove that a piece of simple algebra with the rational numbers makes sense, in terms of the axioms for the natural numbers. We prove in this course that you can do it (which is enough—if I know something is possible, I don't have to actually do it to check it works)—but try actually doing it!

2.6 How to prove it

As you will soon see, it is not easy to find proofs. Sometimes you will be asked to prove a statement where there is an 'obvious' way to proceed—as soon as you understand the statement, you have an idea what to try—but mainly you will not see what to do at first. For some (most!) true statements, no-one has ever figured out a proof; you shouldn't feel bad that you do not find it easy!

However, there are some strategies which you can use to help. The thing to keep in mind is that

a proof is a sequence of implications, but that is not normally the order in which you think of it.

What that means is that you may not see how to get started—or maybe you know what the first thing to do is, but not what comes next in the proof—but you perhaps can see that if you could prove some statement S, then that would imply what you want to prove. If S is 'easier' somehow than the conclusion you want to get to, then that's progress. Sometimes it can be easier to start at the 'end' of the proof and 'work backwards'. You have to be a bit careful doing this—see Mistake 4 below—but it is still a good strategy.

My suggestion, if you think you would like to 'work backwards' to solve a problem, is to write the conclusion at the bottom of the sheet and literally work backwards, writing up the page, occasionally adding stuff at the top, and try to meet in the middle. You'll probably have a big gap in the middle when you're done, but that is fine (it's certainly better than running out of room). If you really don't like it, recopy the proof on a fresh sheet of paper.

However, I can't do that in printed notes to give an example, so I will use different colours. I'm first going to simply write out a proof, then explain what the colours mean and how I got to it.

Example 2.5. Prove that for all real numbers a and b we have $ab \leq \frac{a^2+b^2}{2}$.

Proof. For all real a, b we have $ab \leq \frac{a^2+b^2}{2}$.

Let p and q be real numbers. We have $pq \leq \frac{p^2+q^2}{2}$.

We have $2pq \leq p^2 + q^2$.

We have $p^2 - 2pq + q^2 \geq 0$.

We have $(p-q)^2 \geq 0$.

Since p and q are real numbers, $p-q$ is a real number. Since the square of any real number is non-negative, we have $(p-q)^2 \geq 0$.

Expanding the brackets, we have $p^2 - 2pq + q^2 \geq 0$.

Rearranging, we get $pq \leq \frac{p^2+q^2}{2}$.

Since we proved $pq \leq \frac{p^2+q^2}{2}$ for an arbitrary pair p and q of real numbers, we can conclude that for all real a, b we have $ab \leq \frac{a^2+b^2}{2}$. □

What is going on here? The black text on the left is the proof we wanted. I've written it out in a bit more detail than you would maybe feel necessary, in order to mention a couple of important points. The red text on the right is the 'current aim'—this is *what we want to prove*, we have not yet proved it! The first line is simply repeating the text of the example. Let me repeat what this aim is, in English. It is:

Pick any two real numbers. Then their product is at most half the sum of their squares.

Next, we pick a couple of real numbers p and q. We don't assume anything about them apart from that they are real numbers—that's what the word 'arbitrary' means. We want to check that for *this particular* pair of real numbers, we have the inequality we want—so the current aim (the red text on the right) gets simpler. This is a standard approach to proving 'for all' statements; again, we'll say more about this later.

At this point, I don't see how to proceed 'forwards' in the proof; it's not obvious what the next black line should be, because the 'aim' inequality is complicated. So I try to 'work backwards' and rearrange the 'aim' to something easier. That's the next few red lines: get rid of fractions, collect all the terms on one side, try to factorise—these are all things you can try. If one doesn't turn out to help, no problem, try another! In this example, we get to the nice simple aim $(p-q)^2 \geq 0$.

Now I have reached an aim which I know how to prove true, so I write it down (that's the next black line). Finally, I can write out the rest of the proof, by writing out the red lines in reverse; if you were trying this following the suggestion to work literally backwards from the bottom of the paper, you'd already have written these lines from the bottom of the paper, and this is where you would stop.

Finally—check that this proof makes sense! Does each black line really follow from the previous ones?

I would be perfectly happy with a proof like:

Proof. Let a, b be any real numbers, then $(a-b)^2 \geq 0$, rearranging we get $ab \leq \frac{a^2+b^2}{2}$ so we are done. □

Reading this proof, there is a 'magic step': for some reason we write $(a-b)^2 \geq 0$ and it is completely unclear how we thought of writing that. We can check it works, but we don't get any idea from this of how to find such a proof. You know how—and more or less always, if you read a proof and there is a 'magic step', there is some kind of reason, some thought process which hasn't been written down. If you try to follow this course by just reading all the solutions rather than actually trying to do the exercises, then what you will not learn is how to find these 'magic steps'. Since that will be tested in the exam, you will then suffer.

It's important to be a bit careful about what is going on with the 'for all', because many students get confused here. Read this now, but come back and re-read it once you get to the end of the next chapter and we have formally discussed quantifiers.

When we write 'for all a, b ...' the a and b are placeholders (we say *bound variables*, as opposed to the free variables that appear in predicates) that we introduce just in order to write the inequality conveniently. If you change these two letters for any others, it doesn't change the meaning of the sentence, or indeed if you write it in English without any algebra at all (as in the box above). It doesn't make sense to talk about 'what a is' on the first line; a is just a placeholder. This is why I used different letters p and q on the second line: here we declare that for the rest of the proof, we are going to work with a particular pair of real numbers p and q, and they won't change from line to line. I won't normally bother with this (because normally we are too lazy to use new letters) but you should be aware that this is a little bit naughty.

Finally, we wrapped up the proof by stressing that what 'for all' means is a promise: 'pick any pair of real numbers, check the inequality for that particular pair, and you will find that it is a true inequality.'

Warning 2.6. Is the following logic valid?
Since we picked a pair of real numbers a, b, actually we have $(a-b)^2 > 0$, so we could say that for all real a, b we have $ab < \frac{a^2+b^2}{2}$.

The answer is **no**. It is *not true* that for all real numbers a and b we have $ab < \frac{a^2+b^2}{2}$. For example, it is not true for the real numbers 1 and 1 (as you can check). When we say 'for all a, b..' we *do* include the possibility that a and b are in fact the same.

One final point to note is that this use of red text on the right in a proof is *not standard*; don't expect to see it elsewhere. This is just my best attempt to show you how we get to a proof. I'll do this in several proofs later in the notes: it will *always* be the case that if you completely ignore the red lines, what you have is a complete proof. If you are 'working backwards', you can avoid having to write red lines by literally working back from the bottom of the page; if you want to copy my red lines style, feel free, but think of the red lines as being part of your rough work that should be crossed out once you figured out and wrote down the complete proof.

2.7 What is not a proof?

There are several common mistakes made by students when they are asked to prove something. I've mentioned one already, and more will appear later in the notes. But here are the 'three classics' which I would like you not to repeat.

Mistake 2 (The goose's mistake, 'proof by example')**.** *In January, a goose hatches from an egg. Every day, the farmer feeds it. Towards the middle of December, the goose is sure that it will be fed every day forever...*

Whenever you are supposed to prove 'for all...' statements, you need to do *all* the cases not one or two; whenever you want a counterexample to 'there exists...' statements, than means you have to show *all* the possibilities fail, not just that the most obvious one fails. This probably sounds obvious written out like this, but nevertheless probably about half of you will make the goose's mistake at some point.

Mistake 3 (The ends justify the means)**.** *You are in a park and buy an ice-cream; a small child snatches it away from you. In the end, you will get your ice-cream back—explain how.*

That means: write a story. The first and last lines are given: 'You are in a park and buy an ice-cream; a small child snatches it away from you' and 'You get your ice-cream back'. What's in the middle is important. Maybe it's *'You have a long discussion of comparative morality with the child. It realises the error of its ways'*.

You're used to 'doing maths' meaning making a calculation, and the point of a calculation is to 'get the right answer'. Now, of course, it can happen that you make two mistakes in a calculation which happen to cancel out and you get the right answer even though you made mistakes—but you have to be really lucky for that to happen. Normally, if you make mistakes you get the wrong answer. So you're used to thinking (maybe subconsciously) that if the last line is right, then everything else was probably also good.

We're not doing calculations in this course, though, we're doing proofs. When you write a proof, you usually know the first and last lines before anything else: the first line is what you're assuming, and the last line is what you want to prove. What is important is actually what's in the middle which explains why the last line is true. If (when) you get a proof back from your class teacher marked as wrong even though 'the answer is right', before complaining, think: does it make a difference to the story if the middle line is instead *'You pull out your gun and shoot the child'*?

Mistake 4 (Backwards thinking)**.** *Working in reverse to obtain a proof but then not writing the proof out forwards.*

For example, consider trying to prove the following trigonometric identity: for all real numbers x, we have

$$(\cos x)^2 - \sin x = 1 - (\sin x)^2 + \sin x\,. \tag{2.1}$$

If you just work in reverse, your proof might be:

Proof. Fix a real number x.

$$\begin{aligned}
\text{We want}\qquad (\cos x)^2 - \sin x &= 1 - (\sin x)^2 + \sin x \\
\text{so}\qquad -\sin x &= 1 - (\sin x)^2 + \sin x - (\cos x)^2 && \text{subtracting } (\cos x)^2 \\
\text{so}\qquad (\sin x)^2 &= \big(1 - (\sin x)^2 + \sin x - (\cos x)^2\big)^2 && \text{squaring both sides} \\
\text{so}\qquad 0 &= \big(1 - 1 + \sin x)^2 - (\sin x)^2 = 0 && \text{subtracting } (\sin x)^2\,,
\end{aligned}$$

where to get to the last line we used the identity $(\sin x)^2 + (\cos x)^2 = 1$, which holds for all real numbers x by Pythagoras' Theorem. The last line is true, so we are done. □

Note that normally you wouldn't write justifications for each line of simple algebra—it's obvious enough how we got from each line to the next—but I wanted to do this here for extra clarity.

This looks a lot like what we did in the last section to prove Example 2.5; it's a lot like the red rearranging-the-inequality lines there. We just didn't bother to write the remaining black lines out. What's the problem?

What the above proof shows is that *if* the identity we want to prove, (2.1), holds, *then* $0 = 0$, which is a true statement. But that is the converse of the statement we want to prove, *if* $0 = 0$ *then* (2.1) holds. (Which is the same as just saying that (2.1) holds: $0 = 0$ is True.) We already know that the converse being true doesn't tell us if the original statement is true. If we want to prove the original statement, we need to *end* with the statement we want to prove, not start with it.

That might seem picky—let's see what happens if we try to write it out in the 'right order'.

Proof, take 2. Fix a real number x. We have

$$\begin{array}{lrcll}
 & 0 &=& \big(1-1+\sin x\big)^2-(\sin x)^2 & \\
\text{so} & (\sin x)^2 &=& \big(1-1+\sin x\big)^2 & \text{adding } (\sin x)^2 \\
\text{so} & (\sin x)^2 &=& \big(1-(\sin x)^2+\sin x-(\cos x)^2\big)^2 & \text{since } 1=(\sin x)^2+(\cos x)^2 \\
\text{so} & -\sin x &=& 1-(\sin x)^2+\sin x-(\cos x)^2 & \text{taking square roots} \\
\text{so} & (\cos x)^2-\sin x &=& 1-(\sin x)^2+\sin x & \text{adding } (\cos x)^2
\end{array}$$

which is what we wanted to prove. □

Looks better—but wait! In the last section, I told you to *check* the proof. The first two 'so's are fine, but the third 'so', 'taking square roots', boils down to 'If $a^2 = b^2$ then $-a = b$'—and that's not true; it could equally well be that $a = b$. There is a problem with the proof here—and the reason is that we are trying to prove a *false statement*! In fact,

$$(\cos\tfrac{\pi}{2})^2-\sin\tfrac{\pi}{2}=0^2-1=-1 \quad\text{but}\quad 1-(\sin\tfrac{\pi}{2})^2+\sin\tfrac{\pi}{2}=1-1^2+1=1\,.$$

so the 'identity' simply isn't true.

What you should learn from this example is that it is not being picky to insist on writing arguments (especially calculations with algebra) properly so that the statement to be proved comes at the end not the beginning. It is very easy to do some operation to both sides which is not reversible—in this example, squaring—without noticing and 'prove' a false statement. If you write a proof properly, i.e. forwards, then you are more likely to notice a potential problem.

2.8 Sample exercises

Exercise 2.1. *Is the following statement about natural numbers n true or false? Justify your answer by giving a proof or a counterexample:*

> *If n is divisible by 6 then n is divisible by 3.*

What are the converse and contrapositive of this statement? Is the converse true? Is the contrapositive true?

Exercise 2.2. *Is the following statement about natural numbers n true or false? Justify your answer by giving a proof or a counterexample:*

> *If n is divisible by 2 then n is divisible by 4.*

What are the converse and contrapositive of this statement? Is the converse true? Is the contrapositive true?

Exercise 2.3. *Prove that $\neg(P \wedge Q)$ and $\neg P \vee \neg Q$ are logically equivalent.*

Exercise 2.4. *Prove that the negation of $P \vee Q$ is $\neg P \wedge \neg Q$.*

Exercise 2.5. *Prove by contradiction that there is no largest natural number.*

2.9 Comments on selected activities

Comment on Activity 2.2. We can do this by constructing a truth table. Consider Table 2.8. This proves that $\neg(P \wedge Q)$ and $\neg P \vee \neg Q$ are equivalent.

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

Table 2.8: The truth tables for $\neg(P \wedge Q)$ and $\neg P \vee \neg Q$

Comment on Activity 2.3. The converse is 'if n divides 12 then n divides 4'. This is false. For instance, $n = 12$ is a counterexample. This is because 12 divides 12, but it does not divide 4. The original statement is true, however. For, if n divides 4, then for some $m \in \mathbb{Q}$, $4 = nm$ and hence $12 = 3 \times 4 = 3nm = n(3m)$, which shows that n divides 12.

2.10 Solutions to exercises

Solution to Exercise 2.1. The statement is true. For, suppose n is divisible by 6. Then for some $m \in \mathbb{N}$, $n = 6m$, so $n = 3(2m)$ and since $2m \in \mathbb{N}$, this proves that n is divisible by 3.

The converse is 'If n is divisible by 3 then n is divisible by 6'. This is false. For example, $n = 3$ is a counterexample: it is divisible by 3, but not by 6.

The contrapositive is 'If n is not divisible by 3 then n is not divisible by 6'. This is true, because it is logically equivalent to the initial statement, which we have proved to be true.

Solution to Exercise 2.2. The statement is false. For example, $n = 2$ is a counterexample: it is divisible by 2, but not by 4.

The converse is 'If n is divisible by 4 then n is divisible by 2'. This is true. For, suppose n is divisible by 4. Then for some $m \in \mathbb{N}$, $n = 4m$, so $n = 2(2m)$ and since $2m \in \mathbb{N}$, this proves that n is divisible by 2.

The contrapositive is 'If n is not divisible by 4 then n is not divisible by 2'. This is false, because it is logically equivalent to the initial statement, which we have proved to be false. Alternatively, you can see that it's false because 2 is a counterexample: it is not divisible by 4, but it *is* divisible by 2.

Solution to Exercise 2.3. This can be established by using the truth table constructed in Activity 2.2. See the solution above.

Solution to Exercise 2.4. This is established by Table 2.6. That table shows that $\neg(P \vee Q)$ is logically equivalent to $\neg P \wedge \neg Q$. This is the same as saying that the negation of $P \vee Q$ is $\neg P \wedge \neg Q$.

Solution to Exercise 2.5. Let's prove by contradiction that there is no largest natural number. So suppose there is a largest natural number. Let us call it N. (What we want to do now is somehow show that a conclusion, or something we know for sure must be false, follows.) Well, consider the number $N + 1$. This is a natural number. But since N is the largest natural number, we must have $N + 1 \leq N$, which means that $1 \leq 0$, and that's nonsense. So it follows that we must have been wrong in supposing there is a largest natural number. (That's the only place in this argument where we could have gone wrong.) So there is *no* largest natural number. We could have argued the contradiction slightly differently. Instead of using the fact that $N + 1 \leq N$ to obtain the absurd statement that $1 \leq 0$, we could have argued as follows: $N + 1$ is a natural number. But $N + 1 > N$ and this contradicts the fact that N is the largest natural number.

3

Sets and quantifiers

In this chapter, we discuss a fundamental concept in mathematics: sets. We need sets in order to talk about *quantification*, which means talking about a statement being true 'for all x', or 'for some x'. It doesn't really make sense to say that the statement $(x+2)^2 = x^2 + 2x + 4$ is 'true for all x'—it's not even clear what the statement should mean if x is a banana—but this statement is true for all x *in the set of real numbers.* That's quantification.

As with the previous chapter, there is nothing here that is difficult. However, sets and quantification are not intuitive, and unless you pay attention, you will fall into a whole collection of traps.

Actually, let me clarify that a bit. Sets and quantification are not intuitive *yet.* Once you get to the point where you automatically avoid all the traps in this chapter without having to think about it, you're most of the way to the 'thinking like a mathematician' which is what your future employer is looking for. It will happen, ideally before you sit the exam.

Mathematical grammar

You're probably rather used to feeling that 'writing properly' is a bit picky and the sort of thing you only need to care about if you want to look good for a job. In English writing, that's true. It is true because English is very redundant: you can change letters, drop words, and forget all the punctuation, and you usually don't actually confuse your reader.

In mathematical writing, it is not true. Mathematics is quite terse and we generally do not have much redundancy; this is also why you might need longer to read 10 pages of mathematics than 200 pages of a novel. If you ignore the rules, you will end up writing something which is either nonsense, or (which is worse) something meaningful but not what you intended. You will then proceed to confuse yourself and not be able to continue with the problem.

That might seem a bit ridiculous, but I can promise that in my time teaching mathematics, it has rather often happened that a student comes to my office hour stuck with a problem, I point out where they wrote some piece of bad mathematical grammar, they correct it and then 'Oh! I see how to do it now.'

What this means is things like: Use the correct brackets, and make sure you close them. Put the quantifiers first and in the correct order. Don't write the symbol = unless you really mean 'equals' (if you mean something that you would not want to pronouce 'equals', you either want a different symbol or more likely you should just write the word that comes in to your mind). In short, follow the mathematical version of the SPaG rules, which you'll see in the rest of this chapter.

A final note—when you read an English text, you can often ignore some bits, or you might need to remember that some 'context' means that there's more to think about than is actually written. In maths, neither happens: we write exactly what we mean to, neither more nor less.

3.1 Sets

You have probably already met some basic ideas about sets and there is not too much more to add at this stage, but they are such an important idea in abstract mathematics that they are worth discussing here.

If you look around on the Internet, you might run into some things talking about 'set theory' and saying that this is all very subtle, and 'unproveable' and such things. This is *not what we are going to do.* We are going to take a very simple view of sets (sometimes called *naïve set theory*). We are not going to go looking for trouble, and we will not find it, so don't worry. If you are curious about what trouble you might find if you insist on looking for it, see Section 3.6.

3.1.1 Basics

Loosely speaking, a set may be thought of as a collection of objects. A set is usually described by listing or describing its *members*, or *elements*, inside curly brackets. For example, when we write $A = \{1, 2, 3\}$, we mean that the objects belonging to the set A are the numbers $1, 2, 3$ (or, equivalently, the set A consists of the numbers $1, 2$ and 3). Equally (and this is what we mean by 'describing' its members), this set could have been written as

$$A = \{n \mid n \text{ is a whole number and } 1 \leq n \leq 3\}.$$

Here, the symbol | stands for 'such that'. Often, the symbol ':' is used instead, so that we might write

$$A = \{n : n \text{ is a whole number and } 1 \leq n \leq 3\}.$$

When x is an object in a set A, we write $x \in A$ and say 'x belongs to A', or 'x is in A', or 'x is a member of A'. If x is not in A we write $x \notin A$.

As another example, the set

$$B = \{x \in \mathbb{N} \mid x \text{ is even}\}$$

has as its members the set of positive even integers. Here we are specifying the set by *describing* the defining property of its members.

One point which is important is that it doesn't make sense to say that an object is in a set twice. It's either in or not, and this is the end. We'll avoid writing obvious repetitions, like $S = \{1, 2, 3, 1\}$. That *is* a set, and it is the same as the set $\{1, 2, 3\}$; whichever way I write it, it contains 1, 2 and 3 and nothing else. But sometimes it will be painful to write a description avoiding repetition.

Sometimes it is useful to give a *constructional* description of a set. For example, $C = \{n^2 \mid n \in \mathbb{N}\}$ is the set of natural numbers known as the 'perfect squares'.

We could also write $D = \{z^2 \mid z \in \mathbb{Z}\}$, where $\mathbb{Z}$ is the set of all (not just positive) integers. The difference between C and D is simple: D contains 0 and C does not. That's the only difference. By definition $(-3)^2 = 9$ is in D, but it is also in C, because $3^2 = 9$ is by definition in C. It doesn't matter that our definition of D repeats some elements (like $9 = (-3)^2 = 3^2$).

The set which has no members is called the *empty set* and is denoted by $\varnothing$. The empty set may seem like a strange concept, but it is useful to define. Think about lengths—'zero centimetres' is a funny length, but if we didn't want to use it, we would have trouble with the question 'How much longer is a metre than 100 centimetres?'.

The short version of all of this is: when you want to define a set, you write the complete description within the curly braces, in any of the ways above.

Warning 3.1. You do need to be careful about writing down sets. When we write $B = \{n \in \mathbb{N} \mid n \text{ is even}\}$, the letter n is a bound variable: a placeholder. It doesn't mean anything to ask 'what is n in B'. It makes no difference if you change the letter n for another letter.

Rather often students intend to write down a set, but put some of the description outside the curly braces. Things like writing '$B = \{n \in \mathbb{N}\}$ n is even'. This particular example doesn't make sense—in English, it reads 'B is the set of all natural numbers n is even' which looks like someone forgot a full-stop. Sometimes though, it does make sense but isn't what was intended. Either way, this is guaranteed to lose marks.

You may find this picky: bear in mind that in your future job you'll probably ask computers for answers rather often. If you cannot formulate the question accurately, the computer will either complain or happily give you an answer to a question you didn't mean to ask. This is no different.

3.1.2 A note on notation

You should notice that the 'is a member of' symbol $\in$ is written by drawing a semicircle on its side, lifting the pencil and putting a bar from the middle. There is another symbol ε which looks rather similar; this symbol is drawn in one stroke. This second symbol is the Greek letter epsilon.

Many students in recent years confuse these two symbols. I don't know why—maybe your teacher at school used ε for 'is a member of'. What I do know is that you **must stop doing this**. Later this term, you will be using the Greek letter ε a great deal—in Analysis—and you will at the same time be working with sets. If you draw $\in$ and ε in the same way, you will end up writing 'for all $\varepsilon\varepsilon(0,1)$' and having to remember that one of these ε symbols is supposed to be a real number and the other means 'is a member of'. It's rather easier to see what's going on if you write $\varepsilon \in (0,1)$.

Getting into the bad habit of writing ε when you mean $\in$ will make your life difficult, especially when you do it in the exam and lose marks unnecessarily.

Similarly, the brackets that go around sets are $\{$ and $\}$. They are not (and). Nor [and]. Not even $\langle$ and $\rangle$. Those other kinds of brackets all have different meanings in mathematics (we'll see all but $\langle$ and $\rangle$ in this course).

In general, the more mathematics you do, the more symbols you will encounter, and the more your life will become difficult if you cannot write them distinctly or if you misuse them. You've no doubt already noticed at school that $\times$ and x are distinct symbols and that if you write the latter with two diagonal lines, then you probably at some time tried to cancel an x with a multiplication and got the wrong answer. Similarly, 2, z and Z are sometimes written indistinguishably, with similar consequences. If we can't tell whether your exam answer is correct because we cannot distinguish the symbols you use, then we cannot give you the marks; that would be a particularly silly way to not get the First you want.

3.1.3 Set equality

We've already written = between two sets above, but let's be completely clear what it means. So far, we saw = only to talk about when two numbers are equal—that's something you're so used to that you don't think about what it means (which is fine). But we need to define set equality.

Suppose A and B are two sets. We can write $A = B$ when

$$\textsf{for all } x \textsf{ we have } x \in A \iff x \in B\,.$$

Let's see why $\{1,2,3\} = \{1,2,3,1\}$ according to this definition. We have to check a certain predicate (namely $x \in \{1,2,3\} \iff x \in \{1,2,3,1\}$) is true for every x. Well, for $x = 1$ it's true, 1 is in both sets. For $x = 2$ it is true, 2 is in both sets. For $x = 3$ it is true, 3 is in both sets. For $x = 4$ it is true, 4 is in neither set. For $x = \textsf{banana}$ it is true, banana is in neither set. And so on... for any x except the ones we already checked, the predicate is true because x is in neither set.

3.1.4 Subsets

We say that the set S is a *subset* of the set T, and we write $S \subseteq T$, if every member of S is a member of T. For example, $\{1,2,5\} \subseteq \{1,2,4,5,6,40\}$. (Be aware that some texts use $\subset$ where we use $\subseteq$.) What this means is that we have

$$\textsf{for all } x \textsf{ we have } x \in A \implies x \in B\,.$$

A rather obvious, but sometimes useful, observation is that, given two sets A and B, $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$. So to prove two sets are equal, we can prove that each of these two 'containments' holds. That might seem clumsy, but it is, in many cases, the best approach.

For any set A, the empty set, $\varnothing$, is a subset of A. You might think this is strange, because what it means is that 'every member of $\varnothing$ is also a member of A'. But $\varnothing$ has no members—how can that be true? Let's go back to the logic: 'every member of $\varnothing$ is also a member of A' means 'for each x, if x in $\varnothing$ then $x \in A$'. Check the truth table of if—then ($\Longrightarrow$). The only way some x can be a counterexample to this statement is if x is in $\varnothing$ and not in A. But there is no x such that $x \in \varnothing$, by definition—so we proved $\varnothing \subseteq A$.

It's very easy to get confused about what sets are equal, what are members and what are subsets of a set. I'm about to give an example, which right now will look like a deliberate attempt to trick you. But things like this will show up later, not as a trick, and you need to get it right.

Critical

Warning 3.2. Consider the set $S = \{0, 1, \{0, 1\}, \{2\}\}$. What are its members and subsets?

Well, 0 is a member. And so is 1, and so is $\{0, 1\}$, and so is $\{2\}$. But 2 is **not** a member of S. Furthermore, $\{0, 1\}$ is a subset of S (because 0 and 1 are both members of S) and so is $\{\{0, 1\}\}$. These are **two different sets**—$\{0, 1\} \neq \{\{0, 1\}\}$. And there are some other subsets of S too—try to write them all out; you should get 16 in total.

If you don't like the statements above, maybe think of it this way. Any (mathematical) object can go in a set, so the number 1 can go in, or a function can go in, or even another set. This is just the same thing as saying that you can put a (normal) object in a parcel, so an apple can go in a parcel, or an orange can go in a parcel, or a parcel full of sweets can go in another parcel, and so on. If you think a parcel containing a parcel full of sweets is the same as a parcel full of sweets (or it's the same as just having a lot of sweets), think back to childhood games of Pass-the-Parcel. Just like that game, it really matters how many of the { and } set brackets there are, and what exactly they go round.

3.1.5 Unions and intersections

Given two sets A and B, the *union* $A \cup B$ is the set whose members belong to A or B (or both A and B): that is,

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

Equivalently, writing out the definition of set equality:

$$\text{for all } x \text{ we have } x \in A \cup B \iff (x \in A) \vee (x \in B).$$

Example 3.3. If $A = \{1, 2, 3, 5\}$ and $B = \{2, 4, 5, 7\}$, then $A \cup B = \{1, 2, 3, 4, 5, 7\}$.

Similarly, we define the *intersection* $A \cap B$ to be the set whose members belong to both A and B:

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

In other words,

$$\text{for all } x \text{ we have } x \in A \cap B \iff (x \in A) \wedge (x \in B).$$

3.1.6 Arbitrary unions and intersections

Often we will want to take the union of a lot of sets, for example $A_1 \cup A_2 \cup A_3 \cup A_4 \cup A_5$. This is a pain to write out in this way, and if we wanted to take the union of infinitely many sets, we wouldn't be able to do it at all. So we define a notation which lets us write such a thing easily.

Suppose that I is a set, which we will call the *index set*, and that for each $i \in I$ we have some set A_i (so in the example above, $I = \{1, 2, 3, 4, 5\}$). Then we define the *arbitrary union*

$$\bigcup_{i \in I} A_i = \left\{ x \mid x \in A_i \text{ for at least one } i \in I \right\}.$$

The phrase 'index set' is supposed to help the reader: it is telling you 'this set is here so that we can put it under a $\bigcup$'. It doesn't mean that I is in any way special.

Similarly, we define the *arbitrary intersection*

$$\bigcap_{i \in I} A_i = \left\{ x \mid x \in A_i \text{ for all } i \in I \right\}.$$

You should check for yourself that

$$\bigcup_{i \in \{1,2,3,4,5\}} A_i$$

really defines the same set as $A_1 \cup A_2 \cup A_3 \cup A_4 \cup A_5$, and similarly with the arbitrary intersection.

What do these definitions mean if $I = \varnothing$? It's not very obvious, and we need to talk about *universal sets* to understand it. We'll get back to this later; for now, just think of $\bigcup$ as a convenient way to avoid writing a long string of $\cup$s.

Finally, prior to this 'bound variables' have always had 'for all' or 'there exists' next to them. Here's a different example. In the notation $\bigcap_{i \in I} A_i$, the i is a bound variable: that is, it's just a placeholder and doesn't mean anything 'outside' the expression.

3.1.7 Universal sets and complements

We've been a little informal about what the possible 'objects' in a set might be. In fact, we haven't been very clear about what exactly is and is not a set—this is a genuine difficulty. See Section 3.6 for a brief discussion of this. In this course, we will take the (not very rigorous!) point of view that anything we claim is a set, really is. In order for this to make some kind of sense, we will always work with respect to some 'universal set' E. For example, if we are thinking about sets of natural numbers, the universal set (the possible candidates for membership of the sets we might want to consider) is the set $\mathbb{N}$ of all natural numbers.

This might seem like an unnecessary complication, but it is essential. Suppose I tell you that the set A is the set of all even natural numbers. What are the objects that do not belong to A? Well, in the context of natural numbers, it is all odd natural numbers. The context is important (and it is this that is encapsulated in the universal set). Without that context (or universal set), then there are many other objects that we could say do not belong to A, such as negative integers, apples, bananas and elephants. (I could go on, but I hope you get the point!)

Given a universal set E and a subset A of E, the *complement* of A (sometimes called the *complement of A in E*) is denoted by $E \smallsetminus A$ and is

$$E \smallsetminus A = \{x \in E \mid x \notin A\}.$$

If the universal set is clear, the complement of A is sometimes denoted by $\bar{A}$ or A^c (with textbooks differing in their notation).

Suppose A is any subset of E. Because each member of E is either a member of A, or is not a member of A, it follows that

$$A \cup (E \setminus A) = E.$$

You should never worry 'what is the universal set' in this course. If you need to know it (which is rare), it will be clearly stated what it is. If you don't need to know it, you also don't need to worry about it.

3.1.8 Sets and logic

There are a great many comparisons and analogies between set theory and logic. Using the shorthand notation for complements, one of the 'De Morgan' laws of complementation is that

$$\overline{A \cap B} = \bar{A} \cup \bar{B}.$$

This looks a little like the fact (see Activity 2.2) that $\neg(P \wedge Q)$ is equivalent to $\neg P \vee \neg Q$. And this is more than a coincidence. The negation operation, the conjunction operation, and the disjunction operation on statements behave entirely in the same way as the complementation, intersection, and union operations (in turn) on sets. In fact, when you start to prove things about sets, you often end up giving arguments that are based in logic.

For example, how would we prove that $\overline{A \cap B} = \bar{A} \cup \bar{B}$? We could argue as follows:

$$\begin{aligned}
x \in \overline{A \cap B} &\iff x \notin A \cap B \\
&\iff \neg(x \in A \cap B) \\
&\iff \neg((x \in A) \wedge (x \in B)) \\
&\iff \neg(x \in A) \vee \neg(x \in B) \\
&\iff (x \in \bar{A}) \vee (x \in \bar{B}) \\
&\iff x \in \bar{A} \cup \bar{B}.
\end{aligned}$$

What the result says is, in fact, easy to understand: if x is not in *both* A and B, then that's precisely because it fails to be in (at least) one of them.

For two sets A and B (subsets of a universal set E), the *complement of B in A*, denoted by $A \setminus B$, is the set of objects that belong to A but not to B. That is,

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

Activity 3.1. *Prove that $A \setminus B = A \cap (E \setminus B)$.*

3.1.9 Cartesian products

For sets A and B, the *Cartesian product* $A \times B$ is the set of all *ordered pairs* (a, b), where $a \in A$ and $b \in B$. For example, if $A = B = \mathbb{R}$ then $A \times B = \mathbb{R} \times \mathbb{R}$ is the set of all ordered pairs of real numbers ('the set of points in the plane'), usually denoted by $\mathbb{R}^2$.

We can similarly define products of many sets. You've already seen this, for example

$$\mathbb{R} \times \mathbb{R} \times \mathbb{R} = \mathbb{R}^3 = \{(a, b, c) : a, b, c, \in \mathbb{R}\},$$

which you've probably seen before as the set of points in space.

3.1.10 Power sets

For a set A, the set of all subsets of A, denoted $\mathcal{P}(A)$, is called the *power set* of A. Note that the power set is a set of sets. For example, if $A = \{1, 2, 3\}$, then

$$\mathcal{P}(A) = \big\{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\big\}.$$

Activity 3.2. *Write down the power set of the set* $A = \{1, 2, 3, 4\}$*.*

Activity 3.3. *Suppose that* A *has* n *members, where* $n \in \mathbb{N}$*. How many members does* $\mathcal{P}(A)$ *have?*

3.2 Quantifiers

We have already met the ideas of universal and existential statements involving natural numbers. More generally, given any set E, a *universal statement* on E is one of the form 'for all $x \in E$, $P(x)$'. This statement is true if $P(x)$ is true for all x in E, and it is false if there is some x in E (known as a *counterexample*) such that $P(x)$ is false. We have a special symbol that is used in universal statements: the symbol '$\forall$' means 'for all'. So the typical universal statement can be written as

$$\forall x \in E,\ P(x).$$

(The comma is not necessary, but I think it looks better.) An *existential statement* on E is one of the form 'there is $x \in E$ such that $P(x)$', which is true if there is some $x \in E$ for which $P(x)$ is true, and is false if for every $x \in E$, $P(x)$ is false. Again, we have a useful symbol, '$\exists$', meaning 'there exists'. So the typical existential statement can be written as

$$\exists x \in E,\ P(x).$$

Here, we have omitted the phrase 'such that', but this is often included if the statement reads better with it. For instance, we could write

$$\exists n \in \mathbb{N},\ n^2 - 2n + 1 = 0,$$

but it would probably be easier to read

$$\exists n \in \mathbb{N} \text{ such that } n^2 - 2n + 1 = 0.$$

Often 'such that' is abbreviated to 's.t.'. (By the way, this statement is true because $n = 1$ satisfies $n^2 - 2n + 1 = 0$.)

We have seen that the negation of a universal statement is an existential statement and vice versa. In symbols, $\neg(\forall x \in E,\ P(x))$ is logically equivalent to $\exists x \in E,\ \neg P(x)$; and $\neg(\exists x \in E,\ P(x))$ is logically equivalent to $\forall x \in E,\ \neg P(x)$.

With these observations, we can now form the negations of more complex statements. Consider the statement

$$\forall n \in \mathbb{N}, \exists m \in \mathbb{N}, m > n.$$

Activity 3.4. *What does the statement $\forall n \in \mathbb{N}, \exists m \in \mathbb{N}, m > n$ mean? Is it true?*

What would the negation of the statement be? Let's take it gently. First, notice that the statement is

$$\forall n \in \mathbb{N}, (\exists m \in \mathbb{N}, m > n).$$

The parentheses here do not change the meaning. According to the rules for negation of universal statements, the negation of this is

$$\exists n \in \mathbb{N}, \neg(\exists m \in \mathbb{N}, m > n).$$

But what is $\neg(\exists m \in \mathbb{N}, m > n)$? According to the rules for negating existential statements, this is equivalent to $\forall m \in \mathbb{N}, \neg(m > n)$. What is $\neg(m > n)$? Well, it's just $m \leq n$. So what we see is that the negation of the initial statement is

$$\exists n \in \mathbb{N}, \forall m \in \mathbb{N}, m \leq n.$$

We can put this argument more succinctly, as follows:

$$\begin{aligned} \neg\left(\forall n \in \mathbb{N}(\exists m \in \mathbb{N}, m > n)\right) &\iff \exists n \in \mathbb{N}, \neg(\exists m \in \mathbb{N}, m > n) \\ &\iff \exists n \in \mathbb{N}, \forall m \in \mathbb{N}, \neg(m > n) \\ &\iff \exists n \in \mathbb{N}, \forall m \in \mathbb{N}, m \leq n. \end{aligned}$$

Warning 3.4. This argument is *succinct*, but it is also *hard to read*, at least for me. Just to understand what each line means requires some thought, and then some more thought to see that it actually is equivalent to the previous line. It's also *fragile* in the sense that making some tiny change could break it.

In particular, the *order of quantifiers* is important. Change them, and you probably change the meaning. If you change the order of the quantifiers in Activity 3.4, is what you get a true statement? Try writing out what it means in English.

Critical

You must be able to negate quantified statements as above, whether there are one, two or ten quantifiers. We'll get up to 4 or 5 by the end of term.
You must write quantifiers in order, before the predicate, as we do above. Otherwise you'll accidentally swap the order and change the meaning.

You want to *prove* an existential statement. That means you need to *find one example.* There is a person who has run under 10 seconds for the 100m, *because Usain Bolt did it.*

You want to *prove* a universal statement. That means you need to *check every single possibility.*
There is no person over 10 metres tall, *because (you went round the world and measured the heights of all 8 000 000 000 people).*

You want to *disprove* an existential statement. That means you need to *check every single possibility doesn't work*—in other words, prove a universal statement.

You want to *disprove* a universal statement. That means you need to *find one example where it goes wrong*—which is the same as proving an existential statement, and we normally call the bad example a *counterexample.*

How do proofs actually look that do these things? I can't help you much with proving an existential statement (yet). Sit down and think about what the object you need to find is, and hopefully at some point you can write down 'Usain Bolt' or 'Lamont Marcell Jacobs' or some other example.

But there is a standard strategy to try if you are supposed to prove a universal statement.

Critical

If the statement is 'for all $z \in \mathbb{R}$, $P(z)$' then the proof will often start 'Pick $z \in \mathbb{R}$' or 'Given $z \in \mathbb{R}$'. Then the aim is to prove $P(z)$ for this one particular z.

We will get to *using* existential and universal statements later. You are told some universal statement is true—what can you do with that information? It's best to think of that as a completely different thing to the process of *proving* existential and universal statements; again, we'll get to that later.

3.2.1 Quantifiers and arbitrary unions and intersections; empty sets

Another way of defining arbitrary union is

$$\bigcup_{i\in I} A_i = \left\{x \mid \exists i \in I,\, x \in A_i\right\},$$

and the arbitrary intersection is

$$\bigcap_{i\in I} A_i = \left\{x \mid \forall i \in I,\, x \in A_i\right\}.$$

Check that you see these definitions agree with the ones we gave earlier!

Now, what exactly do we do if I is an empty set? Well, for union it is intuitively clear: the union of no sets had better be an empty set. That's what the definition above says. If I is empty, there is no $i \in I$, so whatever the condition after '$\exists i \in I$' is is irrelevant. The statement '$\exists X \in \varnothing$, $P(x)$' is False whatever $P(x)$ is. This looks obvious written like this, but if $P(x)$ is a statement that looks 'obviously true' you will be tempted to say that '$\exists X \in \varnothing$, $P(x)$' should be True, and then you will run into trouble.

For the arbitrary intersection, it is not so clear what the right answer should be—and in fact we will avoid using this notation—but what the answer should be is that

$$\bigcap_{i\in\varnothing} A_i = E$$

where E is the universal set we're working in. Why? Well, because '$\forall x \in \varnothing$, $P(x)$' is True whatever $P(x)$ is, so by definition every x we are considering is in the arbitrary intersection of no sets. This might sound strange, and for sets it is a bit funny. But it is important in logic: and again, if $P(x)$ is some statement that looks 'obviously false' then you will be tempted to say that '$\forall x \in \varnothing$, $P(x)$' should be False and get into trouble.

Quantifiers and the empty set can be a bit confusing.

Warning 3.5. Suppose $\forall x \in X, P(x)$ is true. Is $\exists x \in X, P(x)$ true?

You probably automatically say: yes, of course it is true! Pick an x in X, then we know $P(x)$ is true (because it is true for all x in X) and this is the example that shows $\exists x \in X, P(x)$ is true.

But the answer is No!

How can that be? Well, if X is the empty set, then we cannot 'pick an x in X'. *There is nothing to pick!* The argument we gave works for *any set X which is not empty*, but it does not work when X is the empty set.

We have $\forall x \in \varnothing, P(x)$ is True whatever $P(x)$ is (even if it is some 'ridiculous' statement like 'x is a ten metre tall person'). This is because *there is nothing we need to check* in order to prove it, or if you prefer, if we try to disprove it *there is nothing in $\varnothing$ to be a counterexample.*

We have $\exists x \in \varnothing, P(x)$ is False whatever $P(x)$ is (even if it is 'x can run a 10 second 100m'), because there doesn't exist *anything* in $\varnothing$, so we never even get to the point of asking if it satisfies $P(x)$.

The name for this funny behaviour is we say a statement is *vacuously true* when it looks like $\forall x \in \varnothing, P(x)$. We might say a statement is *vacuously false* if it looks like $\exists x \in \varnothing, P(x)$, though in practice that does not show up so often.

Even though this looks like nonsense, it turns out to be useful to allow it. Let X be the set of monsters. I can prove that everything in X lives under a child's bed. And everything in X is purple. And everything in X is at least three metres tall. But child beds are less than 2 metres long, so everything that lives under a child's bed is less than 2 metres tall. So it turns out that

X is actually an empty set, because everything in X is simultaneously at least 3 metres tall and less than 2 metres tall; there are no monsters.

If we said 'you can't quantify over empty sets' then I would need to write something much more complicated than 'everything in X lives under a child's bed'. I'd need to write 'either X is empty, or everything in X lives under a child's bed'. I don't want to keep having to write something like that, and so (and only for that reason!) we allow it.

3.3 Proof by contradiction

We've seen a small example of proof by contradiction earlier in the chapter. Suppose you want to prove a statement P. One way to do this is by contradiction. What this means is that you suppose P is false, and you show that, somehow, this leads to a conclusion that you know, definitely, to be false.

Here's an example.

Example 3.6. There are no integers m, n such that $6m + 8n = 1099$.

To prove this by contradiction, we can argue as follows:

Proof. Suppose that integers m, n *do* exist such that $6m + 8n = 1099$. Then since 6 is even, $6n$ is also even; and, since 8 is even, $8n$ is even. Hence $6m + 8n$, as a sum of two even numbers, is even. But this means $1099 = 6m + 8n$ is an even number. But, in fact, 1099 is odd, so we have a contradiction. It follows that m, n of the type required do *not* exist. □

This sort of argument can be a bit perplexing when you first meet it. What's going on in the example just given? Well, what we show is that if such m, n exist, then something impossible happens: namely the number 1099 is both even and odd. Well, this can't be. If supposing something leads to a conclusion you know to be false, then the initial supposition must be false. So the conclusion is that such integers m, n do not exist.

Probably the most famous proof by contradiction is Euclid's proof that there are infinitely many prime numbers[1]. A prime number is a natural number greater than 1 which is only divisible by 1 and itself. Such numbers have been historically of huge importance in mathematics, and they are also very useful in a number of important applications, such as information security. The first few prime numbers are $2, 3, 5, 7, 11, \ldots$. A natural question is: does this list go on forever, or is there a largest prime number? In fact, the list goes on forever: there are infinitely many prime numbers. We'll mention this result again later. A full, detailed, understanding of the proof requires some results we'll meet later, but you should be able to get the flavour of it at this stage. So here it is, a very famous result:

There are infinitely many prime numbers.

Proof. (Informally written for the sake of exposition) Suppose *not*. That is, suppose there are only a finite number of primes. Then there's a largest one. Let's call it M. Now consider the number

$$X = (2 \times 3 \times 5 \times 7 \times 11 \times \cdots \times M) + 1,$$

which is the product of *all* the prime numbers (2 up to M), with 1 added. Notice that $X > M$, so X is not a prime (because M is the largest prime). If the number X is not prime, that means

[1] Historians of mathematics will probably tell you that Euclid's proof is not a proof by contradiction. Which is true, but I want to show you a proof by contradiction, so I am going to write down something which is not actually what Euclid wrote (but it's similar) and call it 'Euclid's proof'. What Euclid actually proved is 'given any finite list of prime numbers, there is a prime number not on the list' and his proof does not use contradiction.

that it has a divisor p that is a prime number and which satisfies $1 < p < X$. [*This is the key observation: we haven't really proved this yet, but we will later.*] But p must therefore be one of the numbers $2, 3, 5, \dots, M$. However, X is *not* divisible by any of these numbers, because it has remainder 1 when divided by any of them. So we have reached a contradiction: on the one hand, X must be divisible by one of these primes, and on the other, it is not. So the initial supposition that there were *not* infinitely many primes simply must be wrong. We conclude there are infinitely many primes. □

This proof has been written in a fairly informal and leisurely way to help explain what's happening. It could be written more succinctly and a bit more formally:

Proof. Suppose the set of prime numbers is not infinite. Then there are t prime numbers, for some integer t. In other words, the set of prime numbers is $\{p_1, \dots, p_t\}$. Consider the integer $N = \big(p_1 \times p_2 \times \cdots \times p_t\big) + 1$. Now N is bigger than any of $p_1, \dots, p_t$, so (by our assumption that $p_1, \dots, p_t$ are all the prime numbers) it cannot be prime. And by construction N is not divisible by any of $p_1, \dots, p_t$ (if we divide by any of them we have a remainder of 1). And since 2 and 3 are prime, certainly N is at least 7, in particular it is bigger than 1. But any integer bigger than 1 is either prime or it is divisible by a prime number, which is a contradiction. □

This proof is still missing a few things—which you can see a bit more clearly because it's written formally. Why does the first sentence imply the second? Well, we didn't formally define the word 'infinite' yet. When we do, you'll see that the second sentence is just writing out the definition of 'not infinite', also known as 'finite'. And we still didn't prove the final sentence—but hopefully it is a bit more clear what exactly we do need to prove. It's worth thinking about this a little bit now—what exactly is missing? We defined a prime number to be an integer greater than 1 which is only divisible by 1 and itself. So we need to know what to do if we are given an integer bigger than 1 which is not prime.

The other point which we should be careful about is the following. Suppose that we take the first t prime numbers, multiply them together and add one. What we just proved is that *either* we will get a new prime number *or* what we get will be divisible by a prime number which isn't one of the first t primes. We don't have any idea which of these two things will happen. If you try this for the first few values of t, you see

$$\begin{gathered} 2 + 1 = 3 \\ 2 \times 3 + 1 = 7 \\ 2 \times 3 \times 5 + 1 = 31 \\ 2 \times 3 \times 5 \times 7 + 1 = 211 \\ 2 \times 3 \times 5 \times 7 \times 11 + 1 = 2311 \end{gathered}$$

which are all prime. It's tempting to think this pattern will continue, but in fact

$$2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031 = 59 \times 509$$

is not prime.

3.4 Some terminology

At this point, it's worth introducing some important terminology. When, in Mathematics, we prove a true statement, we often say we are proving a *Theorem*, or a *Proposition.* (Usually the word 'Proposition' is used if the statement does not seem quite so significant as to merit the description 'Theorem'.) A theorem that is a preliminary result leading up to a Theorem is often called a *Lemma*, and a minor theorem that is a fairly direct consequence of, or special case of, a theorem is called a *Corollary*, if it is not significant enough itself to merit the title Theorem. For your purposes, it is important just to know that these words all mean true mathematical statements.

You should realise that these terms are used subjectively. Some authors call Euclid's result that there are infinitely many prime numbers a Theorem, others call it a Proposition. Mathematically, it doesn't make a difference; the different words are just to help the reader—to give you an idea of how hard the proof might be, or whether you should be interested in the statement for its own sake or for what you can do with it.

3.5 General advice

3.5.1 Introduction

Proving things is difficult. Yes, I already said this, but it bears repetition. So far, everything you did in mathematics was relatively easy—maybe it didn't feel that way at the time, but you probably always had the feeling that whatever problem your teachers set, you could do it. Maybe you didn't get it right first time, maybe you needed a bit more time than the teacher gave you, but would you ever be so stuck that you would spend a week trying, checking your answer, trying again... and never getting it right? Of course not.

Professional mathematicians are used to failure. If I tell a colleague I've got nowhere on some problem for a week, they will probably wonder why I'm even bothering to tell them that—that's normal; in fact months or even years is normal. If I actually managed to solve a problem in less than a week, I'd be likely to go around boasting about it!

In this course, we'll try to give you a mix of problems. Some will not be harder than the ones you did at school—these are there to check you understand the concept we just introduced. A few will be either very hard (so that while I might know how to solve them, you probably will not be able to) or even unsolved problems. These are there so that you get some experience with trying something genuinely difficult and seeing how far you can get. Most will be somewhere in the middle: harder than anything you did in school, but you can solve some or most of them, in more or less time. These are the kinds of questions that will appear on the exam—but by then you will have more experience and things you find difficult now will not be so bad any more—and so training yourself to solve questions at this level will be needed to pass the course.

Inevitably, when you read a proof, in the textbooks or in these notes, you will ask 'How did the writer know to do that?' ('magic steps') and you will often find you asking yourself 'How can I even begin to prove this?'. This is perfectly normal.

Look back to the two-line proof of Example 2.5. That proof has a 'magic step', but you know how the writer thought of it. We will meet more proofs with magic steps in this course (and I will generally try to explain why they are not really magic) and in future courses (where you might be expected to figure things out for yourself a bit more), and there will always be some reason why the step is not as magical as it seems.

We'll discuss more strategies, more things to try, more tools to use, as we go on in the course. At the same time, we'll look at more difficult problems and more complicated concepts. You may well feel the whole time that you are only barely coping with the course, and everything is almost too hard. That's what we are aiming for, more or less: to push your problem solving ability to improve as fast as possible. Every so often, look back at the problems from the first few weeks that you struggled with so that you can see how much you have moved on.

For now, the main thing to remember is: if you don't try, you will never succeed. Try something. You don't have to justify to anyone why you should start with this particular calculation, or why that theorem might help you. No-one will see your rough work. When you fail, think about why—what is missing? What else could you try? Eventually you will get there. This is a bit like integration—there are several methods, different substitutions and so forth; try one until you get there. It's more open ended in that there will be many more things to try.

One thing is vital: before you try to prove anything, you need to understand what it is that you want to prove. That no doubt sounds totally obvious—but every year, I read lots of work from students who obviously do not know what all the words in the question mean. If you do not know what a word means, you have no chance of writing a correct solution! Look up the definition. Then use the definition—there has to be a reason why that word is there!

This is particularly the case when a word has a meaning in mathematics and a meaning in normal English, and these meanings are not the same. We saw that already with 'implies', and there will be many more examples. You don't get to choose, you have to use the mathematical definition.

In general, you should expect that it takes time to read and understand even a rather short mathematical statement. Take the time, look up any words you don't know or are unsure about, check that you know the meanings of all the symbols, and put all the pieces together. As a quick example, what does $A = B$ mean? Well, that depends what A and B are. Are they numbers? vectors? sets? functions? In each of those cases, the symbol = means something different.

3.5.2 How to write mathematics

You should write mathematics **in English**. You shouldn't think that writing mathematics is just using formulae. A good way to see if your writing makes sense is by reading it aloud (where you should only read what you really have written, not adding extra words). If it sounds like nonsense, a sequence of loose statements with no obvious relations, then you need to write it again.

Don't use more symbols than necessary.

Since many people seem to think that mathematics involves writing formulae, they often use symbols to replace normal English words. An eternal favourite is the double arrow "$\Longrightarrow$" to indicate that one thing follows from the other. As in :

$$x^2 = 1 \quad\Longrightarrow\quad x = 1 \text{ or } x = -1.$$

This is not only pure laziness, since it's just as easy to write :

$$x^2 = 1, \text{ hence } x = 1 \text{ or } x = -1.$$

But it is even probably not what was meant! The implication arrow "$\Longrightarrow$" has a logical meaning "if . . . , then . . . ". So if you write "$x^2 = 1 \Longrightarrow x = 1$ or $x = -1$", then that really means "**if** $x^2 = 1$, then $x = 1$ or $x = -1$". And hence this gives no real information about what x is. On the other hand, writing

$$\text{I know } x^2 = 1, \text{ hence } x = 1 \text{ or } x = -1,$$

means that now we know $x = 1$ or $x = -1$ and can use that knowledge in what follows.

Some other unnecessary symbols that are sometimes used are "$\therefore$" and "$\because$". They mean something like "therefore/hence" and "since/because". It is best not to use them, but to write the word instead. It makes things so much easier to read.

Provide all information required.

A good habit is to start by writing what information is given and what question needs to be answered. For instance, suppose you are asked to prove the following :

Problem 3.7. *For any natural numbers a, b, c with $c \geq 2$, there is a natural number n such that $an^2 + bn + c$ is not a prime.*

A good start to an answer would be :

Given : natural numbers a, b, c, with $c \geq 2$.
To prove : there is a natural number n such that $an^2 + bn + c$ is not a prime.

At this point you (and any future reader) has all the information required, and you can start thinking what really needs to be done.

3.5.3 How to do mathematics

In a few words: **by trying** and **by doing it yourself** !!

Try hard

The kind of questions you will be dealing with in this subject often have no obvious answers. There is no standard method to come to an answer. That means that you have to find out what to do yourself. And the only way of doing that is by trial and error.

So once you know what you are asked to do (plus all the information you were given), the next thing is to take a piece of paper and start writing down some possible next steps. Some of them may look promising, so have a better look at those and see if they will help you. Hopefully, after some (or a lot) of trying, you see how to answer the question. Then you can go back to writing down the answer. This rough working is a vital part of the process of answering a question (and, in an examination, you should make sure your working is shown). Once you have completed this part of the process, you will then be in a position to write the final answer in a concise form indicating the flow of the reasoning and the arguments used.

Keep trying

You must get used to the situation that not every question can be answered immediately. Sometimes you immediately see what to do and how to do it. But other times you will realise that after a long time you haven't got any further.

Don't get frustrated when that happens. Put the problem aside, and try to do another question (or do something else). Look back at the question later or another day, and see if it makes more sense then. Often the answer will come to you as some kind of "ah-ha" flash. But you can't force these flashes. Spending more time improves the chances they happen, though.

Don't get the idea that you are looking for 'the right answer'. That might seem funny—in every mathematics class you ever took so far, you were probably told that the point of mathematics is 'to find the right answer'. This is *not true*. We would like to know which statements are true and which are false—but usually there are lots of different correct ways to prove a statement is true. They are all 'right answers'. So don't be surprised if your answer to a problem is not the same as the model solution but it is marked as correct—that just means you found a different way to solve the problem, which is fine.

If you need a long time to answer certain questions, you can consider yourself in good company. For the problem known as "Fermat's Last Theorem", the time between when the problem was first formulated and when the answer was found was about 250 years.

Finally, you should not be unhappy if you find some problems you can't solve at all. What about the following: Suppose I take the first t primes, multiply them together and add one (remember we saw this when we proved that there are infinitely many primes). We know the result is sometimes prime and sometimes not, depending on t (we saw examples of both). Are there infinitely many values of t such that we get a prime number? No-one knows the answer; that problem has been open for over 2 300 years.

Do it yourself

Here is one (of many possible) solutions to Problem 3.7:

Given: natural numbers a, b, c, with $c \geq 2$.

To prove: there is a natural number n such that $an^2 + bn + c$ is not a prime.

By definition, a natural number p is **prime** if $p \geq 2$ and the only divisors of p are 1 and p itself.

Hence to prove: there is a natural number n for which $an^2 + bn + c$ is smaller than 2 or it has divisors other than 1 or itself.

Let's take $n = c$. Then we have $an^2 + bn + c = ac^2 + bc + c$.

But we can write $ac^2 + bc + c = c\,(ac + b + 1)$, which shows that $ac^2 + bc + c$ has c and $ac + b + 1$ as divisors.

Moreover, it's easy to see that neither c nor $ac + b + 1$ can be equal to 1 or to $ac^2 + bc + c$. We've found a value of n for which $an^2 + bn + c$ has divisors other than 1 or itself.

The crucial step in the answer above is the one in which I choose to take $n = c$. Why did I choose that? Because it works. How did I get the idea to take $n = c$? Ah, that's far less obvious. Probably some rough paper and lots of trying was involved. In the final answer, no information about how this clever idea was found needs to be given.

You probably have no problems following the reasoning given above, and hence you may think that you understand this problem. But being able to follow the answer, and **being able to find the answer yourself** are two completely different matters. And it is the second skill you are suppose to acquire in this course. (And hence the skill that will be tested in the examination.) Once you have learnt how to approach questions such as the above and come up with the clever trick yourself, you have some hope of being able to answer other questions of a similar type.

But if you only study answers, you will probably never be able to find new arguments for yourself. And hence when you are given a question you've never seen before, how can you trust yourself that you have the ability to see the "trick" that that particular question requires ?

For many, abstract mathematics seems full of clever "tricks". But these tricks have always been found by people working very hard to get such a clever idea, not by people just studying other problems and the tricks found by other people.

3.5.4 How to become better in mathematics

One thing you might consider is doing more questions. The books are a good source of exercises. Trying some of these will give you extra practice.

But if you want to go beyond just being able to do what somebody else has written down, you must try to explore the material even further. Try to understand the reason for things that are maybe not explicitly asked.

As an illustration of thinking that way, look again at the formulation of the example we looked at before :

For any natural numbers a, b, c with $c \geq 2$, there is a natural number n such that $an^2 + bn + c$ is not a prime.

Why is it so important that $c \geq 2$? If you look at the proof in the previous section, you see that that proof goes wrong if $c = 1$. (Since we want to use that c is a divisor different from 1.) Does that mean the statement is wrong if $c = 1$? (No, but a different proof is required.)

And what happens if we allow one or more of a, b, c to be zero or negative?

And what about more complicated expression such as $an^3 + bn^2 + cn + d$ for some numbers a, b, c, d with $d \geq 2$? Could it be possible that there is an expression like this for which all n give prime numbers ? If you found the answer to the original question yourself, then you probably immediately see that the answer has to be "no", since similar arguments as before work. But if you didn't try the original question yourself, and just studied the ready-made answer, you'll be less well equipped to answer more general or slightly altered versions.

Once you start thinking like this, you are developing the skills required to be good in mathematics. Trying to see beyond what is asked, asking yourself new questions and seeing which you can answer, is the best way to train yourself to become a mathematician.

We've now reached the point in the course where you have all the basic tools you need to start looking at problems. There will be more concepts to introduce in the next chapters, but we will stop with introducing a new concept every page, and start spending much more time finding out what we can do.

3.6 Non-examinable: set theory—take 2

What is a set, exactly? It's supposed to be a mathematical object, which contains other mathematical objects. That sounds like a definition—why not just say that anything goes; put a bunch of objects in a bag and you have a set, which you can name (and in turn you can put it in further sets.

One of the properties we would rather like to have sets to have is that we can write things like

$$\{n \in \mathbb{N} : n \text{ is even}\}$$

and say that this too is a set. More generally, if we have some statement $P(s)$ (whose truth depends on s) and a set S, we would like to say that $\{s \in S : P(s) \text{ is true}\}$ is a set. We'll see that this kind of statement shows up continually throughout your degree programme.

Now, so far this looks fine—if 'anything goes' then certainly this is OK. But if 'anything goes', we can also ask about the set of all mathematical objects—this would also be a set, let's call it $\mathcal{U}$ for 'universe'. And we can write our favourite statement $P(s)$, for example $P(s)$ could be the statement 's is not a member of s'. In that case we get a set

$$X = \{s \in \mathcal{U} : P(s) \text{ is true}\}.$$

Now, you might notice this statement $P(s)$ is a bit funny—how can a set possibly be a member of itself? Well, actually if $\mathcal{U}$ is a set, then $\mathcal{U}$ is a mathematical object so $\mathcal{U}$ has to contain itself. That might already raise a warning sign that strange things are going to happen, but it's not actually a logical contradiction; it's just a bit funny.

But what about this set X? Well, by definition X contains everything which is not a member of itself (and nothing else). So it certainly contains anything which isn't a set (because something which isn't a set doesn't contain anything at all, let alone itself). And it certainly contains a lot of sets, like $\varnothing$ and $\{1, 2, 53\}$. OK, does X contain X? Well, if not, then by definition it should. So X must contain X. But then by definition, X cannot contain X. That's a logical contradiction, pointed out by Bertrand Russell.

That's really nothing more than a mathematical version of the 'Barber of Seville', who shaves everyone in Seville that doesn't shave themself. Who shaves the Barber?

What this logical contradiction tells us is that 'anything goes' is not OK. Some things are not sets. We need to give some rules which allow you to construct new sets from old sets; some *axioms of set theory.* This is what most mathematicians do (when we think about such things at all!), and usually we use some axioms called ZFC (Zermelo-Fraenkel with Choice). These axioms don't, for instance, allow you to construct a 'set of everything'; in fact, they don't allow any set to contain itself (because you have to construct new sets from old sets you already have). These rules don't—as far as we know—lead to logical contradictions like Russell's. If you are worried about trying to explain everything in mathematics, then a good place to start is with ZFC set theory.

However, ZFC set theory is hard work; you spend a lot of time and energy proving things which look 'obvious'. We had to make a choice: do we spend all year building up the basics of mathematics from set theory, so that you have one (hopefully) consistent foundation for the rest of your degree? Or do we want to actually do some mathematics? We chose to do the latter, which means that in this course we are going to assume some things are true without proving them. In particular, we are going to assume statements like that there is such a thing as the set of natural numbers $\mathbb{N}$, that it makes sense to talk about sets of pairs such as $\{(a, b) : a, b \in \mathbb{N}\}$, and so on. All these are things which one can prove from the ZFC axioms, but we will not do so.

If you dislike this, you should go study ZFC set theory (in the summer, when you have time!). However don't expect it to be particularly easy, and don't expect it to be an 'answer to everything'. You'll still need to assume that ZFC set theory itself makes sense; there is no proof that it makes sense.

3.7 Standard strategies: what and why

Critical

You must learn this section now, and you must aim to understand it as soon as possible. Otherwise, there is little point continuing with this course.

We will see more tools to help you prove things in the next few sections. But, you need to understand how to write down a proof, what the bits are for, and when you need to think versus when you should be able to proceed 'automatically'. I will give examples in this section, with explanations. All these examples are going to be quite simple; you can reasonably feel that I am being excessively fussy and that all the detail is unnecessary. However, I still want you to write proofs the way I say, because in a few weeks we will deal with much more complicated situations where you need to have the structure in place, otherwise you will be unable to understand my proofs or write your own. A large part of the next three weeks will be practicing with steadily more complicated setups.

The simplest statements are propositions with no variables (so no quantifiers) in them. Usually, to check these are true or false just means doing some calculation, like $2 \times 2 = 4$ is true. For the purpose of this course, you don't prove these statements, you simply state that they are true or false and we believe you actually did the calculation.

Some statements look simple but aren't really. '8 is even' is not really just a proposition. This is because, by definition, '8 is even' means 'there exists an integer k such that $8 = 2k$'. This statement has an existential quantifier in it.

Just to be clear, let's write out this statement using logical notation: '$\exists k \in \mathbb{Z}\,, 8 = 2k$'. As mentioned, the order of the symbols is important: the quantifier ($\exists k \in \mathbb{Z}$) comes first, then the predicate ($8 = 2k$) on its right.

Critical

To prove existential statements, find an example.

Proof. Let $k = 4$ which is an integer.
Then $2 \times k = 8$, so 8 is even. □

I know this is very simple, but still, let's spell out the procedure we used clearly here. First, we expanded out the statement '8 is even' to '$\exists k \in \mathbb{Z}\,, 8 = 2k$'. (It doesn't matter whether you write English text or logical notation, but if you don't know the definition you can't solve the problem.)

Then, we see that the first line of our proof will need to be 'have an idea': choose $k =$something, and 'something' had better be an integer. Well, we can write 'Let $k =$ which is an integer'. What is supposed to come after this line is the proof of the predicate to the right of the existential quantifier, which is '$8 = 2k$'. In this example, that's just a calculation, and in this example it's also obvious right now what to write to the blank $k =$, so we can do that and the proof is complete.

Now, the 'predicate to the right' might be something much more complicated than this example, which needs a proof. That doesn't mean you start the proof differently, it just means that we do something more from the second line and that we might need to write out more before we have the idea of how to fill the blank.

Finally, we need to be clear about the logic. The k in the statement we want to prove, $\exists k \in \mathbb{Z}, 8 = 2k$, is a bound variable. We can't talk about this k from 'outside' the statement. If we wanted to be very formal, we actually should not re-use the letter, our proof should be something like 'Let $\ell = 4$ which is an integer. Then $2\ell = 8$, and this example proves $\exists k \in \mathbb{Z}, 2k = 8$, so 8 is even'. However, it's annoying to be this formal; we will usually not bother picking a new letter, and we will usually not spell out that having found an example we proved the existential statement, instead we'll just write 'so' and let the reader fill in the detail in their head.

Let's now look at 'for all integers n the quantity $(2n)^2$ is even'. This statement really has two quantifiers in it (the 'even' is, as above, hiding a quantifier). We could right now expand out the definition, but let's instead deal with the 'for all' quantifier (it won't really make much difference).

Critical

To prove 'for all', check all the possibilities.

This is a difficult one. We can 'check all the possibilities' if there are a finite number of possibilities, but we obviously can't 'check all the possibilities' of $n \in \mathbb{Z}$. Here is what we do.

Proof. Given $n \in \mathbb{Z}$, we want to prove $(2n)^2$ is even.
That means, there exists $k \in \mathbb{Z}$ such that $(2n)^2 = 2k$.
We choose $k = 2n^2$, which is an integer because n is an integer. Then $2k = 4n^2 = (2n)^2$, so we are done. □

Probably the best way to view this (as mentioned earlier) is: we're describing how a Checker could 'check all the possibilities', by giving them a procedure which is supposed to work whatever n happens to be given:this is what comes after the line 'Given $n \in \mathbb{Z}$'. Here, the procedure is fairly easy: we have an existential statement to prove, so we try proving it just like any other existential statement.

However, again, we need to be clear about the logic here. The statement we start with, '$\forall n \in \mathbb{Z}, (2n)^2$ is even', is a true-or-false statement; the n is a bound variable. That means we can't talk about the n outside of it; when we start our proof, the letter n has not yet been defined. What we do on the first line is to say: we are now defining it, from this point on it has one fixed value for the rest of the proof. If this line were left out, the Checker would get to 'choose $k = 2n^2$' and say '`ERROR!` What is n?'. Again, if we were being very formal, we should probably have used a letter other than n just to avoid confusing it with the n in the statement we're trying to prove.

Once we got past the 'Given n' line, though, n is defined, it has one fixed value and that value is an integer. As the proof-writer, we don't know what that value is, but we need to remember that it is a fixed value. It is *not* somehow 'all integers at once'.

A good way to think about this is that you are writing a computer program (that the Checker runs); anyone can come to the program and input an integer n (the n that is Given) and expect to get out a reason why '$(2n)^2$ is even' is true. A proof of a 'for all' statement is the same as a computer program which is guaranteed to always output a (good) reason whatever input is given.

Because we will usually be doing 'for all' over sets which are either infinite or too big to want to write out each possibility one after another:

Critical

To prove 'for all $a \in A, \ldots$', start with 'Given $a \in A$' and then write out a procedure that explains why the predicate-to-the-right is true for this particular a.

What goes with this is 'proof by cases': you might well want to do different things depending on what you are Given. For example, 'for all integers n, the quantity $n^2 + n$ is even'.

Proof. Given $n \in \mathbb{Z}$, we ask if n is odd or even (one of these must be true).

If n is even, by definition we can write $n = 2k$ for some $k \in \mathbb{Z}$. So $n^2 + n = 4k^2 + 2k = 2(2k^2 + k)$, and since $2k^2 + k$ is an integer, $n^2 + n$ is even.

If n is odd, by definition we can write $n = 2k + 1$ for some $k \in \mathbb{Z}$. So $n^2 + n = 4k^2 + 4k + 1 + 2k + 1 = 2(2k^2 + 3k + 1)$, and since $2k^2 + 3k + 1$ is an integer, $n^2 + n$ is even. □

Again, if you're thinking of this as a computer program, the logic should be clear. If this program is Given $n = 7$, then it sees that 7 is odd, we can write it as $2 \times 3 + 1$, so $k = 3$, so it will compute $2k^2 + 3k + 1 = 28$ and so the reason it will give us is '$7^2 + 7 = 2 \times 28$'. If on the other hand it's Given $n = 10$, then the program says to do a different computation: n is even, we can write it as 2×5, so $k = 5$ and we compute $2k^2 + k = 55$ and return '$10^2 + 10 = 2 \times 55$'.

The logic of a direct 'for all' proof is *always* like this, even if the 'predicate-to-the-right' is something much more complicated so that we need some much longer procedure to output a reason. Similarly, if we are doing a proof by cases, the logic is always as above: we've two or three (or more) different proof-lets that we might do, depending on some property (like even versus odd, or zero versus positive versus negative, or whatever) of the variable we were Given. We care that (i) each of these proof-lets is actually a correct proof, and (ii) we haven't missed any cases.

Critical

After 'Given x..', if you only see how to deal with some x, (say) even x, then write that down, then think about how to deal with odd x.

Something we've done a bit already, without much comment, is 'definition chasing': when you see a definition that you have to work with, you often need to write out the definition, as it applies in your situation.

A good example of how to do this is with our use of the word 'even' above. The definition in notes is: 'the integer n is even if there exists an integer k such that $n = 2k$'. So '8 is even' means 'there exists an integer k such that $8 = 2k$' (the definition as it applies here). And 'k is even' means 'there exists an integer ℓ such that $k = 2\ell$'. Note that in the second one, we changed the letters in the definition. It wouldn't make sense to say 'there exists an integer k such that $k = 2k$'..! (That is, the statement is true, the integer that exists is 0, but this is not what it means for k to be even..!)

Critical

To work with a definition, replace the defined word or symbol with its meaning from notes. If a letter in the definition from notes is already in use, pick a new one.

This is good advice *for now*, but later in the course you might *not* want to do this: you might instead recognise that you know a theorem which you can apply without needing to write out the definition.

You should also be clear that 'definitions' can be words, but they can also be symbols, and context can be important. For example, the symbol = could appear between two numbers (you know what that means from school and we will not discuss further). It could also appear between two sets S and T, in which case it means

$$\forall x\,,\; x \in S \iff x \in T\,.$$

It could also appear between two functions, in which case the definition is different again...

Let's give an example. I'll number the lines in the following proof to make it easy to refer to.

Theorem 3.8. *For all integers p and q, if p and q are even then $p+q$ is even.*

Proof. $\forall p, q \in \mathbb{Z}, (p, q \text{ even} \implies p+q \text{ even})$

(1) Given p and q integers: $p, q \text{ even} \implies p+q \text{ even}$

(2) Case 1: p and q are both even. $p+q$ even

(3) That means there are integers k and ℓ such that $p = 2k$ and $q = 2\ell$. $\exists m \in \mathbb{Z}, p+q = 2m$

(4) Then $p+q = 2k + 2\ell = 2(k+\ell)$.

(5) Since $k+\ell$ is an integer, by definition $p+q$ is even, so the implication is true.

(6) Case 2: at least one of p and q is not even.

(7) Since the premise of the implication is false, the implication is true. □

Let's follow the use of standard strategies in getting to this proof.

(1): since we're proving a 'for all', let's be Given a pair of integers and then write out a procedure to check the predicate-to-the-right for these two specific integers. That means that our 'aim' written in red gets a bit simpler: now that k and ℓ are fixed integers, we just need to prove this implication.

(2): I don't see how to prove this predicate, which is an implication, instantly, but I have an idea that if the premise happens to be true (Case 1), then I ought to be able to prove the conclusion. So let's try that: suppose that p and q are both even. Looking at the truth-table definition of $\implies$, I have to prove the conclusion '$p+q$ is even' is true, so this is my new aim.

(3): I've written out the definition of 'even' in each of the three situations: applied to p, and to q, and (in red text in the aim) to $p+q$. And I was careful to use different letters for all three.

(4): Looking at the current aim, I want to find an integer m such that $p+q = 2m$. So let's start writing $p+q =$ and then see what I know: it turns out to be $p+q = 2k+2\ell$, and then I can see that this factorises nicely.

(5): I'm justifying that the nice equation $p+q = 2(k+\ell)$ is really finding the m in the red text 'aim'; in particular, that it's really an integer. This finishes off Case 1.

(6): I'm back to the same 'aim' as at Line 1, but at this point I can assume 'p and q are both even' is not true, because Case 1 already dealt with that situation. That means (basic logic) that at least one of p and q is not even.

(7): In this case, I notice that the premise of the implication is false, and according to the truth-table definition of $\implies$ this means the predicate we're trying to prove true, is true whatever the conclusion is. This finishes off Case 2, so we're done.

There are a couple of things to notice here. First, the only 'idea' in this proof is to factorise $2k + 2\ell = 2(k+\ell)$, so even though it's a bit long, it really isn't hard. Standard strategies do most of the work.

Second, the 'Case 2' here really has nothing much to do with the interesting statement we are trying to prove; it's something that in theory we should write every time we are proving an implication. It's tedious to really write this out every time, so instead

Critical

To prove an implication, try assuming the premise.

This leads to the following version, which is what I'd write in lectures and expect to see from you in the exam.

Proof. Given p, q integers, suppose p and q are even.
Then there are integers k and ℓ such that $p = 2k$ and $q = 2\ell$, so $p+q = 2k+2\ell = 2(k+\ell)$.
Since $k+\ell$ is an integer, by definition $p+q$ is even. □

In this use of standard strategies, we turn out to need basic logic, in particular it helps to know how to negate things. That is going to be a recurring theme.

I've also sneaked in one more standard strategy to the proof: how to *use* 'there exists'.

> Critical
>
> When you are told 'there exists', ask for an example.

In this case, you are told 'p is even' and this means that there is an example of an integer k such that $p = 2k$. If we were being very formal, we should next say 'so let k be an integer such that $p = 2k$' before using this k, but we won't be this formal; we'll take it as read that from now on in the proof k is a fixed integer and the equation $p = 2k$ is true. This is 'asking for the example'. We'll see more examples of this later, and we will see how to use 'for all' statements too; that will be our final standard strategy.

At this point, we already have one example of where 'definition chasing' might not be the right thing to do. If you are told that n is even, and you want to prove $n + 6$ is even, you should *not* start writing out the definition of 'even' as applied to n and $n + 6$, you should just note that $6 = 2 \times 3$ is even and the sum of two even numbers is (by a theorem in notes) even.

We also can see a second example of where a standard strategy might not be the right thing to try. If you can see how to prove an implication directly, 'Assume the premise. Work with it. Get to the conclusion' as we did above, great. If you can't, for example if 'Assume the premise' doesn't give you anything helpful to work with? Well, maybe try writing down the contrapositive: that is also an implication, but it might be easier to prove directly. I'll call this one a standard strategy too, because we will use it so often. Again, this works because of basic logic: the contrapositive is logically equivalent to the original implication.

> Critical
>
> To prove an implication, try writing down the contrapositive and proving that.

Something rather similar: if you don't see how to prove some statement directly (and other standard strategies don't help), you might try a proof by contradiction, such as we already saw in Section 3.3. The more you try this, the more you are likely to recognise when this strategy will help, so for now, it's always worth a try when you're stuck.

> Critical
>
> To prove a statement S, try 'Assume for a contradiction $\neg S$. Then...' and then try to get to something obviously false, like '$1 = 0$' or '1099 is both even and odd'.

The reason for listing these two standard strategies together is that to use them, you have to be capable of negating statements. S could easily be some statement with three quantifiers in it. Similarly, to write down the contrapositive of $P \implies Q$, you need to know what $\neg P$ and $\neg Q$ are. Usually, just writing the $\neg$ symbol in front of the statement will not be any help, you will need to use basic logic to get to something useful, either in the form of negating Ands and Ors, or in the form of negating quantifiers, possibly one after another. We already saw how to do this; it is a mechanical process but one you have to be able to do reliably.

This is not a methods course. Standard strategies will not usually write your proofs for you. However, getting completely comfortable with using them, and understanding why they work, is what you need to break down the exam problems to manageable pieces that you can cleverly solve, and to progress to understanding maths in later years. They separate the bits which should not be difficult from the bits that need an idea.

The habit of automatically applying these standard strategies to problems is also a large part of the 'thinking like a mathematician' that you are aiming to develop.

3.8 Sample exercises

Exercise 3.1. *Prove that for all real numbers a, b, c, $ab + ac + bc \leq a^2 + b^2 + c^2$.*

Exercise 3.2. *Prove that there is no smallest positive real number.*

Exercise 3.3. *Suppose A and B are subsets of a universal set E. Prove that*

$$(E \times E) \setminus (A \times B) = ((E \setminus A) \times E) \cup (E \times (E \setminus B)).$$

Exercise 3.4. *Suppose that $P(x, y)$ is a predicate involving two free variables x, y from a set E. (So, for given x and y, $P(x, y)$ is either true or false.) Find the negation of the statement*

$$\exists x \in E, \forall y \in E, P(x, y) .$$

3.9 Comments on selected activities

Comment on Activity 3.1. We have

$$\begin{aligned} x \in A \setminus B &\iff (x \in A) \wedge (x \notin B) \\ &\iff (x \in A) \wedge (x \in E \setminus B) \\ &\iff x \in A \cap (E \setminus B). \end{aligned}$$

Comment on Activity 3.2. $\mathcal{P}(A)$ is the set consisting of the following sets:

$$\varnothing, \{1\}, \{2\}, \{3\}, \{4\}, \{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\},$$

$$\{1,2,3\}, \{2,3,4\}, \{1,3,4\}, \{1,2,4\}, \{1,2,3,4\}.$$

Comment on Activity 3.3. The members of $\mathcal{P}(A)$ are all the subsets of A. A subset S is determined by which of the n members of A it contains. For each member x of A, either $x \in S$ or $x \notin S$. There are therefore two possibilities, for each $x \in A$. It follows that the number of subsets is $2 \times 2 \times \cdots \times 2$ (where there are n factors, one for each element of A). Therefore $\mathcal{P}(A)$ has 2^n members.

Comment on Activity 3.4. The statement means that if we take any natural number n there will be some natural number m greater than n. Well, this is true. For example, $m = n + 1$ will do.

3.10 Solutions to exercises

Solution to Exercise 3.1. We work backwards, since it is not immediately obvious how to begin. We note that what we're trying to prove is equivalent to

$$a^2 + b^2 + c^2 - ab - ac - bc \geq 0.$$

This is equivalent to

$$2a^2 + 2b^2 + 2c^2 - 2ab - 2ac - 2bc \geq 0,$$

which is the same as

$$(a^2 - 2ab + b^2) + (b^2 - 2bc + c^2) + (a^2 - 2ac + c^2) \geq 0.$$

You can perhaps now see how this is going to work, for $(a^2 - 2ab + b^2) = (a - b)^2$ and so on. Therefore the given inequality is equivalent to

$$(a - b)^2 + (b - c)^2 + (a - c)^2 \geq 0.$$

We know this to be true because squares are always non-negative. If we wanted to write this proof 'forwards' we might argue as follows. For any a, b, c, $(a-b)^2 \geq 0$, $(b-c)^2 \geq 0$ and $(a-c)^2 \geq 0$, so

$$(a - b)^2 + (b - c)^2 + (a - c)^2 \geq 0$$

and hence

$$2a^2 + 2b^2 + 2c^2 - 2ab - 2ac - 2bc \geq 0,$$

from which we obtain

$$a^2 + b^2 + c^2 \geq ab + ac + bc,$$

as required.

Solution to Exercise 3.2. We use a proof by contradiction. Suppose that there is a smallest positive real number and let's call this r. Then $r/2$ is also a real number and $r/2 > 0$ because $r > 0$. But $r/2 < r$, contradicting the fact that r is the smallest positive real number. (Or, we could argue: because $r/2$ is a positive real number and r is the smallest such number, then we must have $r/2 \geq r$, from which it follows that $1 \geq 2$, a contradiction.)

Solution to Exercise 3.3. We need to prove that

$$(E \times E) \setminus (A \times B) = ((E \setminus A) \times E) \cup (E \times (E \setminus B)).$$

Now,

$$\begin{aligned}
(x, y) \in (E \times E) \setminus (A \times B) &\iff \neg((x, y) \in A \times B) \\
&\iff \neg((x \in A) \wedge (y \in B)) \\
&\iff \neg(x \in A) \vee \neg(y \in B) \\
&\iff (x \in E \setminus A) \vee (y \in E \setminus B) \\
&\iff ((x, y) \in (E \setminus A) \times E) \vee ((x, y) \in E \times (E \setminus B)) \\
&\iff (x, y) \in ((E \setminus A) \times E) \cup (E \times (E \setminus B)).
\end{aligned}$$

Solution to Exercise 3.4. We deal first with the existential quantifier at the beginning of the statement. So, the negation of the statement is

$$\forall x \in E, \neg(\forall y \in E, P(x, y))$$

which is the same as

$$\forall x \in E, \exists y \in E,\ \neg P(x, y).$$

4 Structures, natural numbers and proof by induction

The material in this chapter is also covered in:

- Biggs, N. L. *Discrete Mathematics.* Chapter 4.
- Eccles, P.J. *An Introduction to Mathematical Reasoning.* Chapters 1–4 and 6.

4.1 Introduction

In this chapter we will discuss what is meant by a 'mathematical structure', and explore some of the properties of one of the most important mathematical structures: the natural numbers. These will not be new to you, but they shall be explained a little more formally. The chapter also studies a very powerful proof method, known as *proof by induction.* This enables us to prove many universal statements about natural numbers that would be extremely difficult to prove by other means.

4.2 Mathematical structures

A mathematical structure is a precisely specified object which one can study. We already saw, informally, several examples in the course:

(1) The natural numbers $\mathbb{N} = \{1, 2, 3, \dots\}$ which come with the operations $+$ and $\times$, and the relation $<$.

(2) The integers $\mathbb{Z}$ which come with the operations $+$ and $\times$, and the relation $<$.

(3) The rational numbers $\mathbb{Q}$ (intuitively, the fractions: numbers which you can write as $\frac{a}{b}$ where a and b are integers and b is not zero), which again come with the operations $+$ and $\times$, and the $<$ relation.

(4) The real numbers $\mathbb{R}$ (intuitively: points on the number line) which again come with the operations $+$ and $\times$, and the $<$ relation.

(5) The complex numbers $\mathbb{C}$ which are numbers of the form $a + bi$, where i is a special symbol representing $\sqrt{-1}$. Again you can add and multiply these, but you don't know any $<$ on these (and in fact, there isn't any sensible choice).

All these examples are structures where you can do arithmetic as you're used to it. Here are another couple of examples. Don't worry if you haven't seen these before. We won't try to study them just yet; they will appear in Winter Term in MA103.

(6) The ‘clock numbers’ $\mathbb{Z}_{24}$, which are the integers $\{0,1,2,\dots,23\}$ on a 24-hour clock, where you add and multiply as you would on a clock; if you get 24 you replace it with 0, if you get 25 you replace it with 1, and so on.

(7) The 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where a, b, c, d are real numbers. Here too we can define addition and multiplication:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix} \quad \text{and}$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix} .$$

These still look like structures where you can ‘do arithmetic as you’re used to it’. But you have to be a little careful now. In $\mathbb{Z}_{24}$ we have $4 \times 5 = 20 = 4 \times 11$. So what should we say $20/4$ is? You’re used to the idea that ‘division by zero’ doesn’t make sense, but in $\mathbb{Z}_{24}$ ‘division by four’ also doesn’t make sense. When you work with 2×2 matrices, then multiplication turns out not to be commutative:

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \quad \text{but} \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} .$$

Here is a rather different example.

(8) The set of social networks, where a social network consists of a (finite) collection of people and a relation ‘friends’ between pairs of people.

Think of taking a snapshot of the Facebook network at some moment: there are something like 1 000 000 000 people in the network, and if I look at any particular pair I will find they are either friends or they are not. That’s a social network (by the definition we gave); if we let some time pass, some people join or leave, some pairs of people friend or de-friend each other, we get a different social network.

It’s not clear what + or × should mean here—how can we multiply social networks? But I probably don’t have to convince you that there are interesting things to study here; and in fact the (results of the) mathematical study of networks (‘Graph Theory’) turns out to be very important in today’s technology. We’re not going to go further into this in MA103; the point of giving this example is to show you that we can be interested as mathematicians in things which don’t involve arithmetic.

More or less, any time you find a precise, unambiguous definition of something, then you have a mathematical structure which you can start studying. Mathematics is a much broader subject than the arithmetic you saw in school. **A lot of mathematics is not about numbers.** Of course, not everything interesting is mathematics—you (maybe) find politics interesting, but you will not be able to come up with a definition of ‘left-wing’ or ‘economically good’ which is generally agreed on, let alone one which is precise and unambiguous. We’ll have to leave politics to the political scientists. The flip side of this is: it’s (more or less) true that all mathematicians agree that all of mathematics is correct, which keeps fights to a minimum. That’s certainly not true for political scientists, who (sometimes) write books whose messages boil down to ‘My idea is right’, ‘You’re wrong’, ‘Am not!’, ‘Wrongy wrongy wrong!’... and so on.

If you’re thinking carefully, you might notice that the structures we mentioned above aren’t really very clearly defined. What are ‘the points on the number line’? In fact, what are ‘the natural numbers’? We probably all feel we know what is meant by a positive integer, how to add and multiply them, and that all of us will get the same answers if we try it. But that's not good enough. It would be very embarrassing if it turned out that some of us made different assumptions to others about the natural numbers, and we started arguing about what statements are true.

The way we solve this in mathematics is to be very careful with assumptions. We write down a rather short list of assumptions, called *axioms*. And then we *prove* that all the other properties of the natural numbers which you are used to follow from those few axioms. This is called the *axiomatic approach* to the natural numbers, and it is part of the Foundations of Mathematics. We will not cover it in this course.

However, what we *will* do in MA103, in Winter Term, is cover the axiomatic approach to groups and to abstract vector spaces—these are structures which you quite possibly have not yet met, and about which you have no intuition. The only way you can hope to prove anything about groups or abstract vector spaces is to get good at working with axioms.

But for now, we will stick to structures that you are familiar with, like the natural numbers. And we will not worry too much about justifying properties carefully from 'axioms', instead we will get on with some mathematics.

4.2.1 Greatest and least elements

Let S be a subset of $\mathbb{N}$. We say ℓ is a *least element* or *least member* of S if $\ell \in S$ and for all $s \in S$ we have $\ell \leq s$. Similarly, we say g is a *greatest element* or *greatest member* of S if $g \in S$ and for all $s \in S$ we have $g \geq s$.

It's obvious that some subsets of $\mathbb{N}$ do not have a greatest element—for example $\mathbb{N}$ itself doesn't have a greatest element, nor does the set of even natural numbers, nor the set of primes (this is what Euclid proved). And by definition the empty set $\varnothing$ doesn't have either a least or a greatest element: it doesn't have any elements at all.

But **every non-empty subset of $\mathbb{N}$ has a least element**. This is called the Well-Ordering Principle (or sometimes the Least Element Principle). It's a rather special property of the natural numbers, which doesn't hold for many other structures, such as the real numbers.

4.3 The principle of induction

4.3.1 Proof by induction

One particularly useful theorem that follows from the axioms of the natural numbers is the following one, known as the *Principle of Induction.* Officially, this is a theorem—a statement which we *don't* assume is true, but which we *prove.* But we will not see a proof in this course (it is not hard, but it is not a good use of your time). I will try to explain why it is *plausible* and then we will assume it is true.

The Principle of Induction: Suppose $P(n)$ is a statement involving natural numbers n. Suppose furthermore that the following two statements are true.

(i) $P(1)$ is true; (we call this the 'Base case')

(ii) For all $k \in \mathbb{N}$, $P(k) \implies P(k+1)$. (we call this the 'Induction step')

Then $P(n)$ is true for all natural numbers n.

We aren't going to prove this right now, but let's give an intuition for why it is true.

We know that $P(1)$ is true. We know that $\forall k \in \mathbb{N}$, $P(k) \implies P(k+1)$. The second of these is a bit complicated—it is saying that we have an infinite list of true statements:

$$P(1) \implies P(2) \quad \text{and} \quad P(2) \implies P(3) \quad \text{and} \quad P(3) \implies P(4) \quad \text{and so on}\,.$$

Well, we can prove $P(2)$ from this. We know $P(1)$ is true, and we know $P(1) \implies P(2)$ is true. Look at the truth table for $\implies$; the only way that that can happen is that $P(2)$ is true.

Now we can prove $P(3)$. We know (now!) that $P(2)$ is true, and we know $P(2) \implies P(3)$. Again, the only way that can happen is that $P(3)$ is true.

And so on...

That looks fairly convincing; and I said (truthfully) that this does prove $P(2)$ and $P(3)$. Why is this not in fact a proof that the Principle of Induction is true? Well, in mathematics we insist that a proof is always a *finite* argument: it has to be something you can get to the end of and check, not an infinite sequence of statements, nor something finishing with a vague 'carry on like that'.

You will probably feel that this particular 'and so on' is clear enough that you would be happy to accept this argument as valid, even though it doesn't quite fit the definition of a mathematical proof. This is a reasonable thing to say.

What is not fine, though, is saying the same thing about other similar arguments.

If you start allowing 'and so on' statements into proofs, it is easy to run into trouble. You might miss something that works fine for the first ten steps but then goes wrong, because you didn't notice it before writing 'and so on'. Your readers might guess a different pattern than you intended for 'and so on'—if I give you the sequence $1, 1, 2, 6, \ldots$ what is actually the next term? there are a few integers you could reasonably argue for. Your readers might not be able to guess at all what you meant 'and so on' to mean, because you are proving something complicated. What certainly is the case is that your mathematics will no longer be something that anyone can check and agree on; different readers might disagree on whether your proof is valid.

So we do not allow 'and so on' in proofs. If you can formulate clearly enough what you intend 'and so on' to mean, then what you will find you have written is a proof by induction.

4.3.2 An example

Here's an example of how we might prove by induction a result we proved directly earlier, in the previous chapter.

Example 4.1. Prove that

$$\forall n \in \mathbb{N}\,,\ n^2 + n \text{ is even}\,.$$

Suppose you looked at this statement for a bit, and didn't notice the 'trick' we used earlier. You would probably see what n^2+n is for a few integers first, to get some idea. $1^2+1=2$ is even. $2^2+2=6$ is even. $3^2+3=12$ is even. Then you might think, the difference between consecutive squares is always odd, and obviously the difference between consecutive integers is always odd, so the difference between consecutive values of n^2+n is always even—if I know that n^2+n is even, that tells me $(n+1)^2+(n+1)$ is even. As soon as you start thinking that it would be useful to know an earlier case to prove a later case, that generally means you want to write a proof by induction. Here it is.

Proof. Let $Q(n)$ be the statement 'n^2+n is even'.

The base case is $n=1$. The statement $Q(1)$ is '1^2+1 is even'. That is true, because $1^2+1=2$.

Fix a natural number k.

As an induction hypothesis, suppose $Q(k)$ is true, i.e. k^2+k is even.

We have $(k+1)^2+(k+1) = k^2+2k+1+k+1 = (k^2+k)+2(k+1)$. Since k^2+k is an even number by the induction hypothesis, and $2(k+1)$ is obviously even, we see that $(k+1)^2+(k+1)$ is even, which is $Q(k+1)$.

So for this k, we proved $Q(k) \implies Q(k+1)$, and since $k \in \mathbb{N}$ is arbitrary, we proved $\forall k \in \mathbb{N}\,, Q(k) \implies Q(k+1)$, the induction step.

By the Principle of Induction, we conclude that $Q(n)$ is true for all $n \in \mathbb{N}$. □

The reason why I used the letter Q rather than P is just to remind you that it's not important which particular letter we use.

Let's recap the logic here quickly. The Principle of Induction says: if you know the base case $Q(1)$ and the induction step $\forall k \in \mathbb{N}\,, Q(k) \implies Q(k+1)$ are true statements, then you also know that $\forall n \in \mathbb{N}\,, Q(n)$ (which is our goal) is a true statement. So a proof by induction will always mean proving the base case $Q(1)$ (which is usually, as here, a simple calculation), and then proving the induction step, and then saying 'so we are done by induction'.

The induction step is a complicated statement: it is a universal statement, and the thing inside the 'for all' that we want to show is itself an implication. Nevertheless, there is a standard thing to try for both of these. Since we want to prove $\forall k \in \mathbb{N}\,, Q(k) \implies Q(k+1)$, the proof of the induction step will start 'fix $k \in \mathbb{N}$' or 'given $k \in \mathbb{N}$' (these mean the same) and then we just have to prove the implication $Q(k) \implies Q(k+1)$ for this particular k, about which we are not going to assume any more (it is 'arbitrary').

There is also a standard first thing to try when we want to prove an implication: *assume* the premise $Q(k)$. We give it the name *induction hypothesis* to help the reader; to remind them that this is a standard part of the induction proof. We then just need to prove $Q(k+1)$ holds, and somewhere along the way we presumably will use the statement $Q(k)$ we assumed. I can't help you any more with this bit—this is usually the hard part of an induction proof, where you need to figure out how in fact you want to prove your implication.

4.3.3 Induction: why be careful?

At least for now, I'm going to insist that when you write a proof by induction, you really need to write it out formally as in the examples in this chapter. I want to see the words 'base case' appearing with a proof of the base case, I want to see the words 'induction step' appearing with a proof of the induction step, and then I want to see a final line like 'so by the principle of induction, ... '. You can afford to give a little less detail than the example above—see the examples below—but those features need to be present.

This is not (just) because I am picky; it is because induction is an easy thing to mess up and 'prove' something which isn't true. Furthermore, later on you may well write a long complicated proof that uses induction in two or three different places, and writing it out formally like this gives you some structure and lets you see clearly where you are using induction and when you are done.

You may get worried about why induction works—it can get confusing, when you have some complicated statement which you are trying to prove, and especially if you are using some variants of induction (see below). Keep in mind that while the predicate $P(n)$ you're working with may be complicated, the logic of induction is just the simple logic above.

You may alternatively begin to feel that induction is obvious and it's not clear why you need all the careful formalities; the examples we will see next mainly look like 'calculate the first case, then just keep doing the same calculation over and over again'. Why can't we simply write in a proof 'and now keep doing this calculation forever'? The answer is that it is easy to write down something which looks convincing, where the 'calculation you do forever' works for the first one or two times, but then it stops working because you missed some difficulty which doesn't show up in the first one or two cases. Induction is nothing more than 'and now keep doing this calculation forever', except that writing out the formalities forces you to say in detail exactly what calculation you will do and check it really works.

Finally, you need to avoid getting confused with what you have proved, when. When you are proving the induction step, you *have not* proved the $P(k)$ induction hypothesis. You've simply assumed it's true—you don't know it. When you finish proving the implication with 'so $P(k+1)$ is true' you *have not* proved $P(k+1)$, what you have proved is that *if* your induction hypothesis $P(k)$ is true, *then* so is $P(k+1)$.

There is a story which goes like this:

Johnny: I've made a diamond machine! If you give me some wood, I'll turn it into diamonds!
Frank: Sounds good.
Johnny: I am going to sell half the diamonds and buy some gold!
Frank: Sounds good.
Johnny: I'll pay a goldsmith to show me how to make a ring!
Frank: Sounds good.
Johnny: I'm going to make a diamond wedding ring!
Frank: Sounds good.
Johnny: Frankie baby, we're getting married!
Frank: Johnny... wait a minute... I'm not sure I'm ready for that...

What has happened here is that Johnny has forgotten the base of his induction. If Frank gives Johnny wood, he can make diamonds. If Johnny sells diamonds, he can buy gold, and so on. These logical implications are all fine. But they do not prove a wedding is in the waiting. Frank doesn't want to get married, so he probably will not be giving Johnny wood.

4.3.4 Variants

Sometimes you want to prove that a statement is true not for all positive integers (natural numbers) but perhaps for all non-negative integers, or all integers at least 8, or something similar. Something like induction still works, commonly called 'induction with base case N'. Here N is some particular integer, which is the smallest case you want to prove (such as 0, or 8).

The Principle of Induction with base case N: Suppose $P(n)$ is a statement involving integers $n \geq N$. Suppose furthermore that the following two statements are true.

(i) $P(N)$ is true; (the 'Base case')
(ii) For all integers $k \geq N$, $P(k) \implies P(k+1)$. (the 'Induction step')

Then $P(n)$ is true for all integers $n \geq N$.

Note that the Principle of Induction is the same thing as the Principle of Induction with base case 1. The more general statement above can be proved using the (original) Principle of Induction: this is an exercise.

Example 4.2. Prove that

$$\forall n \geq 4\,,\; n^2 \leq 2^n\,.$$

Let's notice that we *can't* prove this by the usual induction. The 'base case' $n = 1$ is true, so is the $n = 2$ case, but the $n = 3$ case is false; 3^2 is bigger than 2^3. That means that we would get stuck proving the induction step if we tried. Try to figure out the proof for yourself!

Activity 4.1. *Prove that* $\forall n \geq 4\,,\; n^2 \leq 2^n$.

Another variant of the Induction Principle is the following, known as the Strong Induction Principle:

The Strong Induction Principle: Suppose $P(n)$ is a statement involving natural numbers n. Suppose furthermore that the following statement is true.

$$\forall k \in \mathbb{N}\,,\; \big(\forall t \in \mathbb{N} \text{ such that } t < k\,,\; P(t)\big) \implies P(k)\,.$$

Then $P(n)$ is true for all natural numbers n.

It's worth taking several minutes to think about this statement. What on Earth does it mean? I don't think the string of symbols in the middle is easy to understand, and I suspect you are less happy with it than I am.

Critical

Nevertheless, the ability to make sense of a statement like this is an important skill you need to learn.

To begin understanding it, remember that the $\forall k \in \mathbb{N}$ is another way of saying 'all of the following infinite list of statements are true', where the statements in question are

$$\begin{aligned}
&\big(\forall t \in \mathbb{N} \text{ such that } t < 1\,,\; P(t)\big) \implies P(1)\\
&\big(\forall t \in \mathbb{N} \text{ such that } t < 2\,,\; P(t)\big) \implies P(2)\\
&\big(\forall t \in \mathbb{N} \text{ such that } t < 3\,,\; P(t)\big) \implies P(3)\\
&\big(\forall t \in \mathbb{N} \text{ such that } t < 4\,,\; P(t)\big) \implies P(4)\\
&\big(\forall t \in \mathbb{N} \text{ such that } t < 5\,,\; P(t)\big) \implies P(5) \quad \text{and so on.}
\end{aligned}$$

Does that help? Well, yes, a bit. We can recognise that over on the right, the conclusions of these implications are $P(1)$, $P(2)$, and so on—we're hoping to find that all those statements are true. So presumably we expect to find all the premises are true, for some reason. The premises are still complicated, so let's replace the quantifier by writing out the lists of statements explicitly. These are all finite lists of statements. In fact, on the first line we are quantifying over an empty set—there is no natural number less than 1—so for that line we need to check the definition to remember that 'for all' things in an empty set is *vacuously true.* What we get is

$$\begin{aligned} \mathsf{true} &\implies P(1) \\ P(1) &\implies P(2) \\ P(1) \wedge P(2) &\implies P(3) \\ P(1) \wedge P(2) \wedge P(3) &\implies P(4) \\ P(1) \wedge P(2) \wedge P(3) \wedge P(4) &\implies P(5) \quad \text{and so on.} \end{aligned}$$

At this point, you can start to believe that this Strong Induction Principle makes sense. The first line above is true; that tells us (check the truth table for $\implies$) that $P(1)$ is true.

But if $P(1)$ is true, the second line tells us $P(2)$ is true.

And then the third line says, since $P(1)$ and $P(2)$ are true, that $P(3)$ is true. And so on.

This 'and so on' is of course *not a proof* of the Strong Induction Principle. But we can prove it using the Principle of Induction.

Activity 4.2. *Try to understand why the Strong Induction Principle follows from the Principle of Induction. Hint: consider $Q(n)$, the statement '$\forall s \leq n,\ P(s)$ is true'.*

This is difficult, so you may want to omit this activity at first.

Here is a reformulation, less 'mathematically precise' but maybe more useful, of the Strong Induction Principle. Remember 'assuming $P(1)$ we prove $P(2)$' is the same thing as 'we prove $P(1) \implies P(2)$', and so on.

The Strong Induction Principle: Suppose $P(n)$ is a statement about natural numbers n. Suppose furthermore that you can prove $\mathsf{true} \implies P(1)$ (i.e. you can prove $P(1)$).
And, if you assume $P(1)$, you can prove $P(2)$.
In fact for every $k \in \mathbb{N}$, if you assume $P(1), P(2), \ldots, P(k-1)$ are true, you can prove $P(k)$.
Then $P(n)$ is true for all natural numbers n.

It's immediately worth pointing out that just because you *assume* $P(1), P(2), ..., P(k-1)$ when you want to prove $P(k)$ doesn't mean you have to *use* all of them in your proof. It just means you *can* if you want to.

A standard question at this point is 'what is the base case in strong induction? is it $P(1)$?' The answer to this is a bit complicated—it can be yes, it can be no, it depends. This will be easier to understand once you saw a few examples!

What is probably very unclear at this point is *when* or *why* you might want to use this complicated-looking Strong Induction. The answer, below, is simple enough, but probably it is not easy to understand until after you've read the next couple of sections.

Just as induction is what you should think of using when you try to prove a predicate $P(n)$ and think 'it would really help me if I knew the last case $P(n-1)$ was true', strong induction is what you should think of using when you try to prove $P(n)$ and think 'it would really help me if I knew one or several smaller cases were true'.

4.4 Summation formulae

Suppose $a_1, a_2, a_3, \ldots$ is a sequence (an infinite, ordered, list) of real numbers. Then the sum $\sum_{r=1}^{n} a_r$ is the sum of the first n numbers in the sequence. It is useful to define these sums 'recursively' or 'inductively', as follows:

$$\sum_{r=1}^{1} a_r = a_1 \quad \text{and} \quad \text{for } n \in \mathbb{N}, \sum_{r=1}^{n+1} a_r = \left(\sum_{r=1}^{n} a_r\right) + a_{n+1}.$$

With this observation, we can use proof by induction to prove many results about the values and properties of such sums. Here is a simple, classical, example.

Example 4.3. For all $n \in \mathbb{N}$, $\sum_{r=1}^{n} r = \frac{1}{2}n(n+1)$. This is simply the statement that the sum of the first n natural numbers is $\frac{1}{2}n(n+1)$.

Proof. We prove the result by induction. Let $P(n)$ be the statement that $\sum_{r=1}^{n} r = \frac{1}{2}n(n+1)$. Then $P(1)$ states that $1 = \frac{1}{2} \times 1 \times 2$, which is true; that is the base case.

Given $k \in \mathbb{N}$, suppose (the induction hypothesis) $\sum_{r=1}^{k} r = \frac{1}{2}k(k+1)$ is true.

Consider $\sum_{r=1}^{k+1} r$. We have

$$\begin{aligned}
\sum_{r=1}^{k+1} r &= \sum_{r=1}^{k} r + (k+1) \\
&= \tfrac{1}{2}k(k+1) + (k+1) \text{ by the induction hypothesis} \\
&= \tfrac{1}{2}(k^2 + k + 2k + 2) \\
&= \tfrac{1}{2}(k^2 + 3k + 2) \\
&= \tfrac{1}{2}(k+1)(k+2) \\
&= \tfrac{1}{2}(k+1)((k+1)+1).
\end{aligned}$$

Checking the first and last lines, what we have proved (assuming the induction hypothesis) is $P(k+1)$, i.e. we proved $P(k) \implies P(k+1)$. We did this for an arbitrary k, so we proved the induction step. By the Principle of Induction, $P(n)$ is true for all natural numbers n. □

Note how the the induction hypothesis was used. In the induction step, you always prove $P(k+1)$ to be true assuming $P(k)$ is. Unless you do so, it isn't really a proof by induction.

If you write a 'proof by induction' and notice that you never *use* the induction hypothesis in the induction step, then what you have is a *fake induction.* Cross out all the lines talking about induction, and check that what is left is still a proof. Unless you're answering a question that explicitly says 'prove by induction...', we're happier to get a direct proof than a fake induction (even though both are proofs!).

Activity 4.3. *Prove by induction that the sum of the first n terms of an arithmetic progression with first term a and common difference d (that is, the sequence a, $a+d$, $a+2d$, $a+3d$,...) is $\frac{1}{2}n(2a+(n-1)d)$.*

4.5 Recursively defined sequences

Sequences of numbers are often defined 'recursively' or 'inductively'.

Example 4.4. The sequence x_n is given by $x_1 = 9$, and $x_2 = 13$, and, for $n \geq 3$, by $x_n = 3x_{n-1} - 2x_{n-2}$. Prove that for all $n \in \mathbb{N}$ we have $x_n = 5 + 2^{n+1}$.

This will be our first proof using Strong Induction—I'll explain it after.

Proof. First, we can check that the formula works for $n = 1$ and $n = 2$, which we will call *base cases*.

We have $9 = x_1 = 5 + 2^2$. And we have $13 = x_2 = 5 + 2^3$.

Now suppose $k \geq 3$. Aim: if our formula holds for all $t < k$ then $x_k = 5 + 2^{k+1}$.

Assume, as the strong induction hypothesis, that $x_t = 5 + 2^{t+1}$ is true for each integer $t < k$.

In particular, the induction hypothesis means we assume $x_{k-2} = 5 + 2^{k-1}$, and $x_{k-1} = 5 + 2^k$.

Now by definition (since $k \geq 3$) we have

$$\begin{aligned} x_k &= 3x_{k-1} - 2x_{k-2} \\ &= 3\left(5 + 2^k\right) - 2\left(5 + 2^{k-1}\right) \\ &= 15 + 6 \times 2^{k-1} - 10 - 2 \times 2^{k-1} \\ &= 5 + 4 \times 2^{k-1} \\ &= 5 + 2^{k+1} \end{aligned}$$

which is the statement we wanted to show, so we proved the *induction step*.

By strong induction, we conclude the formula holds for all natural numbers n. □

Let's notice that we could replace 'the statement we want to show' with a defined predicate so that it looks more like Strong Induction. Then we would have written:

Proof. For each $n \in \mathbb{N}$, let $S(n)$ be the statement '$x_n = 5 + 2^{n+1}$'.

First, we can check that $S(1)$ and $S(2)$ hold, which we will call *base cases*.

We have $9 = x_1 = 5 + 2^2$. And we have $13 = x_2 = 5 + 2^3$.

Now suppose $k \geq 3$. We want to prove $\big(\forall t < k\,,\, S(t)\big) \implies S(k)$.

Assume, as the strong induction hypothesis, that $S(t)$ is true for each integer $t < k$.

In particular, the induction hypothesis means we assume $S(k-2)$ and $S(k-1)$, i.e. that $x_{k-2} = 5 + 2^{k-1}$, and $x_{k-1} = 5 + 2^k$.

Now by definition (since $k \geq 3$) we have

$$\begin{aligned} x_k &= 3x_{k-1} - 2x_{k-2} \\ &= 3\left(5 + 2^k\right) - 2\left(5 + 2^{k-1}\right) \\ &= 15 + 6 \times 2^{k-1} - 10 - 2 \times 2^{k-1} \\ &= 5 + 4 \times 2^{k-1} \\ &= 5 + 2^{k+1} \end{aligned}$$

which is $S(k)$, so we proved the *induction step*.

By strong induction, we conclude $S(n)$ holds for all natural numbers n. □

The second version looks 'more formal', but both are equally good. As long as you can write clearly, you don't need to write some predicate $P(n)$ (or $S(n)$, or whatever other letter) in an induction proof. **But** if you do write some $P(n)$, you need to **define it**. 'It's obvious from the question what that should be' isn't acceptable.

Warning 4.5. When you write a predicate, by definition that is *a true-or-false statement.* If you write 'Let $P(k) = 5 + 2^{k+1}$' then you will definitely lose marks, because on the next few lines you will write things like '7 is True' which are *nonsense*. In general, any time you write $P(n) = ..$ where $P(n)$ is supposed to be a predicate, the = sign has instantly lost you marks. We *never* write that a logical statement is = something. (You can use the symbol $\iff$, but usually it is better to use words.)

Let's check that we really are using Strong Induction correctly here. When we say 'by Strong Induction' we're claiming that we proved each of the implications that we have to prove.

We proved $\mathsf{true} \implies S(1)$ by proving $S(1)$ directly. And we proved $S(1) \implies S(2)$ by proving $S(2)$ directly.

And for each $k \geq 3$, we proved $S(1) \wedge S(2) \wedge \cdots \wedge S(k-1) \implies S(k)$ in the 'induction step'. So, yes, we did prove all the statements we were supposed to.

This also explains why we called $S(1)$ and $S(2)$ 'base cases' and the rest 'the induction step'. We did something special and different to prove those first two cases, which didn't use any induction hypothesis. To help the reader (who might expect us to have used $S(1)$ to prove $S(2)$!) we call it a base case; that's just telling the reader 'this case will be special'. And for the rest of the cases, we used one argument that deals with all of them (and it *does* assume some smaller cases are true) so we call it 'the induction step'.

We'll see later examples of strong induction arguments with one base case, or two, or three—or even sometimes with no base case at all. The base cases are just the cases you find you need to handle separately because the 'main argument' doesn't work for them. In the example above, in the 'main argument' we used the recursion formula $x_k = x_{k-1} + x_{k-2}$. We were only told that that formula makes sense if $k \geq 3$, so the 'main argument' can't handle $k = 1$ or $k = 2$. You can find out what base cases you need by reading over the induction step, once you figure it out, and checking whether it really works for all values of k (if so, no base cases) or if there are a few small values of k for which it doesn't work (these are the base cases, make sure you write a proof separately for each of them).

4.6 Sample exercises

Exercise 4.1. *Prove by induction that, for all* $n \in \mathbb{N}$, $2^n \geq n + 1$.

Exercise 4.2. *Prove by induction that the sum* $a + ar + ar^2 + \cdots + ar^{n-1}$ *of the first* n *terms of a geometric progression with first term* a *and common ratio* $r \neq 1$ *is* $a(1 - r^n)/(1 - r)$.

Exercise 4.3. *Prove by induction that for all* $n \in \mathbb{N}$,

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

Exercise 4.4. *Prove by induction that* $\displaystyle\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}$.

Exercise 4.5. *Suppose the sequence* x_n *is given by* $x_1 = 7$, $x_2 = 23$ *and, for* $n \geq 3$, $x_n = 5x_{n-1} - 6x_{n-2}$. *Prove by induction that, for all* $n \in \mathbb{N}$, $x_n = 3^{n+1} - 2^n$.

Exercise 4.6. *Prove by induction that, for all* $n \in \mathbb{N}$, $2^{n+2} + 3^{2n+1}$ *is divisible by* 7.

Exercise 4.7. *For a sequence of numbers* $x_1, x_2, x_3, \ldots$, *and for* $n \in \mathbb{N}$, *the number* $\prod_{r=1}^{n} x_r$ *is the product of the first* r *numbers of the sequence. It can be defined inductively as follows:*

$$\prod_{r=1}^{1} x_r = x_1, \quad \textit{and} \ \text{ for } k \geq 1, \prod_{r=1}^{k+1} x_r = \left(\prod_{r=1}^{k} x_r\right) x_{k+1}.$$

Suppose that $x \neq 1$. Prove that

$$\prod_{r=1}^{n}(1 + x^{2^{r-1}}) = \frac{1 - x^{2^n}}{1 - x}.$$

4.7 Comments on selected activities

Comment on Activity 4.1. When $n = 4$, $n^2 = 16$ and $2^n = 2^4 = 16$, so in this base case, the statement is true. Suppose we make the inductive hypothesis that for some $k \geq 4$, $k^2 \leq 2^k$. We want to show

$$(k + 1)^2 \leq 2^{k+1}.$$

We have

$$(k + 1)^2 = k^2 + 2k + 1 \leq 2^k + 2k + 1$$

(by the inductive hypothesis). So we'll be done if we can show that $2k + 1 \leq 2^k$. This will follow from $2k + 1 \leq k^2$ and the assumed fact that $k^2 \leq 2^k$. Now,

$$2k + 1 \leq k^2 \iff k^2 - 2k - 1 \geq 0 \iff (k - 1)^2 \geq 2,$$

which is true for $k \geq 4$. So, finally,

$$(k + 1)^2 \leq 2^k + 2k + 1 \leq 2^k + k^2 \leq 2^k + 2^k = 2^{k+1}.$$

as required. So the result is true for all $n \geq 4$.

Comment on Activity 4.2. Let $Q(n)$ be the statement '$\forall s \leq n$, $P(s)$ is true'. Then $Q(1)$ is true if and only if $P(1)$ is true. The statement $Q(k) \implies Q(k + 1)$ is the same as

$$(P(s) \text{ true } \forall s \leq k) \implies (P(s) \text{ true } \forall s \leq k + 1).$$

But if $P(s)$ is true for all $s \leq k$ then its truth for all $s \leq k + 1$ follows just from its truth when $s = k + 1$. That is, $Q(k) \implies Q(k + 1)$ is the same as $(P(s) \text{ true } \forall s \leq k) \implies P(k + 1)$. The (standard) Induction Principle applied to the statement $Q(n)$ tells us that: $Q(n)$ is true for all $n \in \mathbb{N}$ if the following two statements are true:

(i) $Q(1)$ is true;

(ii) For all $k \in \mathbb{N}$, $Q(k) \implies Q(k + 1)$.

What we've established is that (i) and (ii) can be rewritten as:

(i) $P(1)$ is true;

(ii) For all $k \in \mathbb{N}$, $(P(s) \text{ true } \forall s \leq k) \implies P(k + 1)$.

We deduce that: $P(n)$ is true for all $n \in \mathbb{N}$ if the following two statements are true:

(i) $P(1)$ is true;

(ii) For all $k \in \mathbb{N}$, $(P(s) \text{ true } \forall s \leq k) \implies P(k + 1)$.

This is exactly the Strong Induction Principle. So the Strong Induction Principle follows from the standard one and is, therefore, not really 'stronger'.

Comment on Activity 4.3. Let $P(n)$ be the statement that the sum of the first n terms is $(n/2)(2a+(n-1)d)$. The base case is straightforward. The first term is a, and the formula $(n/2)(2a+(n-1)d)$ gives a when $n=1$. Suppose that $P(k)$ holds, so the sum of the first k terms is $(k/2)(2a+(k-1)d)$. Now, the $(k+1)$st term is $a+kd$, so the sum of the first $k+1$ terms is therefore

$$\begin{aligned} a+kd+\frac{k}{2}(2a+(k-1)d) &= a+kd+ak+\frac{k(k-1)}{2}d \\ &= (k+1)a+\frac{k(k+1)}{2}d \\ &= \frac{(k+1)}{2}(2a+kd) \\ &= \frac{(k+1)}{2}(2a+((k+1)-1)d), \end{aligned}$$

so $P(k+1)$ is true. The result follows for all n by induction.

4.8 Solutions to exercises

Solution to Exercise 4.1. Let $P(n)$ be the statement '$2^n \geq n+1$'. When $n=1$, $2^n=2$ and $n+1=2$, so $P(1)$ is true. Suppose $P(k)$ is true for some $k \in \mathbb{N}$. Then $2^k \geq k+1$. It follows that

$$2^{k+1} = 2.2^k \geq 2(k+1) = 2k+2 \geq k+2 = (k+1)+1,$$

so $P(k+1)$ is also true. Hence, by induction, for all $n \in \mathbb{N}$, $2^n \geq n+1$.

Solution to Exercise 4.2. Let $P(n)$ be the statement that the sum of the first n terms is $a(1-r^n)/(1-r)$. $P(1)$ states that the first term is $a(1-r^1)/(1-r)=a$, which is true. Suppose $P(k)$ is true. Then the sum of the first $k+1$ terms is the sum of the first k plus the $(k+1)$st term, which is ar^k, so this sum is

$$\begin{aligned} \frac{a(1-r^k)}{1-r}+ar^k &= \frac{a(1-r^k)+(1-r)ar^k}{1-r} \\ &= \frac{a-ar^k+ar^k-ar^{k+1}}{1-r} \\ &= \frac{a(1-r^{k+1})}{1-r}, \end{aligned}$$

which shows that $P(k+1)$ is true. Hence, for all $n \in \mathbb{N}$, $P(n)$ is true, by induction.

Solution to Exercise 4.3. Let $P(n)$ be the statement that

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

Then $P(1)$ states that $1 = 1(2)(3)/6$, which is true. Suppose $P(k)$ is true for $k \in \mathbb{N}$. Then

$$\sum_{r=1}^{k} r^2 = \frac{1}{6}k(k+1)(2k+1)$$

and $P(k+1)$ is the statement that

$$\sum_{r=1}^{k+1} r^2 = \frac{1}{6}(k+1)(k+2)(2(k+1)+1) = \frac{1}{6}(k+1)(k+2)(2k+3).$$

We have

$$\begin{aligned}
\sum_{r=1}^{k+1} r^2 &= (k+1)^2 + \sum_{r=1}^{k} r^2 \\
&= (k+1)^2 + \frac{1}{6}k(k+1)(2k+1) \quad \text{(by the induction hypothesis)} \\
&= \frac{1}{6}(k+1)\left[6(k+1) + k(2k+1)\right] \\
&= \frac{1}{6}(k+1)\left(2k^2 + 7k + 6\right) \\
&= \frac{1}{6}(k+1)(k+2)(2k+3),
\end{aligned}$$

so $P(k+1)$ is true. By induction, $P(n)$ is true for all $n \in \mathbb{N}$.

Solution to Exercise 4.4. Let $P(n)$ be the statement that $\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}$. Then $P(1)$ states that $\frac{1}{1 \times 2} = \frac{1}{1+1}$, which is true. Suppose $P(k)$ is true for $k \in \mathbb{N}$. Then

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

and $P(k+1)$ is the statement that

$$\sum_{i=1}^{k+1} \frac{1}{i(i+1)} = \frac{k+1}{k+2}.$$

Now,

$$\begin{aligned}
\sum_{i=1}^{k+1} \frac{1}{i(i+1)} &= \frac{1}{(k+1)(k+2)} + \sum_{i=1}^{k} \frac{1}{i(i+1)} \\
&= \frac{1}{(k+1)(k+2)} + \frac{k}{k+1} \quad \text{(by the induction hypothesis)} \\
&= \frac{1 + k(k+2)}{(k+1)(k+2)} \\
&= \frac{k^2 + 2k + 1}{(k+1)(k+2)} \\
&= \frac{(k+1)^2}{(k+1)(k+2)} \\
&= \frac{k+1}{k+2},
\end{aligned}$$

so $P(k+1)$ is true. By induction, $P(n)$ is true for all $n \in \mathbb{N}$.

Solution to Exercise 4.5. Let $P(n)$ be the statement that $x_n = 3^{n+1} - 2^n$. We use the Strong Induction Principle to prove $P(n)$ is true for all $n \in \mathbb{N}$. The base cases are $n = 1$ and $n = 2$. When $n = 1$, $x_1 = 7$ and $3^{n+1} - 2^n = 9 - 2 = 7$. When $n = 2$, $x_2 = 23$ and $3^{n+1} - 2^n = 27 - 4 = 23$, so these are true. Suppose that $k \geq 2$ and that for all $s \leq k$, $P(s)$ is true. In particular, $P(k)$ and

$P(k-1)$ are true and so

$$\begin{aligned}
x_{k+1} &= 5x_k - 6x_{k-1} \\
&= 5(3^{k+1} - 2^k) - 6(3^k - 2^{k-1}) \\
&= 5(3^{k+1}) - 5(2^k) - 6(3^k) + 6(2^{k-1}) \\
&= 15(3^k) - 6(3^k) - 10(2^{k-1}) + 6(2^{k-1}) \\
&= 9(3^k) - 4(2^{k-1}) \\
&= 3^{k+2} - 2^{k+1} \\
&= 3^{(k+1)+1} - 2^{k+1},
\end{aligned}$$

so $P(k+1)$ is true. Therefore, $P(n)$ is true for all $n \in \mathbb{N}$.

Solution to Exercise 4.6. Let $P(n)$ be the statement that $2^{n+2} + 3^{2n+1}$ is divisible by 7. When $n = 1$, $2^{n+2} + 3^{2n+1} = 8 + 27 = 35$ and this is a multiple of 7 because $35 = 5 \times 7$. Suppose $P(k)$ is true, which means that for some $m \in \mathbb{N}$, $2^{k+2} + 3^{2k+1} = 7m$. Now, when we take $n = k+1$,

$$\begin{aligned}
2^{n+2} + 3^{2n+1} &= 2^{k+3} + 3^{2k+3} \\
&= 2(2^{k+2}) + 9(3^{2k+1}) \\
&= 2(2^{k+2} + 3^{2k+1}) + 7(3^{2k+1}) \\
&= 14m + 7(3^{2k+1}) \\
&= 7\left(2m + 3^{2k+1}\right),
\end{aligned}$$

which is a multiple of 7. So the statement is true for $P(k+1)$. This proves $P(k) \implies P(k+1)$, the induction step, and hence, by induction, for all $n \in \mathbb{N}$.

Solution to Exercise 4.7. Let $P(n)$ be the statement

$$\prod_{r=1}^{n}(1 + x^{2^{r-1}}) = \frac{1 - x^{2^n}}{1 - x}.$$

When $n = 1$, the left hand side is $1 + x^{2^0} = 1 + x$ and the right hand side is $(1 - x^2)/(1 - x) = 1 + x$, so $P(1)$ is true. Suppose $P(k)$ is true, so that

$$\prod_{r=1}^{k}(1 + x^{2^{r-1}}) = \frac{1 - x^{2^k}}{1 - x}.$$

Then

$$\begin{aligned}
\prod_{r=1}^{k+1}(1 + x^{2^{r-1}}) &= (1 + x^{2^{(k+1)-1}}) \times \prod_{r=1}^{k}(1 + x^{2^{r-1}}) \\
&= (1 + x^{2^k})\frac{1 - x^{2^k}}{1 - x} \quad \text{(by the induction hypothesis)} \\
&= \frac{1 - (x^{2^k})^2}{1 - x} \quad \text{(where we've used } (1+y)(1-y) = 1 - y^2\text{)} \\
&= \frac{1 - x^{2^k \times 2}}{1 - x} \\
&= \frac{1 - x^{2^{k+1}}}{1 - x},
\end{aligned}$$

which shows that $P(k+1)$ is true. So $P(n)$ is true for all $n \in \mathbb{N}$, by induction.

5 Functions and counting

The material in this chapter is also covered in:

- Biggs, N. L. *Discrete Mathematics.* Chapters 5 and 6.
- Eccles, P.J. *An Introduction to Mathematical Reasoning.* Chapter 10, Sections 10.1 and 10.2, and Chapter 11.

5.1 Introduction

In this chapter we look at the theory of functions, and we see how the idea of the 'size' of a set can be formalised.

5.2 Functions

5.2.1 Basic definitions

You have worked extensively with functions in your previous mathematical study. Chiefly, you will have worked with functions from the real numbers to the real numbers, these being the primary objects of interest in calculus.

You are probably used to writing a function down by writing a formula, something like '$f(x) = x^2 + \sin x$'. This is *not* the approach we are going to take, because it's too restrictive. For a very simple example, take the function $g(x)$ which is defined as follows:

$$g(x) = \begin{cases} 0 & \text{if } x \leq 11850\,, \\ \frac{1}{5}(x - 11850) & \text{if } 11850 < x \leq 46350 \text{ and} \\ \frac{2}{5}(x - 46350) + 6900 & \text{if } x > 46350\,. \end{cases}$$

This is a perfectly good function, but finding a single formula for it is a bit tricky. Furthermore, once you find it you'll notice that the formula is much less helpful than the definition above.[1]

Activity 5.1. *Find a single formula which gives the function $g(x)$ above.*

[1] This function was actually an important function (at least in the UK): $g(x)$ is the (in 2018) income tax you pay on income £x. Last year I didn't update it because Liz Truss didn't seem too clear what she wanted to change it to, and this year I am too lazy.

So we do not want to think of 'function' as meaning 'defined by a formula'. In fact, we don't want to think about how to go from the input x to the output $f(x)$ at all—we will think of a function as a 'black box' which takes in a number and spits out a number; the only rule is that we insist that it always spits out the same number.

Actually, even that is too restrictive; we don't want to insist that the input or output is a number. Maybe we would like the input or output to be 'Yes', or 'No', or a colour, or a social network... we need a definition which allows any of these possibilities. The only thing we want to stick to is: if we give the function the same input twice, we should get the same output each time. Here is the definition which formalises this.

Definition 5.1. Suppose that X and Y are sets. Then a *function* (also known as a *mapping*) from X to Y is a rule that associates a unique member of Y to each member of X. We write $f : X \to Y$. The set X is called the *domain* of f and Y is called the *codomain*.

The element of Y that is assigned to $x \in X$ is denoted by $f(x)$ and is called the *image* of x. We can write $x \mapsto f(x)$ to indicate that x maps to $f(x)$.

There are lots of examples of functions you already know, such as $\sin x$, or $g(x)$ defined above.

If you have a social network, then that social network contains a number of friendships (i.e. pairs of people who are friends); that defines a function from social networks to the integers, which given a social network returns the total number of friendships.

If you have a road map of some country, then there may or there may not be a way to drive through all the villages without ever having to return to a village you already visited. That defines a function from road maps to $\{\text{Yes}, \text{No}\}$.

You can also generate your own personal function as follows. Throw a die 1 000 000 times, and write down the numbers in order that you get—that defines you a function from $\{1, \dots, 1\,000\,000\}$ to $\{1, \dots, 6\}$. (It's extremely unlikely anyone ever wrote down your personal function before. Of course, the next time you try this you are very likely to get a different function..!)

Some of these functions are easier to work with, or more interesting, than others. You know $\sin x$ shows up a lot in real-world calculations (in engineering, for example), and you know how to do algebra and calculus with it.

What about the road map function? If you're a fraudster, you need to keep moving on, and you probably care a lot about not going back to villages where you already conned people—but how do you actually work out, for a given road map with maybe 50 000 villages, whether the answer is 'Yes' or 'No'? It's an interesting function, but it's very hard to work with.

Finally, what about one of these generated-by-dice functions? It's not easy to describe—you don't want to read a list a million characters long—and it's not clear what it should be useful for. Often (but certainly not all the time), we are really only interested in functions which we can describe in some useful way.

There are various ways of describing a function.

- If X has only finitely many members, we can simply list the images of the members of X.
- You're used to seeing a function defined by giving a formula for the function. For instance, $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = 2x$ is the function that maps each real number a to the real number $2a$.
- Sometimes a function can be defined *recursively*. For example, we might define $f : \mathbb{N} \to \mathbb{N}$ by

$$f(1) = 1 \text{ and } f(n) = 2 + 3f(n-1), \text{ for } n \geq 2\,.$$

- We might also define a function by writing down some properties it has. For example, I could say 'let $h : \mathbb{R} \to \mathbb{R}$ be the function such that $h(0) = 1$ and $\frac{\mathrm{d}h(x)}{\mathrm{d}x} = h(x)$ holds for all $x \in \mathbb{R}$.' You probably recognise from school that $h(x) = e^x$ is the exponential function. Here, we really need to be careful: am I actually defining a function? In this case, yes: there is exactly one function that satisfies the properties I wrote down. But if I left out the condition $h(0) = 1$ then I would be writing something *not well-defined*, i.e. something that looks like it's defining a function but in fact isn't. The reason is there would be many possible valid answers, such as $h(x) = 2024e^x$.

Finally, we define one very basic function. For any set X, the *identity* function $\mathbb{1} : X \to X$ is given by $\mathbb{1}(x) = x$.

5.2.2 Function equality

What does it mean to say that two functions f and g are equal? Well, first, they must have the same domain X and codomain Y. Then, for each $x \in X$, we must have $f(x) = g(x)$. For example, if $\mathbb{R}^+$ is the set of positive real numbers, then the function $f : \mathbb{R}^+ \to \mathbb{R}$ given by $f(x) = x^2$ and the function $g : \mathbb{R} \to \mathbb{R}$ given by $g(x) = x^2$ are *not* equal because their domains are different.

You might think it is picky to say that, for example, the function $f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ defined by $f(x) = x^2$ and the function $g : \mathbb{R}_{\geq 0} \to \mathbb{R}$ defined by $g(x) = x^2$ are different (The set $\mathbb{R}_{\geq 0}$ is the non-negative real numbers). After all, what you can put into both functions is the same, and what comes out is also the same—the only difference is that the codomains of f and g are different. However, it turns out often to be important what the codomain is—for example, we'll see later that only one of f and g is a 'bijection'.

To repeat from a previous chapter—we've just met *another* definition of the symbol =. When we write $f = g$, and f and g are functions, we mean:
the domains of f and g are equal (as sets),
the codomains of f and g are equal (as sets), and
$f(x) = g(x)$ is true for all x in the domain of f (which is the same as the domain of g).

What do we mean by $f(x) = g(x)$? Well, if the codomains of f and g are numbers, we mean equality of numbers. If they are sets, we mean equality of sets. If they are functions (yes, the output of a function could actually be a function..!) then it means equality as we just defined it of functions; and there are more things that $f(x)$ and $g(x)$ could be.

5.2.3 Composition of functions

Suppose that X, Y, Z are sets and that $f : X \to Y$ and $g : Y \to Z$. Then the *composition* $g \circ f$ is the function from X to Z given by

$$(g \circ f)(x) = g\big(f(x)\big) \quad \text{for} \quad x \in X\,.$$

If X and Z are distinct sets, there is only one way we can compose f and g.

If $X = Z$, then both $f \circ g$ and $g \circ f$ make sense—but they are generally *not* the same function: the order is important.

In some textbooks you will see a different notation for function composition, leaving out the $\circ$. So you might see fg where I would write $f \circ g$. This notation fg can cause confusion (which is why I won't use it). For example, suppose $X = Y = Z = \mathbb{R}$. Then you might be tempted to think that gf denotes the *product* function $x \to g(x)f(x)$. But this would be wrong. The notation $g \circ f$ avoids this confusion.

Example 5.2. Suppose $f : \mathbb{N} \to \mathbb{N}$ and $g : \mathbb{N} \to \mathbb{N}$ are given by $f(x) = x^2 + 1$ and $g(x) = (x+1)^2$.

$$\begin{aligned}
\text{Then}\quad & (f \circ g)(x) = f\big(g(x)\big) = f\big((x+1)^2\big) = \big((x+1)^2\big)^2 + 1 = (x+1)^4 + 1\,,\\
\text{while}\quad & (g \circ f)(x) = g\big(f(x)\big) = g\big(x^2+1\big) = \big((x^2+1)+1\big)^2 = (x^2+2)^2\,,\\
\text{and}\quad & g(x)f(x) = (x+1)^2(x^2+1)\,.
\end{aligned}$$

All three are different.

5.3 Bijections, surjections and injections

There are three very important properties that a function might possess:

Definition 5.3 (Surjection)**.** Suppose f is a function with domain X and codomain Y. Then f is said to be a *surjection* (or '*f is surjective*') if every $y \in Y$ is the image of some $x \in X$; that is, f is a surjection if and only if $\forall y \in Y, \exists x \in X, \text{s.t. } f(x) = y$.

Definition 5.4 (Injection)**.** Suppose f is a function with domain X and codomain Y. Then f is said to be an *injection* (or '*f is injective*') if every $y \in Y$ is the image of *at most one* $x \in X$. In other words, the function is an injection if different elements of X have different images under f. Thus, f is an injection if and only if

$$\forall x, x' \in X, x \neq x' \implies f(x) \neq f(x')$$

or (equivalently, taking the contrapositive), if and only if

$$\forall x, x' \in X, f(x) = f(x') \implies x = x'.$$

This latter characterisation often provides the easiest way to verify that a function is an injection.

Definition 5.5 (Bijection)**.** Suppose f is a function with domain X and codomain Y. Then f is said to be a *bijection* (or '*f is bijective*) if it is *both* an injection and a surjection. So this means two things: each $y \in Y$ is the image of some $x \in X$, and each $y \in Y$ is the image of no more than one $x \in X$. Well, of course, this is equivalent to: each $y \in Y$ is the image of *precisely one* $x \in X$.

Example 5.6. $f : \mathbb{N} \to \mathbb{N}$ given by $f(x) = 2x$ is not a surjection, because there is no $n \in \mathbb{N}$ such that $f(n) = 1$. (For, $2n = 1$ has no solution where $n \in \mathbb{N}$.) However, it is an injection. To prove this, suppose that $m, n \in \mathbb{N}$ and $f(m) = f(n)$. Then $2m = 2n$, which implies $m = n$.

Activity 5.2. *Prove that $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = 2x$ is a bijection.*

We write (a,b) (which is called an *open interval* and we will meet again later) for the set of real numbers x such that $a < x < b$. And we write $|x|$ for the *absolute value* of x, defined by $|x| = x$ if $x \geq 0$ and $|x| = -x$ if $x < 0$. Thus $|x|$ is always non-negative.

Example 5.7. The function $f : \mathbb{R} \to (-1,1)$ given by $f(x) = \frac{x}{1+|x|}$ is a bijection.

Proof. First, we prove f is **injective.** Given $x, y \in \mathbb{R}$, we need to prove that $f(x) = f(y)$ implies $x = y$. So, suppose $f(x) = f(y)$. Then

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

Rearranging, we want to solve $x + x|y| = y + y|x|$.
Suppose $x \geq 0$. If $y < 0$, then the left hand side of the above equation is non-negative and the right hand side is negative—this cannot be a solution. So $y \geq 0$. But then $|x| = x$ and $|y| = y$, and we get $x + xy = y + xy$, which tells us $x = y$.
Suppose $x < 0$. If $y \geq 0$, then the left hand side of the above equation is negative and the right hand side is non-negative—this cannot be a solution. So $y < 0$. Then $|x| = -x$ and $|y| = -y$, we get $x - xy = y - xy$ and again $x = y$.

Next, we show f is **surjective.** Given $y \in (-1,1)$, we need to prove that there is some $x \in \mathbb{R}$ such that $\frac{x}{1+|x|} = y$.
Suppose $y \geq 0$. Then, to have $\frac{x}{1+|x|} = y$, we need $x \geq 0$. So $|x| = x$ and we need to solve $\frac{x}{1+x} = y$. This has solution $x = \frac{y}{1-y}$, which is well-defined and non-negative because we know $0 \leq y < 1$.
Suppose $y < 0$. Then we'll need to have $x < 0$ and the equation to solve is $\frac{x}{1-x} = y$, for a solution $x = \frac{y}{1+y}$; this is well-defined and negative since $0 > y > -1$.

Since we showed f is injective and surjective, by definition it is bijective. □

At first, you might well think that the above proof is difficult; it's certainly not short, and has a bunch of somewhat complicated formulae and cases to consider.

But actually, this proof is *long, but not hard.* We will see quite a few proofs which are long, but not hard, in this course. This is one of the standard places where students are put off the course (and maybe mathematics as a whole), because they feel that how difficult it will be to find a proof has to be proportional to the length of the proof, and the proofs are getting rapidly longer.

There will certainly be difficult proofs in the course. But proof difficulty doesn't have much to do with length. In this case, most of the proof is generated by applying standard strategies, and what's left over to deal with once you run out of standard strategies turns out to be easy.

To begin with, we're supposed to prove a function is bijective. That means (definition chasing) we need to prove it is injective and surjective (because that's what 'bijective' means). Well, if we want to prove two things, we should probably do them one after the other. So we do that (and unsurprisingly, if we prove two things it will be twice as long).

Next, we look up the definition of 'f is injective' in order to prove it. We take the hint from the lecture notes to use the contrapositive form: we should (definition chasing) try to prove that for all $x, y \in \mathbb{R}$ we have $f(x) = f(y) \implies x = y$. Well, this is a 'for all' statement, so we use the standard first thing to try: fix x and y, and try to prove the statement for this particular x and y. We write in the definition of $f(x)$ and $f(y)$ (definition chasing, again) and hope to get some nice equation that we can hit with algebra and solve. What we get is $x + x|y| = y + y|x|$.

This isn't quite a nice equation, because of the $|\cdot|$ signs; we would be much happier if we could get rid of them. How can we do that? Well, we can get rid of $|x|$ by definition chasing (again!): let's think about the cases $x \geq 0$ (which is when $|x| = x$) and $x < 0$ (so $|x| = -x$) separately. That case distinction in the proof is *not* magic, it was copied straight from the definition of $|x|$.

We still have a nasty $|y|$ around. Let's repeat the definition chasing: in each of our two cases for x, let's separately consider whether $y \geq 0$ or $y < 0$ (so we have four cases in total).

At this point, we need to think for a couple of seconds to notice that two of our four cases can't really happen: if $x \geq 0$ and $y < 0$ (or vice versa) then we don't need to start doing algebra because there can't be a solution.

What would happen if you *did* just start doing algebra here? Well, you'd try to solve $x - xy = y + xy$ (plugging in $|x| = x$ and $|y| = -y$) and so $x = y + 2xy$, so $y = \frac{x}{1+2x}$. Then you need to notice that since $x \geq 0$, the 'solution' you've just found gives us $y \geq 0$, whereas we assumed $y < 0$. So it's not really a solution; it violates the assumption we made.

And then we do just do the algebra in the two remaining cases, and in both cases it is easy.

Now we move to 'f is surjective'. Again, we definition-chase, and write out what that means. Again, we need to deal with the $|x|$ and again the right thing to do is to separate the two cases (since we are *given* y and want to *find* x such that $f(x) = y$, it makes sense to consider the two possible cases for y). And again, we can then do the algebra and double-check our solution makes sense.

Because there were a lot of steps in this proof, you have *no chance* of looking at the problem and seeing how the proof will go; it's easy to get scared and skip the question.

But if you simply *try*, you can write the proof down without ever having to pause for thought for more than a minute (if you're revising, you're probably at the stage where it takes longer to write the next line than to think what it should be). Whenever we had some not-so-nice concept left over, we used definition chasing to replace it with something nicer (even when that means considering cases, this is a winner: two nice things is better than one not-so-nice thing). Until we finally got down to a problem you know how to do from high school 'solve this nice equation'.

That is 'long but not hard'; get used to it. Don't get scared until standard strategies *don't* help.

5.4 Inverse functions

5.4.1 Definition, and existence

Suppose we are given a function $f : X \to Y$. Then $g : Y \to X$ is an *inverse function* of f if for all $x \in X$ we have $(g \circ f)(x) = x$, and for all $y \in Y$ we have $(f \circ g)(y) = y$.

An equivalent characterisation is that $y = f(x) \iff x = g(y)$.

The following theorem tells us precisely when a function has an inverse. It also tells us that if an inverse exists, then there is only one inverse. For this reason we can speak of *the* inverse function, and give it a specific notation, namely f^{-1}.

This is also the place where we get to our final standard strategy: how to use 'for all' statements.

Critical

To use 'for all x, the predicate $P(x)$ is true', pick a good x (or several).

Remember that '$\forall x \in \mathbb{N}, P(x)$' simply means: all of $P(1)$, and $P(2)$, and $P(3)$, and... are true. '$\forall x \in A, P(x)$' means some similar 'list' of statements are all true. But we rarely want to use all of a long list of statements in a proof: we usually want to pick one or two that are 'helpful'. Just like with proving a 'there exists', where finding a good example needs an idea, it needs an idea to find the right helpful statement.

In terms of the computer program analogy: we're given a program and a promise that it checks the 'for all' statement; now we can play the rôle of the Checker and input some value x to it, and expect to see a reason why $P(x)$ is true coming back out.

Theorem 5.8. *$f : X \to Y$ has an inverse function if and only if f is a bijection. If an inverse function exists, it is unique.*

First, we prove:
$f : X \to Y$ has an inverse $\iff$ f is bijective.

Proof. This is an $\iff$ theorem, so there are two things to prove: the $\Leftarrow$ and the $\Rightarrow$.

First, we show: (f is bijective) $\Rightarrow$ ($f : X \to Y$ has an inverse).

Suppose f is a bijection. In particular, it is surjective. That means we know: for all $y' \in Y$ there is $x' \in X$ with $f(x') = y'$.

We want to define a function $g : Y \to X$ which (we should prove) is the inverse function of f. Since we have the domain and codomain, we need to decide on the function values.

Given $y \in Y$, we use 'f is surjective'. In particular, we use the statement 'there is $x \in X$ with $f(x) = y$', for this particular y.

We would like to define $g(y) = x$. We need to check this is well-defined. Certainly this x exists, the question is whether there might be several (so we wouldn't really know how to pick one). Well, but if there is another x'', not equal to x, such that $f(x'') = y$ then we'd have a contradiction to 'f is injective'. So there really is exactly one x satisfying $f(x) = y$ (for this one given y), and we can define $g(y) = x$.

At this point, we've given an example function which we claim proves that f has an inverse (i.e. that there exists an inverse). We need to check that it really satisfies the definition.

The domain and codomain are correct. So we need to check the two 'for all' composition statements; we do one after the other.

Given $a \in X$, let $f(a) = b$. Well, by definition of g this tells us $g(b) = a$ (recall we checked that there is exactly one solution to the equation $f(x) = y$ for any given y, and in particular for $y = b$). So $g \circ f(a) = a$, which proves $\forall a \in X\,,\ g \circ f(a) = a$.

Now given $d \in Y$, let $g(d) = c$. By definition of g, that tells us that $f(c) = d$ (again, there was exactly one solution), so $g \circ f(d) = d$ which proves $\forall d \in Y\,,\ f \circ g(d) = d$.

This completes this direction of the 'iff'.

Next, we show: $f : X \to Y$ has an inverse $\Rightarrow$ f is bijective.

Suppose f has an inverse function g. We'll prove f is surjective, then injective.

Given $y \in Y$, by definition of inverse, $f(g(y)) = (f \circ g)(y) = y$, so there is some $x \in X$ (namely $x = g(y)$) such that $f(x) = y$. So f is surjective.

Now, given $x, x' \in X$, suppose $f(x) = f(x')$. Then $g(f(x)) = g(f(x'))$. But $g(f(x)) = (g \circ f)(x) = x$ and, similarly, $g(f(x')) = x'$. So: $x = x'$ and f is injective. □

Now we prove that if an inverse function exists, it is unique.

Proof. Suppose that g and h are inverses of f. Then both have domain Y and codomain X, and we just need to check that for every $y \in Y$ we have $g(y) = h(y)$. Well, $h \circ f$ is the identity function on X and $f \circ g$ is the identity function on Y. So, given $y \in Y$ we have

$$g(y) = (h \circ f)\big(g(y)\big) = \big((h \circ f) \circ g\big)(y) = \big(h \circ (f \circ g)\big)(y) = h\big((f \circ g)(y)\big) = h(y)\,,$$

so $g = h$. □

Note that if $f : X \to Y$ is a bijection, then its inverse function (which exists, by Theorem 5.8) is also a bijection. The easiest way to see that is: if g is the inverse function of f, then also by definition f is the inverse function of g. So g has an inverse function, so by Theorem 5.8 g is bijective.

Again, you need to be a bit careful with the notation if your function is (for example) from $\mathbb{R}$ to $\mathbb{R}$. Do *not* confuse f^{-1}, the inverse function, with the function $x \to \big(f(x)\big)^{-1} = 1/f(x)$.

This theorem and proof are important for the course. But this was also our first example of using 'for all' statements, so let's recap how this went, in the 'bijective implies there is an inverse' bit of the proof.

Since we're proving an implication, we assume the premise 'f is a bijection'. We now want to conclude 'there exists an inverse', so the standard strategy is to give an example and explain why it's an example; in this case, 'an example' is a function, so the next job is to write down a function (which we need to give a name to, since f is already in use let's call it g); and as usual, here we need to think to see what the right function is. The domain and codomain of g are clear, what's not clear is what the function values are.

It helps here to have the picture of the function f as two bubbles X and Y with arrows going from X to Y in mind. The inverse function is supposed to be reversing these arrows. Intuitively, if I see an arrow in the f-picture from x in X to y in Y, then I want to draw a g-arrow going from y to x.

But to define a function from Y to X, I need to start with an element y in Y and then figure out what $g(y)$ should be. Putting it another way, I need to write a procedure which, *Given* $y \in Y$, will output an $x \in X$. This procedure is computing the function values.

This looks tricky because we do not have any nice formula for f that we could do algebra with. We're simply told it is a bijection: that is, it is injective and surjective. Both of those statements are 'for all' statements, so we can think of them as procedures which, Given any (valid) input, should output a reason why their predicate-to-the-right is True for that input. What we need to think is: we can use those procedures in order to write out 'defining g' procedure. We don't need to know *why* they work, we can afford to just believe they do work (just like when you use some library function in normal computer programming).

In this case, we are Given an element $y \in Y$. So the obvious statement to look at is 'f is surjective', because that statement is 'for all $y \in Y$, there is $x \in X$ such that $f(x) = y$'. That is, it's a procedure which can be given an input $y \in Y$ (whereas 'injective' expects to see two elements of X). We can start writing our define-g procedure by seeing what we get out of 'f is surjective' for input y. What we get is a reason why '$\exists x \in X \, , \, f(x) = y$' is true; in other words, we should get shown an element of X which f will map to the given y. So we give it a name (we call it x). This is the element of X that our define-g procedure should output. In a computer program, we'd stop here and output, but proofs are a bit different; we need to output as well the reason 'and this is correct because..'.

A function must output a value for every input in the domain, and our procedure clearly does that. But also it is only allowed to output one value for any given input—it should be impossible that you put the same thing in twice and get different things out—so we need to check that it really is impossible. The obvious way to do this is a proof by contradiction: suppose the 'impossible thing' happens, and hope to get to a contradiction. This is where 'f is injective' comes in. If it were possible to put in some particular $y \in Y$ to our define-g procedure and get two different values in X out, then we'd be able to give them names, say x and x'', and we'd have that $x \neq x''$ while $f(x) = f(x'') = y$. This looks very much like the input that 'f is injective' takes: we can put x, x'' into 'f is injective', and we will get told that 'if $x \neq x''$ then $f(x) \neq f(x'')$'. Well, we know that $x \neq x''$ *is* true—that's the 'impossible thing' we're supposing is true—so that means we're being told $f(x) \neq f(x'')$. This is our contradiction: two things, $f(x)$ and $f(x'')$, can't be simultaneously equal and not equal.

At this point, our define-g procedure is done: we've written a procedure which, for any input $y \in Y$, will always output an $x \in X$, together with a reason why it will always output the same thing every time that y is put in (because the definition of 'function' requires that). After this, we need to go on and write a further procedure which checks that the function define-g produces really satisfies the definition of 'inverse function'. This is also substantially about standard strategies, but let's stop here.

Let's be clear about why we need to check that define-g can only produce one output for any given input $y \in Y$. It is because *the definition of 'function' requires this.* The definition of 'f is surjective' only says that, given $y \in Y$, there is an $x \in X$ such that $f(x) = y$; for some functions and a given y, there might be lots of different examples x. In terms of the program analogy—if someone goes back to the 'f is surjective' procedure and changes it, they are only going to look at the requirement 'must give an example x such that $f(x) = y$'. Their new code might give a different reason to the old code: that's all fine, there often are several different reasons why a 'there exists' statement is true.

But we are using 'f is surjective' in our procedure define-g. And define-g has a more stringent requirement: for a given input, the output must always be the same. It cannot be the case that the output depends on whether we use the old or the new version of 'f is surjective'. So we need a reason why, in our particular case, no matter how 'f is surjective' is implemented, we won't get different outputs. In this case, we're using 'f is injective' to provide that reason.

If you go on to a career in software (even if LLMs are writing most of the code), this is something you will care about very much. The way this works is: every procedure has some specification that it must keep to; as a coder, you can assume any procedure you want to use (that someone else wrote) keeps to the specification, but you cannot assume anything not in the specification. This is exactly analogous to: you can assume the definition holds, you cannot assume more. One of the places where serious errors get into complex programs is when you write a procedure that calls some other one, your procedure works, you test it and it works, and then after you've moved on to something else the called procedure is rewritten and now your procedure stops working (or it gives changed answers when it was supposed never to do that). This is what happens when you assume something that was not in the specification of the 'other procedure'. This is something which a mathematician (hopefully) will automatically avoid doing.

5.4.2 Examples

Example 5.9. The function $f : \mathbb{R} \to \mathbb{R}$ is given by $f(x) = 3x + 1$. Find the inverse function.

To find a formula for f^{-1}, we use: $y = f(x) \iff x = f^{-1}(y)$. Now,

$$y = f(x) \iff y = 3x + 1 \iff x = \tfrac{1}{3}(y - 1),$$

so

$$f^{-1}(y) = \tfrac{1}{3}(y - 1).$$

Recall $\mathbb{Z}$ denotes the set of all integers (positive, zero, and negative).

Example 5.10. The function $f : \mathbb{Z} \to \mathbb{N} \cup \{0\}$ is defined as follows:

$$f(n) = \begin{cases} 2n & \text{if } n \geq 0 \\ -2n - 1 & \text{if } n < 0. \end{cases}$$

Prove that f is a bijection and determine a formula for the inverse function f^{-1}.

First, we prove that f is **injective**: Suppose $f(n) = f(m)$. Since $2n$ is even and $-2n - 1$ is odd, either (i) $n, m \geq 0$ or (ii) $n, m < 0$. (For otherwise, one of $f(n), f(m)$ is odd and the other even, and so they cannot be equal.)

In case (i), $f(n) = f(m)$ means $2n = 2m$, so $n = m$.

In case (ii), $f(n) = f(m)$ means $-2n - 1 = -2m - 1$, so $n = m$. Therefore f is injective.

Next, we prove that f is **surjective**: We show that $\forall m \in \mathbb{N} \cup \{0\}, \exists n \in \mathbb{Z}$ such that $f(n) = m$. Consider separately the case m even and the case m odd.

Suppose m is even. Then $n = m/2$ is a non-negative integer and $f(n)$ is $2(m/2) = m)$.

If m odd, then $n = -(m+1)/2$ is a negative integer and

$$f(n) = f(-(m+1)/2) = -2\left(-\frac{(m+1)}{2}\right) - 1 = m.$$

The proof that f is surjective reveals to us what the inverse function is. We have

$$f^{-1}(m) = \begin{cases} m/2 & \text{if } m \text{ even} \\ -(m+1)/2 & \text{if } m \text{ odd.} \end{cases}$$

Finally, let's give an important non-example.

Example 5.11. Let $f : \mathbb{R} \to \mathbb{R}_{\geq 0}$ be defined by $f(x) = x^2$, and let $g : \mathbb{R}_{\geq 0} \to \mathbb{R}$ be defined by $g(x) = \sqrt{x}$.

It's tempting to think that g is the inverse function of f, and indeed $(f \circ g)(x) = x$ for all $x \in \mathbb{R}_{\geq 0}$. But $(g \circ f)(-1) = g(1) = 1$, because $\sqrt{x}$ means the *non-negative* square root of x. If you check Theorem 5.8 you'll see that in fact f doesn't have an inverse function: it is not a bijection. For example $f(1) = 1 = f(-1)$. It's a somewhat common mistake in basic algebra to assume $\sqrt{x^2} = x$; as we just saw it's not true when $x < 0$. We saw essentially this error as Mistake 4 in Section 2.7.

5.5 Functions on sets

Suppose we have a function $f : X \to Y$. It is very common that, given some $S \subseteq X$, we want to talk about the set $\{f(x) : x \in S\}$. To make this easier, we define

$$f(S) = \{f(x) : x \in S\}.$$

Note that $f(\varnothing) = \varnothing$, and for any single $x \in X$ we have $f\big(\{x\}\big) = \big\{f(x)\big\}$. It's important to remember that $\big\{f(x)\big\}$ is *not* the same as $f(x)$ (in the same way that an apple in a box is not the same as an apple).

We also define, for *any* function $f : X \to Y$ and any $T \subseteq Y$, the set

$$f^{-1}(T) = \big\{x \in X : f(x) \in T\big\}.$$

Again, it's important to remember that for $y \in Y$, the set $f^{-1}\big(\{y\}\big)$ is a set of elements in X, and it always exists, in contrast to $f^{-1}(y)$ which is a member of X and is only defined if f is an invertible function.

If f is invertible, then for every $y \in Y$ the set $f^{-1}\big(\{y\}\big)$ contains exactly one element, namely $f^{-1}(y)$. However if f is not invertible, then by Theorem 5.8 either there will be some $y \in Y$ such that $f^{-1}\big(\{y\}\big) = \varnothing$ (i.e. f is not surjective) or there will be some $y \in Y$ such that $f^{-1}\big(\{y\}\big)$ has two or more elements (i.e. f is not injective), or both.

Given a function $f : X \to Y$, the set $f(X)$ is sometimes called the *image of* f. The image $f(X)$ of f is always a subset of the codomain Y (by definition!). It might be that $f(X) = Y$, or it might not be—by definition, $f(X) = Y$ if and only if f is surjective.

Warning 5.12. This section is really rather bad notation, and especially the notation $f^{-1}(T)$ is bad notation. We already are using f^{-1} to mean the inverse function when it exists; we're now using the same symbol to talk about something a little bit similar but also completely different: it's easy to get confused. This is one to blame on long-past mathematicians, but it is so standard that we cannot change it. You will simply need to be careful to check whether what is being put in to f, or to f^{-1}, is a single element of the domain or codomain respectively, or a subset. This is what tells you whether you're looking at the function f itself or the derived function on sets.

5.6 Counting as a bijection

What does it mean to say that a set has three objects? Well, it means that I can take an object from the set, and call that 'Object 1', then I can take a different object from the set and call that 'Object 2', and then I can take a different object from the set and call that 'Object 3', and then I have named all the objects in the set. Obvious, I know, but this is the fundamental way in which we can abstractly define what we mean by saying that a set has m members.

For $m \in \mathbb{N}$, let $\mathbb{N}_m$ be the set $\{1, 2, \ldots, m\}$ consisting of the first m natural numbers. Then we can make the following formal definition:

Definition 5.13. A set S has m members if there is a bijection from $\mathbb{N}_m$ to S.

So, the set has m members if to each number from 1 to m, we can assign a corresponding member of the set S, and all members of S are accounted for in this process. This is like the attachment of labels 'Object 1', etc, described above.

Note that an entirely equivalent definition is to say that S has m members if there is a bijection from S to $\mathbb{N}_m$. This is because if $f : \mathbb{N}_m \to S$ is a bijection, then the inverse function $f^{-1} : S \to \mathbb{N}_m$ is a bijection also. In fact, because of this, we can simply say that S has m members if there is a bijection 'between' $\mathbb{N}_m$ and S. (Eccles uses the definition that involves a bijection from $\mathbb{N}_m$ to S and Biggs uses the definition that involves a bijection from S to $\mathbb{N}_m$.)

For $m \in \mathbb{N}$, if S has m members, we say that S has *cardinality* m (or *size* m). The cardinality of S is denoted by $|S|$, so we would usually simply write $|S| = m$ for 'S has cardinality m'.

Warning 5.14. If you are very alert, you might notice that there is a potential problem with our definition of cardinality. We said something about 'the cardinality of S'. That means we have some idea that there should only be one number m such that $|S| = m$. Well, if I have a set of five fruit, you'll probably happily agree with me that it has cardinality five and nothing else. But is that kind of statement always true whatever S is a set of? What we're worried about here is whether cardinality is *well-defined*. We'll shortly see that it is.

In general 'well-defined' means that whatever definition we just wrote down is not 'cheating' or 'wrong' in some way. What might be an example of a bad definition? Suppose I say 'let t be the number of cards in a deck'. I am claiming to define a number t here; there should be only one answer to the question of what t is. But what deck of cards? A bridge deck (with 52 cards)? or a skat deck (with 32)? Or something else? This t is *not well-defined*, and it's exactly this kind of problem that the warning is getting into. Could it be that there is a set S such that by our definition we have $|S| = 32$ and also $|S| = 52$?

It's usually easiest to write down a definition and then try to argue that it makes sense; we say we are showing the definition is well-defined. We'll do that for cardinality shortly, but we need some more theory first.

5.7 The pigeonhole principle

5.7.1 The principle

The 'pigeonhole principle' is something that you might find obvious, but it is very useful.

Informally, what it says is that says is that if you have n letters and you place them into m pigeonholes in such a way that no pigeonhole contains more than one letter, then $n \leq m$. Equivalently, if $n > m$ (so that you have more letters than pigeonholes), then some pigeonhole will end up containing more than one letter. This is very intuitive. Obvious as it may be, however, can you think about how you would actually prove it?

We can't really hope to prove any vague statement until we make it more formal. So let's first do that.

Theorem 5.15 (Pigeonhole Principle (PP))**.** *Suppose that A and B are sets with $|A| = n$ and $|B| = m$, where $m, n \in \mathbb{N}$. If there is an injection from A to B, then $n \leq m$.*

We've just formalised the first statement above: if we place (the function f) letters (the set A) into pigeonholes (the set B) such that no pigeonhole contains more than one letter (f is injective) then A cannot be bigger than B. This is now a clear formal statement: we know exactly what we need to prove.

But coming up with a proof is not easy. We'll need to talk about injective functions (because there is an injective function in the statement), but we will also need to use the definition of cardinality, because that also shows up (we say $|A| = n$) and that talks about (completely different!) bijective functions. And furthermore, we will probably need to talk about the members of A and of B, which are two arbitrary sets—we don't know what the members are. To get around that (temporarily!) let's try to prove the statement for a couple of specific sets.

Theorem 5.16 (Pigeonhole Principle (PP), special case)**.** *The following statement is true for all $n \in \mathbb{N}$: For all natural numbers m, if there is an injection from $\mathbb{N}_n$ to $\mathbb{N}_m$, then $n \leq m$.*

This version doesn't talk about cardinality; we know (by definition!) that $|\mathbb{N}_n| = n$ and $|\mathbb{N}_m| = m$, and we know what the elements of these two sets are. This will make it easier to write a formal proof. But it's still not easy to see what to do next.

We know we need to deal with injective functions to prove this special case. So let's prove a statement about injective functions. For now, it is going to be unclear what this statement has to do with the Pigeonhole Principle; I'll try to explain where it comes from later.

Lemma 5.17. *Suppose that A and B are sets, each of which has at least two distinct elements. Suppose that a is an element of A, and b is an element of B. If there is an injection $f : A \to B$, then there is an injection $g : A \setminus \{a\} \to B \setminus \{b\}$.*

Critical

You must understand the proof of this lemma.

In recent years, I've asked a few exam questions which test whether students have the skills needed to prove this lemma (this is not a guarantee I will do that again this year). Even though this is a small part of the course and of the exam, the score students get on that question correlates very well with their course grade.

The 'story of the proof' is as follows. You're a hotel manager; you have a collection of guests A checked in to your set of single rooms B. You might or might not be full—it doesn't matter for this story—but of course any two different guests are checked in to different rooms.

One morning, a guest a arrives at the front desk to check out. At the same time, the plumber comes along to tell you that Room b's en-suite toilet has exploded.

Your job is to write out who is staying where for the next night. Since Guest a is checking out, you'll have to be sure not to put them on the new list. And since Room b is in poor condition, you can't have anyone staying there. What do you do?

The simplest option is just to recopy the list from last night but skip Guest a. Can you do that? Well, ask the plumber if there was any luggage in Room b. If No, then that will work.

If Yes? Then you know you'll have to move that person: look them up on last night's list, and let's call them Guest s. Where can they stay? Well, the easiest option is to ask Guest a which room they were staying in, and send Guest s there (and recopy the rest of the list).

The function f is 'last night's list', and the description above is a procedure to construct g, 'the new list'. You should notice that the computation that is done depends on what f is; there are two cases. You should also notice that even though a lot of the new list g is the same as f, still these are different lists.

A standard question here is 'What if Guest a was in Room b?'. Well—it doesn't affect the procedure. Guest a has already left the room, the plumber will report that the room is empty. If Guest a hears the plumber's report and says 'Ha! I exploded that!' then it will affect the mood of the hotel manager, but still all that has to be done is recopy the old list absent Guest a.

Let's now write this formally.

Proof. Given A and B, and elements $a \in A$ and $b \in B$, we want to prove that if there is an injection $f : A \to B$, then there is an injection $g : A \setminus \{a\} \to B \setminus \{b\}$.

So suppose that $f : A \to B$ is an injection. We need to construct a function $g : A \setminus \{a\} \to B \setminus \{b\}$ and prove it is an injection.

Case 1: for each $x \in A \setminus \{a\}$ we have $f(x) \in B \setminus \{b\}$.

We define a function $g : A \setminus \{a\} \to B \setminus \{b\}$ by $g(x) = f(x)$ for each x. This is well-defined because we assumed that for each x in $A \setminus \{a\}$, indeed $f(x)$ is in $B \setminus \{b\}$. We just need to check that g is indeed injective. Well, suppose $g(x) = g(y)$. Then by definition $f(x) = f(y)$, and since f is injective $x = y$. So g is indeed injective.

Case 2: there is $s \in A \setminus \{a\}$ such that $f(s) = b$.

Let's first check that there is exactly one s such that $f(s) = b$. Indeed, suppose that for some $t \in A$ we have $f(t) = b$. Then $f(t) = f(s)$, and since f is injective, we conclude $t = s$. In particular, since a and s are different, we have $f(a) \neq b$.

We define $g : A \setminus \{a\} \to B \setminus \{b\}$ by

$$g(x) = \begin{cases} f(x) & \text{if } x \neq s \\ f(a) & \text{if } x = s \end{cases} .$$

This is well-defined—that is, $g(x)$ is in $B \setminus \{b\}$ for each x in the domain—because if $x \neq s$ then we just checked $f(x) \neq b$ so $g(x) = f(x) \in B \setminus \{b\}$, while $g(s) = f(a)$ is not equal to b.

We still have to check g is injective. Given $x, y \in A \setminus \{a\}$, we need to prove $g(x) = g(y) \implies x = y$. So suppose $g(x) = g(y)$, and we need to conclude that $x = y$. Since there are cases in the definition of g, we'll need to consider those cases here.

Subcase A: $x = s$ and $y = s$. Since $x = s = y$ in particular $x = y$.

Subcase B: $x \neq s$ and $y \neq s$. Then $g(x) = f(x)$ and $g(y) = f(y)$. So $f(x) = f(y)$, and since f is injective we have $x = y$.

Subcase C: $x = s$ and $y \neq s$. Then $g(x) = f(a)$ and $g(y) = f(y)$. So $f(a) = f(y)$, since f is injective $y = a$, but $y \in A \setminus \{a\}$ which is a contradiction—this case can't happen.

Subcase D: $x \neq s$ and $y = s$. This case is symmetric to Subcase C: just swap x and y in the text above.

This completes the check that in Case 2 the function g is injective.

In either case, we were able to construct an injective g as desired, and the two cases are exhaustive. □

We'll see this Lemma is what we need to prove Theorem 5.16 by induction. As a quick remark, it's maybe not clear why in the statement of the Lemma we say that A and B each have at least *two* distinct elements. The reason is that we do not want $A \setminus \{a\}$ or $B \setminus \{b\}$ to be the empty set; it's not clear what a function with domain or codomain the empty set should be. We can now prove Theorem 5.16.

Proof of Theorem 5.16. We prove this by induction. The statement we want to prove is the statement $P(n)$: 'for all $m \in \mathbb{N}$, if there is an injection from $\mathbb{N}_n$ to $\mathbb{N}_m$, then $n \leq m$.'

The base case, $n = 1$, is true because for all $m \in \mathbb{N}$ we have $1 \leq m$.

Given a natural number k, we want to prove $P(k) \implies P(k+1)$.

Suppose for an induction hypothesis that $P(k)$ is true. We want to prove $P(k+1)$. That is, given m, we want to show that if there is an injection $f : \mathbb{N}_{k+1} \to \mathbb{N}_m$, then $k+1 \leq m$.

So suppose there is an injection $f : \mathbb{N}_{k+1} \to \mathbb{N}_m$. We want to show $k+1 \leq m$. Since $k \geq 1$, we have $k+1 \geq 2$.

If $m = 1$, then the codomain of f is $\{1\}$, so $f(1) = f(2) = 1$. But this is a contradiction to our assumption that f is injective; this case cannot occur.

If $m \geq 2$, then f is an injective function from $\mathbb{N}_{k+1}$ to $\mathbb{N}_m$, and both of these sets have at least two elements (both contain 1 and 2). So we can apply Lemma 5.17, with $A = \mathbb{N}_{k+1}$ and $a = k+1$, and $B = \mathbb{N}_m$ and $b = m$. The Lemma says that there is an injective function $g : \mathbb{N}_k \to \mathbb{N}_{m-1}$.

And now our induction hypothesis $P(k)$ tells us that $k \leq m-1$. Adding 1 to both sides, we conclude $k+1 \leq m$, which is what we wanted.

This proves the induction step. By the Principle of Induction, we conclude that $P(n)$ is true for all $n \in \mathbb{N}$. □

Finally, let's explain why the special case of the Pigeonhole Principle implies the general case, Theorem 5.15.

Proof of Theorem 5.15. From the definition of cardinality, there are bijections $g : \mathbb{N}_n \to A$ and $h : \mathbb{N}_m \to B$. We also have an inverse bijection $h^{-1} : B \to \mathbb{N}_m$ by Theorem 5.8. In particular both g and h^{-1} are injections.

Suppose there is an injection $f : A \to B$. We prove in exercises that the composition of two injections is an injection, so $f \circ g$ is an injection. Applying the same statement again, $h^{-1} \circ f \circ g$ is an injection, with domain $\mathbb{N}_n$ and codomain $\mathbb{N}_m$.

By Theorem 5.16 it follows that $n \leq m$. □

This was a long proof. Before we make a couple of comments on what you should learn from it, let's deduce one important conclusion.

Theorem 5.18. *Suppose n, m are two natural numbers. If there is a bijection from $\mathbb{N}_n$ to $\mathbb{N}_m$, then $n = m$.*

Proof. Suppose $f : \mathbb{N}_n \to \mathbb{N}_m$ is a bijection. Then f is an injection. So from Theorem PP, $n \leq m$.

But by Theorem 5.8 there is an inverse function $f^{-1} : \mathbb{N}_m \to \mathbb{N}_n$ and this is also a bijection. In particular, f^{-1} is an injection from $\mathbb{N}_m$ to $\mathbb{N}_n$, and hence $m \leq n$.

Now we have both $n \leq m$ and $m \leq n$, hence $n = m$. □

What this theorem tells us is that our definition of cardinality is well-defined. Remember we were worried that possibly there is some set S which has cardinality both m and n, and m and n aren't the same; then it wouldn't make sense to say that either is 'the size of S'. But if both 'S has cardinality m' and 'S has cardinality n' hold, then there are by definition bijections $f : \mathbb{N}_m \to S$ and $g : \mathbb{N}_n \to S$. Then $f^{-1} \circ g$ is a bijection from $\mathbb{N}_n \to \mathbb{N}_m$. And now Theorem 5.18 says $n = m$. This justifies that it makes sense to write $|S| = n$.

The pigeonhole principle is remarkably useful (even in some very advanced areas of mathematics). It has many applications. For most applications, it is the contrapositive form of the principle that is used. This states:

If $m < n$ and $f : \mathbb{N}_n \to \mathbb{N}_m$ is any function, then f is not an injection..

So, if $m < n$, and f is *any* function $f : \mathbb{N}_n \to \mathbb{N}_m$, then there are $x, y \in \mathbb{N}_n$ with $x \neq y$ such that $f(x) = f(y)$.

In other words, if you have more letters than pigeonholes, then you will have to put at least two letters into some one pigeonhole.

5.7.2 What will be on the exam?

We've just seen our first 'long' proof which is examinable, the proof of the Pigeonhole Principle. You might be tempted to make a tactical guess that I will not ask you to reproduce this proof in the exam (which is correct, I won't ask it) and hence skip it. And you might think that it is too obvious to be interesting.

This would be an error. The proof is in the course for a reason: it's the first proof you have seen which uses 'abstract information' in a serious way, and I can and quite possibly will ask questions on the exam which test your ability to do something similar, maybe in a simpler scenario (the proof of PP is too long for an exam question, and would be too hard if you hadn't seen it before).

There are a few steps to the proof of the Pigeonhole Principle. The first one, after sorting out how to write down the right formal statement (Theorem 5.15) is to notice that it's enough to prove Theorem 5.16. This isn't 'necessary'—you can write a proof of Theorem 5.15 without deducing it from Theorem 5.16—but it does make a lot of statements simpler; it's easier to understand the way we wrote it.

After this, how does one think of the proof of Theorem 5.16? If you hadn't seen the proof before, most likely you would try to prove it directly, and at some point you'd get stuck. Then you might notice that since it is a 'for all natural numbers' statement, a possibility would be to try an induction proof. I think realistically you won't find the induction argument unless you're looking for it here.

Once you think of trying induction on n, then it's obvious that the base case is true—we don't need to think at all about the condition 'if there is an injection from $\mathbb{N}_1$ to $\mathbb{N}_m$' at all, because $1 \le m$ is true for all natural numbers m.

So the difficulty is to prove the induction step. Now, it is not obvious how to do this—it is certainly not the case that a Real Mathematician instantly sees how to do it. What we do is look for something more we can say, ideally something that will let us use our induction hypothesis. There is one more thing we can easily say. We are given that there is an injection from $\mathbb{N}_{k+1}$ to $\mathbb{N}_m$; in particular $k+1$ is at least 2, and we can immediately rule out the possibility $m = 1$. Note we do *not* use the induction hypothesis to do this (even though we are in the middle of the induction step). So what is left (in the induction step) is to deal with the case $m \ge 2$.

Now, at this point Lemma 5.17 plus the induction assumption immediately deals with this case and we are done. But this is 'cheating'—the only reason you would care about Lemma 5.17 is in order to prove Theorem 5.16. It is certainly not the case that some historical mathematician proved Lemma 5.17 and then noticed that they could use it to prove Theorem 5.16. What we can see at this point is that our induction hypothesis $P(k)$ will tell us $k \le m-1$ (which is basically what we want) provided we can somehow find an injective function from $\mathbb{N}_k$ to $\mathbb{N}_{m-1}$. So our aim has to be to find such an injective function, and this has to come somehow from the injection we know exists, namely f.

That means it's natural to write down a statement 'if $m \ge 2$ and there is an injection $f : \mathbb{N}_{k+1} \to \mathbb{N}_m$ then there is an injection $g : \mathbb{N}_k \to \mathbb{N}_{m-1}$'; it's what we want to be true. And this is more or less the same thing as Lemma 5.17. One could (and in years long past we did) not bother to write a separate Lemma, but simply prove the statement in quotes above at this point. Students generally complained it was confusing, so now we separate the Lemma out explicitly.

At last, we have one more question: how do we think of the proof of the Lemma? Well, the first few lines are 'automatic'; we've just written down the information we're given in the lemma statement, and then we have to prove an implication—so we go for the simplest route, namely assume the premise and try to prove the conclusion from it.

Then we get to a case distinction. This case distinction looks a bit complicated at first, but it follows the basic idea mentioned earlier in these notes: if you're not sure how to prove something, identify a special 'easy' case you can do, do it, then figure out how to do the rest. The 'easy case' is Case 1; here f really immediately gives us the injection g we want, we just need to write it down and check it.

The 'hard' case is Case 2. All we do to write it down is figure out what it means that 'we are not in Case 1', but it turns out to give us a piece of *abstract information*; we get told something about the function values of f, namely $f(s) = b$, which we did not know before, and which we should try to use. And, finally, once we got this far it turns out not to be that hard!

This kind of understanding is what I want you to get from the proof of PP. For all the longer proofs in these notes, I would like you to get an idea of why the proof works and what ideas you are being shown that you can use elsewhere in your own proofs; this is why these proofs are there. Sometimes, as here, I'll break the proof into bitesize pieces and give more details of what and why we are doing something, but not always. It is good for you to learn to break a long complicated argument into pieces yourself—identify the key points, figure out which things are 'automatic' (i.e. the first thing you should try works) and which are 'difficult' (everything else, especially the times where the second and third things you should try don't work either). It's not quite as good as coming up with a long complicated proof of your own, but it's a next best.

5.7.3 Some applications of the Pigeonhole Principle

We start with an easy example.

Theorem 5.19. *In any group of* 13 *or more people, there are two persons whose birthday is in the same month.*

Proof. Consider the function that maps the people to their months of birth. Since $13 > 12$, this cannot be a bijection, so two people are born in the same month. □

This next one is not hard, but perhaps not immediately obvious.

Theorem 5.20. *In a room full of people, there will always be at least two people who have the same number of friends in the room.*

Proof. Let X be the set of people in the room and suppose $|X| = n \geq 2$. Consider the function $f : X \to \mathbb{N} \cup \{0\}$ where $f(x)$ is the number of friends x has in the room.

Let's assume that a person can't be a friend of themselves. (We could instead assume that a person is always friendly with themselves: we simply need a convention one way or the other.)

Then $f(X) = \{f(x) : x \in X\} \subseteq \{0, 1, \ldots, n-1\}$. But there can't be x, y with $f(x) = n-1$ and $f(y) = 0$. **Why?** Well, such an x would be a friend of all the others, including y, which isn't possible since y has no friends in the room.

So either $f(X) \subseteq \{0, 1, \ldots, n-2\}$ or $f(X) \subseteq \{1, \ldots, n-1\}$. In each case, since $f(x)$ can take at most $n-1$ values, there must, by PP, be at least two $x, y \in X$ with $f(x) = f(y)$. And that's what we needed to prove. □

Here's an interesting geometrical example. For two points (x_1, y_1), (x_2, y_2) in the plane, the **midpoint** of (x_1, y_1) and (x_2, y_2) is the point

$$\left(\tfrac{1}{2}(x_1 + x_2), \tfrac{1}{2}(y_1 + y_2)\right)$$

(the point on the middle of the line connecting (x_1, y_1) to (x_2, y_2)).

Theorem 5.21. *If we have a set A of five or more points in the plane with* ***integer*** *coordinates, then there are two points in A whose midpoint has integer coordinates.*

Proof. For two integers a, b, $\frac{1}{2}(a+b)$ is an integer if and only if $a+b$ is even, so if and only if a, b are both even or are both odd.

So the midpoint of $(x_1, y_1), (x_2, y_2)$ has both coordinates integer if and only if x_1, x_2 are **both** even or **both** odd, **and also** y_1, y_2 are **both** even or **both** odd.

Let's label each of the points (a, b) of A with one of "(even,even)", "(even,odd)", "(odd,even)" or "(odd,odd)".

Since $|A| \geq 5$, there will be at least two points which receive the same label. Hence these two points have the same parity (odd or even) for the first coordinate, and the same parity for the second coordinate. This means the midpoint of these two points must be integer as well. □

By the way, this result would not necessarily hold if we only had four points in the set. Consider $(0,0)$, $(1,0)$, $(1,0)$ and $(1,1)$.

Here's a very interesting number theory application (with a very sneaky proof). It uses the notion of remainders on division by n, which we'll cover properly in Lent Term: for now, all we need is that, for every natural number m, the "remainder, r, upon division by n" is one of the numbers $0, 1, \ldots, n-1$, and that $m - r$ is divisible by n.

Theorem 5.22. *Let $a_1, a_2, \ldots, a_n$ be n integers (where $n \geq 2$). Then there exists a non-empty collection of these integers whose sum is divisible by n.*

Proof. Consider the numbers $s_0, s_1, \ldots, s_n$ given by

$$s_0 = 0,$$

$$s_1 = a_1,$$

$$s_2 = a_1 + a_2,$$

$$s_3 = a_1 + a_2 + a_3,$$

etc., until

$$s_n = a_1 + a_2 + \cdots + a_n.$$

(It is not obvious, at all, why we should do this, but it will work!)

For each of these s_i, consider the remainder upon division by n. Since there are $n+1$ numbers s_i, but only n possible remainders $(0, 1, \ldots, n-1)$, two of the s_i will have the same remainder upon division by n.

So suppose s_k and s_ℓ have the same remainder, where $k < \ell$. Then $s_\ell - s_k$ is divisible by n. But since $s_\ell - s_k = a_{k+1} + a_{k+2} + \cdots + a_\ell$, this means that the sum $a_{k+1} + a_{k+2} + \cdots + a_\ell$ is divisible by n. Se we have proved the result. □

In fact we proved something even stronger than what we set out to prove:
Let $a_1, a_2, \ldots, a_n$ be a list of n integers (where $n \geq 2$). Then there exists a non-empty collection of **consecutive** numbers from this list $a_{k+1}, a_{k+2}, \ldots, a_\ell$ whose sum is divisible by n.

The theorem isn't true if we have fewer than n integers. For instance, if for any $n \geq 2$ we take the numbers $a_1, \ldots, a_{n-1}$ all equal to 1, then it's impossible to find a sum that adds up to something divisible by n.

5.8 A generalised form of PP

We state without proof the following more general version of the PP. Again, it's rather obvious. Isn't it?

Theorem 5.23. *Suppose $f : A \to B$ and that $|A| > k|B|$ where $k \in \mathbb{N}$. Then there is some element of B that is the image of at least $k + 1$ elements of A.*

I should maybe point out why the proof of this is not in the course. First, it is something you can find or generate for yourself fairly easily if you want. More importantly, it won't show you any new ideas; you wouldn't learn anything you didn't already see earlier.

Last year, 241 students were registered for this course. I knew, before marking the exams, that at least three of them would get the same exam mark.

Why? Well, apply the theorem, with A being the students, B being the set $\{0, 1, \ldots, 100\}$ of all possible marks (which is of size 101) and $f(x)$ the mark of student x. Since $241 > 2(101)$, there's some mark y such that at least $2 + 1 = 3$ students will have $y = f(x)$, which means they get the same mark.

5.9 Infinite sets

We say that a set A is *finite* when there is some $n \in \mathbb{N}$ such that $|A| = n$. Otherwise, A is said to be *infinite*.

For example, the set of natural numbers is infinite. You might think that's obvious, but how would you prove it? (Remember that the formal definition that a set A has cardinality n is that there is a bijection between $\mathbb{N}_n$ and A.)

One way to show this is to use a proof by contradiction. Suppose (for a contradiction) that $\mathbb{N}$ is finite, of cardinality $n \in \mathbb{N}$, and that $f : \mathbb{N}_n \to \mathbb{N}$ is a bijection. Consider the number $N = f(1) + f(2) + \cdots + f(n)$. Since each $f(i)$ is a natural number, for all $i \in \mathbb{N}_n$, N is also a natural number. But $N > f(i)$ for all $i \in \mathbb{N}_n$. So here is a natural number, N, that is not equal to $f(i)$ for any $i \in \mathbb{N}_n$. But that contradicts the fact that f is a bijection, because if it's a bijection then it's certainly a surjection and there should be some $i \in \mathbb{N}_n$ with $f(i) = N$.

5.10 Sample exercises

Exercise 5.1. *Suppose that X, Y, Z are sets and that $f : X \to Y$ and $g : Y \to Z$. Prove that if f and g are injections, so is the composition $g \circ f$. Prove also that if f and g are surjections, then so is the composition $g \circ f$.*

Exercise 5.2. *Let $\mathbb{Z}$ be the set of all integers and suppose that $f : \mathbb{Z} \to \mathbb{Z}$ is given, for $x \in \mathbb{Z}$, by*

$$f(x) = \begin{cases} x + 1 & \text{if } x \text{ is even} \\ -x + 3 & \text{if } x \text{ is odd.} \end{cases}$$

Determine whether f is injective. Determine also whether f is surjective.

Exercise 5.3. *Suppose that X, Y, Z are sets, and we have functions $f : X \to Y$, $g : Y \to Z$, and $h : Y \to Z$. Suppose that the compositions $h \circ f$ and $g \circ f$ are equal, and also that f is surjective. Prove that $g = h$.*

Exercise 5.4. *Suppose that X, Y, Z are sets and that $f : X \to Y$ and $g : Y \to Z$. Prove that if the composition $g \circ f$ is injective, then f is injective. Prove that if $g \circ f$ is surjective, then g is surjective.*

Exercise 5.5. *Suppose that A and B are non-empty finite sets and that they are disjoint (i.e. $A \cap B = \varnothing$). Prove, using the formal definition of cardinality, that $|A \cup B| = |A| + |B|$.*

Exercise 5.6. *Suppose that X, Y are any two finite sets. By using the fact that*

$$X \cup Y = (X \setminus Y) \cup (Y \setminus X) \cup (X \cap Y),$$

together with the result of Exercise 5.5, prove that

$$|X \cup Y| = |X| + |Y| - |X \cap Y|.$$

Exercise 5.7. *Suppose $n \in \mathbb{N}$ and that $f : \mathbb{N}_{2n+1} \to \mathbb{N}_{2n+1}$ is a bijection. Prove that there is some odd integer $k \in \mathbb{N}_{2n+1}$ such that $f(k)$ is also odd. (State clearly any results you use.)*

5.11 Comments on selected activities

Comment on Activity 5.1. To get started, observe that we can describe the function $h(x)$ defined by $h(x) = 0$ for $x < 0$ and $h(x) = 2x$ for $x \geq 0$ using the formula $h(x) = x + |x|$, where $|x|$ is (as is usual) the *absolute value of* x, i.e. the function $|x| = x$ if $x \geq 0$ and $|x| = -x$ if $x < 0$. (We could also write $|x| = \sqrt{x^2}$). It follows that

$$g(x) = \tfrac{1}{10}\big((x - 11850) + |x - 11850|\big) + \tfrac{1}{10}\big((x - 46350) + |x - 46350|\big).$$

Would that formula be more or less useful to you than the description we gave to define it?

Comment on Activity 5.2. Given any $y \in \mathbb{R}$, let $x = y/2$. Then $f(x) = 2(y/2) = y$. This shows that f is surjective. Also, for $x, y \in \mathbb{R}$,

$$f(x) = f(y) \implies 2x = 2y \implies x = y,$$

which shows that f is injective. Hence f is a bijection.

5.12 Solutions to exercises

Solution to Exercise 5.1. Suppose f and g are injective. Then, for $x, y \in X$,

$$\begin{aligned}(g \circ f)(x) = (g \circ f)(y) &\implies g(f(x)) = g(f(y)) \\ &\implies f(x) = f(y) \text{ (because } g \text{ is injective)} \\ &\implies x = y \text{ (because } f \text{ is injective).}\end{aligned}$$

This shows that $g \circ f$ is injective.

Suppose that f and g are surjective. Let $z \in Z$. Then, because g is surjective, there is some $y \in Y$ with $g(y) = z$. Because f is surjective, there is some $x \in X$ with $f(x) = y$. Then

$$(g \circ f)(x) = g(f(x)) = g(y) = z,$$

so z is the image of some $x \in X$ under the mapping gf. Since z was any element of Z, this shows that $g \circ f$ is surjective.

Solution to Exercise 5.2. Suppose one of x, y is even and the other odd. Without any loss of generality, we may suppose x is even and y odd. (‘Without loss of generality’ signifies that there is no need to consider also the case in which x is odd and y is even, because the argument we’d use there would just be the same as the one we’re about to give, but with x and y interchanged.)

So $f(x) = x+1$ and $f(y) = -y+3$. But we cannot then have $f(x) = f(y)$ because $x+1$ must be an odd number and $-y+3$ an even number. So if $f(x) = f(y)$, then x, y are both odd or both even. If x, y are both even, this means $x+1 = y+1$ and hence $x = y$. If they are both odd, this means $-x+3 = -y+3$, which means $x = y$. So we see that f is injective.

Is f surjective? Let $z \in \mathbb{Z}$. If z is odd, then $z-1$ is even and so $f(z-1) = (z-1)+1 = z$. If z is even, then $3-z$ is odd and so $f(3-z) = -(3-z)+3 = z$. So for $z \in \mathbb{Z}$ there is $x \in \mathbb{Z}$ with $f(x) = z$ and hence f is surjective.

Solution to Exercise 5.3. Suppose f is surjective and that $h \circ f = g \circ f$. Let $y \in Y$. We show $g(y) = h(y)$. Since y is any element of Y in this argument, this will establish that $g = h$. Because f is surjective, there is some $x \in X$ with $f(x) = y$. Then, because $h \circ f = g \circ f$, we have $h(f(x)) = g(f(x))$, which means that $h(y) = g(y)$. So we've achieved what we needed.

Solution to Exercise 5.4. Suppose $g \circ f$ is injective. To show that f is injective we need to show that $f(x) = f(y) \implies x = y$. Well,

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

by definition of a function. Now $g(f(x)) = (g \circ f)(x)$, and similarly for y; this is what $\circ$ means. And

$$(g \circ f)(x) = (g \circ f)(y) \implies x = y\,,$$

because $g \circ f$ is injective. So we proved

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

i.e. f is injective.

Now suppose $g \circ f$ is surjective. So for all $z \in Z$ there is some $x \in X$ with $(g \circ f)(x) = z$. So $g(f(x)) = z$. Denoting $f(x)$ by y, we therefore see that there is $y \in Y$ with $g(y) = z$. Since z was any element of Z, this shows that g is surjective.

Solution to Exercise 5.5. Suppose $|A| = m$ and $|B| = n$. We need to show that $|A \cup B| = m+n$ which means, according to the definition of cardinality, that we need to show there is a bijection from $\mathbb{N}_{m+n}$ to $A \cup B$. Because $|A| = m$, there is a bijection $f : \mathbb{N}_m \to A$ and because $|B| = n$, there is a bijection $g : \mathbb{N}_n \to B$. Let us define $h : \mathbb{N}_{m+n} \to A \cup B$ as follows:

$$\text{for } 1 \le i \le m,\ h(i) = f(i) \quad \text{and for } m+1 \le i \le m+n,\ h(i) = g(i-m).$$

Then h is injective. We can argue this as follows: if $1 \le i, j \le m$ then

$$h(i) = h(j) \implies f(i) = f(j) \implies i = j,$$

because f is injective. If $m+1 \le i, j \le m+n$ then

$$h(i) = h(j) \implies g(i-m) = g(j-m) \implies i-m = j-m \implies i = j,$$

because g is injective. The only other possibility is that one of i, j is between 1 and m and the other between $m+1$ and $m+n$. In this case, the image under h of one of i, j belongs to A and the image of the other to B and these cannot be equal because $A \cap B = \emptyset$. So h is indeed an injection. It is also a surjection. For, given $a \in A$, because f is a surjection, there is $1 \le i \le m$ with $f(i) = a$. Then $h(i) = a$ also. If $b \in B$ then there is some $1 \le j \le n$ such that $g(j) = b$. But then, this means that $h(m+j) = g((m+j)-m) = b$, so b is the image under h of some element of $\mathbb{N}_{m+n}$. So h is a bijection from $\mathbb{N}_{m+n}$ to $A \cup B$ and hence $|A \cup B| = m+n$.

Solution to Exercise 5.6. Note first that the two sets $(X \smallsetminus Y) \cup (Y \smallsetminus X)$ and $X \cap Y$ are disjoint. Therefore,

$$|X \cup Y| = |(X \smallsetminus Y) \cup (Y \smallsetminus X)| + |X \cap Y|.$$

Now, $(X \smallsetminus Y)$ and $(Y \smallsetminus X)$ are disjoint, so

$$|(X \smallsetminus Y) \cup (Y \smallsetminus X)| = |(X \smallsetminus Y)| + |(Y \smallsetminus X)|$$

and therefore

$$|X \cup Y| = |(X \smallsetminus Y)| + |(Y \smallsetminus X)| + |X \cap Y|.$$

Now, the sets $X \smallsetminus Y$ and $X \cap Y$ are disjoint and their union is X, so

$$|X| = |(X \smallsetminus Y) \cup (X \cap Y)| = |X \smallsetminus Y| + |X \cap Y|.$$

A similar argument shows that

$$|Y| = |(Y \smallsetminus X) \cup (X \cap Y)| = |Y \smallsetminus X| + |X \cap Y|.$$

These mean that

$$|X \smallsetminus Y| = |X| - |X \cap Y| \text{ and } |Y \smallsetminus X| = |Y| - |X \cap Y|.$$

So we have

$$\begin{aligned} |X \cup Y| &= |(X \smallsetminus Y)| + |(Y \smallsetminus X)| + |X \cap Y| \\ &= (|X| - |X \cap Y|) + (|Y| - |X \cap Y|) + |X \cap Y| \\ &= |X| + |Y| - |X \cap Y|. \end{aligned}$$

Solution to Exercise 5.7. Let E be the set of even integers, and O the set of odd integers, in the range $\{1, 2, \ldots, 2n+1\}$. Then $|E| = n$ and $|O| = n+1$. If f was such that $f(k)$ was even for all $k \in O$, then $f^* : O \to E$ given by $f^*(x) = f(x)$ would be an injection. But, by the pigeonhole principle, since $|O| > |E|$, such an injection cannot exist. Hence there is some odd k such that $f(k)$ is odd.

6

Equivalence relations and the rational numbers

The material in this chapter is also covered in:

- Biggs, N. L. *Discrete Mathematics*. Chapter 7.
- Eccles, P.J. *An Introduction to Mathematical Reasoning*. Chapter 22.

6.1 Introduction

In this chapter of the notes we study the important idea of an *equivalence relation*, a concept that is central in abstract mathematics.

6.2 Equivalence relations

6.2.1 Relations in general

The idea of a *relation* is quite a general one. For example, consider the set of natural numbers $\mathbb{N}$ and let us say that two natural numbers m, n are related, denoted by $m\,R\,n$, if $m + n$ is even. So we have, for instance, $6\,R\,2$ and $7\,R\,5$, but that 6 and 3 are not related. This relation has some special properties. For one thing, since $2n$ is even for all $n \in \mathbb{N}$, $n\,R\,n$ for all $n \in \mathbb{N}$. (We say such a relation is *reflexive*.) Also, if $m\,R\,n$, then $m + n$ is even. But $m + n = n + m$ and hence, also, $n\,R\,m$. (We say such a relation is *symmetric*.) It is because $m\,R\,n \iff n\,R\,m$ that we can simply say that 'm and n are related' rather than 'm is related to n' or 'n is related to m'. The relation R has other important properties that we will come back to later.

Formally, a relation R on a set X is a subset of the Cartesian product $X \times X$ (which, recall, is the set of all ordered pairs of the form (x, y) where $x, y \in X$). You should just keep in mind that $x\,R\,y$ is a true-or-false statement; if you're not told any more about the relation, there's not much more you can say—maybe for some x and y you are told $x\,R\,y$ is true, but it doesn't tell you whether or not $y\,R\,x$ is true, for example.

In some textbooks, the author insists on using the Cartesian product notation; so you might see $(6, 2) \in R$ where we write $6\,R\,2$. The Cartesian product notation has the advantage of being clear and unambiguous, but the (big!) disadvantage that you already know a lot of relations, such as equality, greater than, and so on, and in fact you write them in the $6\,R\,2$ style.

Example 6.1. Suppose R is the relation on $\mathbb{R}$ given by $x\,R\,y \iff x > y$. Regarded as a subset of $\mathbb{R} \times \mathbb{R}$, this is the set $\{(x, y) \mid x > y\}$. This relation does not possess the reflexive and symmetric properties we met in the example above. For no $x \in \mathbb{R}$ do we have $x\,R\,x$ because x is not greater than x. Furthermore, if $x\,R\,y$ then $x > y$, and we cannot therefore also have $y\,R\,x$, for that would imply the contradictory statement that $y > x$.

In many cases, we use special symbols for relations. For instance '=' is a relation, as is >. It is often convenient to use a symbol other than R: for instance, many textbooks use $x \sim y$ rather than $x\,R\,y$ as a symbol for 'some relation', particularly if the relation is an *equivalence relation* (see below).

6.2.2 The special properties of equivalence relations

There are three special properties that a relation might have (two of which we saw in one of the earlier examples):

Definition 6.2. Suppose that R is relation on a set X. Then

- [**The reflexive property**] R is said to be *reflexive* if, for all $x \in X$, $x\,R\,x$.
- [**The symmetric property**] R is said to be *symmetric* if, for all $x, y \in X$, $x\,R\,y$ implies $y\,R\,x$ (equivalently, for all $x, y \in X$, $x\,R\,y \implies y\,R\,x$).
- [**The transitive property**] R is said to be *transitive* if, for all $x, y, z \in X$, whenever $x\,R\,y$ and $y\,R\,z$, we also have $x\,R\,z$; that is, $(x\,R\,y) \wedge (y\,R\,z) \implies xRz$.

A relation that has all three of these properties is called an *equivalence relation.*

Definition 6.3. A relation is an *equivalence relation* if is reflexive, symmetric and transitive.

Example 6.4. We saw earlier that the relation on $\mathbb{N}$ given by

$$m\,R\,n \iff m + n \text{ is even}$$

is reflexive and symmetric. It is also transitive. To prove that, suppose x, y, z are three natural numbers and that $x\,R\,y$ and $y\,R\,z$. Then $x + y$ is even and $y + z$ is even. To show that $x\,R\,z$ we need to establish that $x + z$ is even. Well,

$$x + z = (x + y) + (y + z) - 2y,$$

and all three terms on the right ($x + y$, $y + z$, and $2y$) are even. Therefore, $x + z$ is even and so $x\,R\,z$.

Example 6.5. Let X be the set of $n \times n$ real matrices. Define a relation $\sim$ on X by:

$$M \sim N \iff \exists r, s \in \mathbb{N} \text{ such that } M^r = N^s.$$

Then $\sim$ is an equivalence relation.

Reflexivity and symmetry are easy to see: $M^1 = M^1$ and, if $M^r = N^s$, then $N^s = M^r$. Proving transitivity requires more work. Suppose $M \sim N$ and $N \sim R$. Then there are $r, s, t, u \in \mathbb{N}$ with $M^r = N^s$ and $N^t = R^u$. Then

$$M^{rt} = (M^r)^t = (N^s)^t = (N^t)^s = (R^u)^s = R^{us},$$

so there are integers $w = rt$ and $x = us$ such that $M^w = R^x$ and hence $M \sim R$.

Example 6.6. Let S be a set of people in a given social network, and let F be the relation 'friendship', i.e. aFb if a and b are people in S who are friends in the social network. This relation is symmetric (in real life, it might be that a says they are friends with b but b disagrees. Social networks such as Facebook don't allow this one-sided 'friendship'). Let's say that you are automatically a friend of yourself, so the relation is reflexive.

Is the relation transitive? Well, that depends on the social network. You probably want to say 'No', because (if you're on Facebook) you surely have some friend not all of whose friends you know. So for the example of S and F coming from Facebook, you know the relation F is not transitive; you have a counterexample—and hence it's also not an equivalence relation. But it doesn't have to be that way. If S is all the people in this lecture hall—well, we're all friends (I hope!) and so from the lecture example we do get a transitive relation, and hence (because we checked all three properties) an equivalence relation.

6.3 Rational numbers

You know $\frac{1}{7}$ and $\frac{2}{14}$ are the same fraction. But why? If you plug both into your calculator, then you'll get the same sequence of digits on the display—but this is only part of a complicated infinite sequence of digits; maybe they are different somewhere later off your screen? The answer is something like 'because you can cancel twos'. How can we make that formal?

6.3.1 An important equivalence relation

Rational numbers are simply the fractions you already studied in primary school. You'll certainly be aware that there are many ways of representing a given rational number. For instance, $\frac{2}{5}$ represents the same number as $\frac{4}{10}$. We can capture these sorts of equivalences more formally by using an equivalence relation on pairs of integers (m,n), where $n \neq 0$. So let $X = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ be the set of all pairs (m,n) where $m,n \in \mathbb{Z}$ and $n \neq 0$, and define a relation Q on X by:

$$(m,n)\,Q\,(m',n') \iff mn' = m'n.$$

You should quickly check that this relation Q does what you think it should do: if (by your school-style calculation) the fractions $\frac{m}{n}$ and $\frac{m'}{n'}$ are the same, then indeed we have $(m,n)Q(m',n')$. However so far in this course we did not define 'division' nor 'fraction'—that's exactly what we want to do now. The relation Q only uses the properties of $\mathbb{Z}$ which we are already happy with.

Let's prove that Q is indeed an equivalence relation.

Q **is Reflexive:** $(m,n)Q(m,n)$ because $mn = nm$.

Q **is Symmetric:** $(m,n)Q(p,q)$ means $mq = np$. Rearranging we get $pn = qm$, which by definition is the same as $(p,q)Q(m,n)$.

Q **is Transitive:** Suppose $(m,n)Q(p,q)$ and $(p,q)Q(s,t)$. Then $mq = np$ and $pt = qs$. So, $(mq)(pt) = (np)(qs)$ and, after cancelling qp, this gives $mt = ns$, so $(m,n)Q(s,t)$.
But, wait a minute: can we cancel pq? Sure, if it's nonzero. If it *is* zero then that means $p = 0$ (since we know that $q \neq 0$). But then $mq = 0$, so $m = 0$; and $qs = 0$, so $s = 0$. So, in this case also we get $mt = ns$ (both sides are zero) and so $(m,n)Q(s,t)$.

Where we are now is: we can think of a fraction $\frac{a}{b}$ as being the same thing as a pair (a,b) in X, and we have formalised that two fractions are 'the same number' if they are related by Q.

A natural thing to think about at this point is 'all the fractions which represent 0.5'. This is the same thing as: all the pairs $(m,n)\in X$ such that $(m,n)Q(1,2)$. And it would be natural to think about the set we get: $\{(m,n)\in X : (m,n)Q(1,2)\}$. In fact, this is such a natural thing to think about, we give it a name and notation: this is the *equivalence class* of $(1,2)$,

$$\big[(1,2)\big]_Q = \big\{(m,n)\in X : (m,n)Q(1,2)\big\}.$$

This is a nice way to avoid 'the problem with fractions' that there are lots of different ways to write the same fraction: when we write $\frac{1}{2}$, or $\frac{-2}{-4}$, or any other representation, we can think that what we really mean is the equivalence class $[(1,2)]_Q$; it turns out that $[(1,2)]_Q$ is the same set as $[(-2,-4)]_Q$. The other nice thing is that we started this section with integers, and we found a way to talk about fractions: this is called *constructing* the fractions.

We will return to this topic in Winter Term, formally define equivalence classes, and (among other things) prove the above statement. In particular, we will see how to use equivalence relations to construct new number systems from old ones. You're already totally familiar with $\mathbb{Q}$ and maybe don't see the point of formally constructing it: but we will also see how to construct number systems that you have not seen before, called modular arithmetic (and in future courses we will return to constructions too).

You might ask why you should care about some new number system. In classes earlier, we saw that there is no integer n such that n^2+5 is divisible by 13, and the proof was both fairly painful to write down and hard to come up with. Once you learn modular arithmetic, you'll both see a much easier way to write the proof down and a way to think that makes the proof completely obvious.

6.4 Sample exercises

Exercise 6.1. *Define a relation R on $\mathbb{Z}$ by: for $x,y\in\mathbb{Z}$, $x\,R\,y \iff x^2=y^2$. Prove that R is an equivalence relation.*

Exercise 6.2. *Define the relation R on the set $\mathbb{N}$ by $x\,R\,y$ if and only if there is some $n\in\mathbb{Z}$ such that $x=2^n y$. Prove that R is an equivalence relation.*

Exercise 6.3. *Let X be the set of $n\times n$ real matrices. Define a relation $\sim$ on X by:*

$$M\sim N \iff \exists \text{ an invertible } P\in X \text{ s.t. } N=P^{-1}MP.$$

Prove that $\sim$ is an equivalence relation.

Exercise 6.4. *Let $f:X\to Y$ be a function. Define the relation R on X by $x\,R\,y \iff f(x)=f(y)$. Prove that R is an equivalence relation.*

6.5 Solutions to exercises

Solution to Exercise 6.1. R is reflexive because for any x, $x^2 = x^2$. R is symmetric because $x^2 = y^2 \iff y^2 = x^2$. To show R is transitive, suppose $x, y, z \in \mathbb{Z}$ and $x\,R\,y$ and $y\,R\,z$. Then $x^2 = y^2$ and $y^2 = z^2$, so $x^2 = z^2$, which means $x\,R\,z$. Thus R is an equivalence relation.

Solution to Exercise 6.2. R is reflexive because for any x, $x = 2^0 x$. R is symmetric because if $x\,R\,y$ then $\exists n \in \mathbb{Z}$ with $x = 2^n y$. This means that $y = 2^{-n}x$ and hence, taking $m = -n$, $\exists m \in \mathbb{Z}$ such that $y = 2^m x$. So $y\,R\,x$. To show R is transitive, suppose $x, y, z \in \mathbb{Z}$ and $x\,R\,y$ and $y\,R\,z$. Then there are $m, n \in \mathbb{Z}$ such that $x = 2^n y$ and $y = 2^m z$, so $x = 2^n y = 2^n(2^m z) = 2^{m+n} z$ which, since $m + n \in \mathbb{Z}$, shows that $x\,R\,z$. Thus R is an equivalence relation.

Solution to Exercise 6.3. For any M, $M = I^{-1}MI$ where I is the identity matrix, so $M \sim M$. For matrices $M, N \in X$, if $M \sim N$ then there's an invertible P with $N = P^{-1}MP$ and so $M = PNP^{-1}$, which can be written as $M = (P^{-1})^{-1}MP^{-1}$. So there is an invertible matrix Q (equal to P^{-1}) such that $M = Q^{-1}NQ$ and hence $M \sim N$. This shows the relation is symmetric. Suppose $M \sim N$ and $N \sim R$. Then there are invertible matrices P and Q such that $N = P^{-1}MP$ and $R = Q^{-1}NQ$. We therefore have

$$R = Q^{-1}(P^{-1}MP)Q = (Q^{-1}P^{-1})M(PQ) = (PQ)^{-1}M(PQ),$$

so there is an invertible matrix $T = PQ$ so that $R = T^{-1}MT$ and hence $M \sim R$, establishing that $\sim$ is transitive. It follows that $\sim$ is an equivalence relation. (We used here the fact that $(PQ)^{-1} = Q^{-1}P^{-1}$. This follows from the fact that $(Q^{-1}P^{-1})(PQ) = Q^{-1}(P^{-1}P)Q = Q^{-1}IQ = Q^{-1}Q = I$.)

Solution to Exercise 6.4. $x\,R\,x$ because $f(x) = f(x)$. If $x\,R\,y$ then $f(x) = f(y)$ so $f(y) = f(x)$ and hence $y\,R\,x$. If $x\,R\,y$ and $y\,R\,z$ then $f(x) = f(y)$ and $f(y) = f(z)$, so $f(x) = f(z)$ and $x\,R\,z$. Hence R is an equivalence relation.

7 Real and complex numbers

The material in this chapter is also covered in:

- Biggs, N. L. *Discrete Mathematics.* Chapter 9.
- Eccles, P.J. *An Introduction to Mathematical Reasoning.* Chapters 13 and 14.

The treatment in Biggs is probably better for the purposes of this course.

Neither of these books covers complex numbers. You do not have to know very much about complex numbers for this course, but because this topic is not in these books, I have included quite a bit of material on complex numbers in this chapter.

You can find useful reading on complex numbers in a number of books, including the following (which you might already have, given that it is the MA100 text).

- Anthony, M. and M. Harvey. *Linear Algebra: Concepts and Methods.* Cambridge University Press 2012. Chapter 13.

7.1 Introduction

In this chapter, we explore real numbers and complex numbers.

We are going to stick, mainly, to your intuition and what you already know about numbers from school—which means we are not going to formally construct the real numbers.

7.2 Rational numbers and real numbers

So far, you probably never really saw a need for numbers which are not rational. You can add, subtract, multiply and divide rational numbers and you always get a rational number—why do we need more?

Theorem 7.1. *The real number $\sqrt{2}$ is irrational. That is, there are no positive integers m, n with $\left(\frac{m}{n}\right)^2 = 2$.*

Proof. Suppose, for a contradiction, that there were such m, n.

If m, n are divisible by some $d > 1$, we may divide both m and n to obtain m', n' such that the rational number m'/n' equals m/n. So we may assume that m, n have no common divisors greater than 1. In particular, we can assume that they are not both divisible by 2.

Now, the equation $(m/n)^2 = 2$ means $m^2 = 2n^2$. So we see that m^2 is even. We know (from Chapter 2) that this means m must be even. So there is some m_1 such that $m = 2m_1$. Then,

$m^2 = 2n^2$ becomes $4m_1^2 = 2n^2$, and so $n^2 = 2m_1^2$. Well, this means n^2 is even and hence n must be even. So m and n are both divisible by 2. But this is a contradiction; we just said we can assume they are *not* both divisible by 2.

So our assumption that $(m/n)^2 = 2$ must have been wrong and we can deduce no such integers m and n exist. □

Isn't this theorem a thing of beauty?

Activity 7.1. *Make sure you understand that this is a proof by contradiction, and that you understand what the contradiction is.*

What this theorem tells us is that, at least if we want to solve equations like $x^2 = 2$, then the rational numbers are not enough; we need more. Of course, we could just invent new symbols and define them to satisfy the equations we want. But this is a dangerous thing to do—we might be assuming something exists which doesn't in fact exist; whose existence leads to a contradiction. We'd better rather construct the reals.

7.2.1 Non-examinable: what are the real numbers exactly?

There is a simple way to define the real numbers, which you already saw in school. We just say that these are all the things you can get by writing down a decimal number: 123.4124581... for example. Except that we say 0.9999 and 1.000 are to be considered the same (and similarly for any other decimal which after some point consists only of nines). How do we formalise that?

Well, it's easy enough; we can write a decimal as consisting of (for example) an integer n together with a string of digits after the decimal: $(123, 4, 1, 2, 4, 5, 8, 1, ...)$. This is a member of the set $\mathbb{N} \times \{0, 1, \dots, 9\} \times \{0, 1, \dots, 9\} \times \dots$. (There's nothing wrong with an infinite product of sets.) And we can easily write down an equivalence relation which says that $(n, a_1, a_2, \dots, a_k, 9, 9, 9, \dots)$ is equivalent to $(n, a_1, a_2, \dots, a_k{+}1, 0, 0, 0, \dots)$ (whenever a_k is not 9); and the relation is reflexive—we just did it. The real numbers are then the equivalence classes of this relation. (We didn't really go in to equivalence classes in the last chapter, but you don't need to know more than we did. If you want to think harder about this non-examinable subsection, you should probably wait till the first few weeks of Winter Term.)

It is a pain to define addition and multiplication formally. It is *not* hard, it is just annoying. You simply write out the details of how you would in practice add or multiply two numbers by hand (as you learnt to do in primary school). It's not hard, but it is painful, to check that it doesn't matter which representative of an equivalence class you take.

But there is something a bit worrying about this definition: it depends on the fact that we do arithmetic in base 10. Maybe the Martians (who have six fingers, at least in the B-movies I watch) will have a different set of real numbers? That would be terrible—they would certainly attack us if they found out. And in any case, it's not even obvious this definition fixes the problem—is there a decimal whose square is equal to 2?

In fact, these concerns turn out not to be real problems. It doesn't make a difference what base you use, and there is such a decimal. But nevertheless, mathematicians tend to prefer one of two different constructions. These two constructions are really different; depending on what you want one or the other might look 'better', and some mathematicians will get very angry if you don't like their favourite construction. However—and we will *not* prove it!—it doesn't really make a difference which construction you use; you still get a set which behaves the way you think the real numbers should.

The first way is called the 'Dedekind cut' construction.

The idea is the following: if I pick a point on the number line, intuitively it separates the number line into the smaller points and the points at least as large. I can't really make formal sense of that idea—it's recursive: I'm talking about the number line in order to define the number line. But I can also talk about separating the fractions into two sets, and I know how to work with those. Formalising this, I can say a set S of rational numbers is a Dedekind cut if for every rational number x, either x is in S and there is an element s of S which is larger than x, or alternatively x is larger than all elements of S. And then I can say a real number is the same thing as a Dedekind cut. I can easily define addition: it's not hard to check that if S and S' are Dedekind cuts, then the set $\{s + s' : s \in S, s' \in S'\}$ is a Dedekind cut. More or less the same idea works for multiplication (but you have to be rather careful with negative numbers!). If q is a rational number, then $\{x \in \mathbb{Q} : x < q\}$ is a Dedekind cut which we can easily check behaves like the rational number q (in the same way that the rational number $\frac{2}{1}$ behaves like the integer 2). Now, this definition at least solves the $\sqrt{2}$ problem: $\{q \in \mathbb{Q} : q < 0 \text{ or } q^2 < 2\}$ is a Dedekind cut, and its square is 2. This is a nice clean definition, but it only works because we have a definition of 'order' $<$ on $\mathbb{Q}$.

The second route is the 'Cauchy sequence' construction. This is rather more complicated.

The idea is the following: if I want to specify a real number, I'll give a sequence of rational numbers which get closer and closer to the number I want (the formal term is 'Cauchy sequence'; it'll be defined later), such as longer and longer parts of the decimal expansion of $\sqrt{2}$; I might give the sequence

$$(1, 1.4, 1.41, 1.414, ...) .$$

It's easy to add such sequences—I just add the terms:

$$(a_1, a_2, a_3, ...) + (b_1, b_2, b_3, ...) = (a_1 + b_1, a_2 + b_2, a_3 + b_3, ...) .$$

Multiplication works similarly (this time negative numbers aren't a problem). So far this looks rather like the 'decimals' construction. But of course I might have many possible sequences of rational numbers which get closer and closer to say 0 (or any other real number), so I should write down an equivalence relation which says two such sequences are equivalent. And then the real numbers are the equivalence classes of this relation.

By the end of this term, you will have studied sequences in sufficient detail to make sense of this 'Cauchy sequence' construction, and prove that it really works. It's worth trying—this is fairly hard work, but it is also a good test of the Analysis you'll learn.

7.2.2 Real numbers: a 'sketchy' introduction

For the time being, you can just think of the real numbers $\mathbb{R}$ as given; they are all the points on the number line, or equivalently they are all the decimal numbers (bearing in mind that 0.4999... = 0.5000...). Let's think for a bit about these decimals, and (again a little bit informally) let's write down some properties they have.

First, let's note that if $a_0 \in \mathbb{N} \cup \{0\}$ and $a_i \leq 9$ for $1 \leq i \leq n$, then the (finite) decimal expansion

$$a_0.a_1a_2\dots a_n$$

represents the rational number

$$a_0 + \frac{a_1}{10} + \frac{a_2}{(10)^2} + \dots + \frac{a_n}{(10)^n}.$$

For example, what we mean by 1.2546 is the number

$$1+\frac{2}{10}+\frac{5}{100}+\frac{4}{1000}+\frac{6}{10000}.$$

Every positive real number can be represented by an infinite decimal expansion

$$a_0.a_1a_2a_3\dots a_i\dots,$$

where $a_i \in \mathbb{N} \cup \{0\}$ and $a_i \leq 9$ for $i \geq 1$. We allow for a_i to be 0, so, in particular, it is possible that $a_i = 0$ for all $i \geq N$ where N is some fixed number: such an expansion is known as a *terminating* expansion. Given such an infinite decimal expansion, we say that it represents a real number a if, for all $n \in \mathbb{N} \cup \{0\}$,

$$a_0.a_1a_2\dots a_n \leq a \leq a_0.a_1a_2\dots a_n + 1/(10)^n.$$

This formalism allows us to see that the infinite decimal expansion 0.99999..., all of whose digits after the decimal point are 9, is in fact the same as the number 1.0000000....

For example, two infinite decimal expansions are

$$3.1415926535\dots$$

and

$$0.1833333333333\dots.$$

(You'll probably recognise the first as being the number π.) Suppose, in this second decimal expansion, that every digit is 3 after the first three (that is, $a_i = 3$ for $i \geq 3$). Then we write this as $0.18\overline{3}$ (or, in some texts, $0.18\dot{3}$). We can extend this notation to cases in which there is a repeating pattern of digits. For example, suppose we have

$$0.1123123123123\dots,$$

where the '123' repeats infinitely. Then we denote this by $0.1\overline{123}$.

7.2.3 Rationality and repeating patterns

You probably have heard stories of strange, obsessive mathematicians working out the expansion of π to millions and millions of decimal places. (This has been the subject of a novel, a play, a film, and a song!) This is relevant because the digits of π have no repeating pattern, which you might think quite remarkable. In fact, it turns out that a real number will have an infinitely repeating pattern in its decimal expansion (which includes the case in which the pattern is 0, so that it includes terminating expansions) *if and only if* the number is rational.

Let's look at part of this statement: if a number is rational, then its decimal expansion will have a repeating pattern (which might be 0). Let's look at an example.

Example 7.2. We find the decimal expansion of 4/7 by long division.

$$
\begin{array}{rl}
 & 0.5714285\cdots \\
7 & \overline{\big)4.0000000} \\
 & \underline{3.5} \\
 & .50 \\
 & \underline{.49} \\
 & 10 \\
 & \underline{7} \\
 & 30 \\
 & \underline{28} \\
 & 20 \\
 & \underline{14} \\
 & 60 \\
 & \underline{56} \\
 & 40 \\
 & \underline{35} \\
 & 50
\end{array}
$$

So,

$$4/7 = 0.\overline{571428}.$$

Notice: we must have the same remainder re-appear at some point, and then the calculation repeats. Here's the calculation again, with the repeating remainder highlighted.

$$
\begin{array}{rl}
 & 0.5714285\cdots \\
7 & \overline{\big)4.0000000} \\
 & \underline{3.5} \\
 & .{\color{red}\mathbf{5}}0 \\
 & \underline{.49} \\
 & 10 \\
 & \underline{7} \\
 & 30 \\
 & \underline{28} \\
 & 20 \\
 & \underline{14} \\
 & 60 \\
 & \underline{56} \\
 & 40 \\
 & \underline{35} \\
 & {\color{red}\mathbf{5}}0
\end{array}
$$

We can formalise this very easily:

Theorem 7.3. *If $\frac{p}{q} = a_0 \cdot a_1 a_2 a_3 \dots$ in decimal, where p and $q > 0$ are integers, then there exist some natural numbers N and k such that for each $n \geq N$ we have $a_{n+k} = a_n$.*

The idea here is that the first few digits might not fit the 'repeating pattern' (as is the case for, for example, $\frac{1}{6} = 0.16666....$) but from digit N onwards, the repeating pattern starts, and the length of the repeating block of digits is k.

Rather than just jumping into a proof of this theorem, let's think about how we can get to it. This is about the right level of difficulty for a (moderately hard) exam question (or it would be if it wasn't in the notes..!) and so you might want to close the notes for a while and try to solve it yourself.

We've seen in an example how we get to a repeating pattern. When we do long division to work out $\frac{4}{7}$ as a decimal, at some point the remainder repeats and after that point the calculation will repeat forever. Maybe the same statement is true if we replace $\frac{4}{7}$ by $\frac{p}{q}$? Then we would be done.

So we have two things to prove. First, *at some point the remainder repeats.* Second, *after that point the calculation repeats forever.*

Why should the remainder repeat at some point? Intuitively, this is almost obvious. The remainder on division by q is an integer between 0 and $q-1$ inclusive. There are q such integers, so after at most $q+1$ steps we surely have to repeat. That is not quite a formal proof, but 'once we have more steps than possible remainders we have to repeat' should sound like a special case of something you know. That something is the Pigeonhole Principle, so we should be using the Pigeonhole Principle. In order to avoid talking about 'the first remainder', it will help to give it a name. Let's say that r_1 is the first remainder, i.e. when we try to divide p by q, we get the quotient a_0 and remainder r_1. Then r_2 is the second remainder; when we try to divide $10r_1$ by q, we get the quotient a_1 and remainder r_2, and so on. The Pigeonhole Principle should tell us that there exist N and k such that $r_N = r_{N+k}$.

Why does the calculation repeat from this point? Again, this is almost obvious. We know that a_N is the quotient when we try to divide $10r_N$ by q, and r_{N+1} is the remainder. And we know that a_{N+k} is the quotient when we try to divide $10r_{N+k}$ by q, and r_{N+k+1} is the remainder. But that is the same calculation, so $a_N = a_{N+k}$ and $r_{N+1} = r_{N+k+1}$.

Well, now we know that $r_{N+1} = r_{N_k+1}$, we can use exactly the same argument to show $a_{N+1} = a_{N+k+1}$ and $r_{N+2} = r_{N+k+2}$. And so on... in other words, this is an induction with base case N.

Let's write that formally.

Proof. We define two sequences recursively. We let a_0 be the quotient when we try to divide p by q, and r_1 be the remainder. Then, for each integer $i \geq 1$, we let a_i be the quotient when we try to divide $10a_i$ by q, and r_{i+1} be the remainder.

Since each r_i is an integer such that $0 \leq r_i \leq q-1$, we can define a function f from $\{1, 2, \dots, q+1\}$ to $\{0, 1, \dots, q-1\}$ by setting $f(i) = r_i$. Since the domain is larger than the codomain, by the Pigeonhole Principle there exist $i, j \in \{1, 2, \dots, q+1\}$ which are distinct such that $f(i) = f(j)$. Suppose that $i < j$, and define $N = i$ and $k = j - i$. Then $f(N) = f(N+k)$, i.e. $r_N = r_{N+k}$.

We now try to prove by induction that for each $n \geq N$ we have the statement $P(n)$, where $P(n)$ is '$a_n = a_{n+k}$ and $r_{n+1} = r_{n+k+1}$'.

The base case is $n = N$. We know a_N is the quotient when we try to divide $10r_N$ by q, and r_{N+1} is the remainder. And we know that a_{N+k} is the quotient when we try to divide $10r_{N+k}$ by q, and r_{N+k+1} is the remainder. Since $10r_N = 10r_{N+k}$, this is the same calculation, so $a_N = a_{N+k}$ and $r_{N+1} = r_{N+k+1}$ as required.

Now let $s \geq N$, and suppose the induction hypothesis $P(s)$ holds. In particular, we have $r_{s+1} = r_{s+k+1}$. We know a_{s+1} is the quotient when we try to divide $10r_{s+1}$ by q, and r_{s+2} is the remainder. And we know that a_{s+k+1} is the quotient when we try to divide $10r_{s+k+1}$ by q, and r_{s+k+2} is the remainder. Since $10r_{s+1} = 10r_{s+k+1}$, this is the same calculation, so $a_{s+1} = a_{s+k+1}$ and $r_{s+2} = r_{s+k+2}$. That is $P(s+1)$, so we proved the induction step. By the Principle of Induction, we have $P(n)$ for all $n \geq N$.

In particular, we have $a_n = a_{n+k}$ for all $n \geq N$, which proves the theorem. □

We're calling it 'obvious' that when we divide p by q in the above, there is only one possible answer for the quotient and remainder. If you're not happy about that—maybe you shouldn't be—you will see a proper proof that this is true in Winter Term.

Next, we think about the second part of the statement: that if the decimal expansion repeats, then the number is rational.

Clearly, if the decimal expansion is terminating, then the number is rational. But what about the infinite, repeating, case? We've given two examples above. Let's consider these in more detail.

Example 7.4. Consider $a = 0.18\overline{3}$. Let $x = 0.00\overline{3}$. Then $10x = 0.0\overline{3}$ and so $10x - x = 0.0\overline{3} - 0.00\overline{3} = 0.03$. So, $9x = 0.03$ and hence $x = (3/100)/9 = 1/300$, so

$$0.18\overline{3} = 0.18 + 0.00\overline{3} = \frac{18}{100} + \frac{1}{300} = \frac{55}{300} = \frac{11}{60},$$

and this is the rational representation of a.

Example 7.5. Consider the number $0.1\overline{123}$. If $x = 0.0\overline{123}$, then $1000x = 12.3\overline{123}$ and $1000x - x = 12.3$. So $999x = 12.3$ and hence $x = 123/9990$. So,

$$0.1\overline{123} = \frac{1}{10} + x = \frac{1}{10} + \frac{123}{9990} = \frac{1122}{9990}.$$

In general, if the repeating block is of length k, then an argument just like the previous two, in which we multiply by 10^k, will enable us to express the number as a rational number.

Activity 7.2. *Formalise this argument.*

7.2.4 Irrational numbers

A real number is *irrational* if it is not a rational number. So, given what we said above, an irrational number has no infinitely repeating pattern in its decimal expansion.

What's clear from above is that any real number can be approximated well by rational numbers: for the rational number $a_0.a_1a_2\dots a_n$ is within $1/(10)^n$ of the real number with infinite decimal expansion $a_0.a_1a_2\dots$.

We can, in some cases, prove that particular numbers are irrational. We already saw that $\sqrt{2}$ is irrational, and in general for any natural number n, either $\sqrt{n}$ is irrational or it is an integer (i.e. it is never a rational number which is not an integer).

Activity 7.3. *Prove that if n is any natural number then either $\sqrt{n}$ is an integer or it is irrational.*

Many other important numbers in mathematics turn out to be irrational. I've already mentioned π, and there is also e (the base of the natural logarithm). It's not easy to prove either of these numbers is irrational.

What about $\pi + e$, or πe? We don't know if those are rational. I think every mathematician believes neither is rational—but we don't know how to prove it in either case. Rather amazingly, though, we do know that *at least one of* $\pi + e$ and πe is irrational.

7.2.5 ‘Density’ of the rational numbers

As we’ve seen, some important numbers in mathematics are not rational. An intuitive question that arises is ‘how many real numbers are rational’ and this is a difficult question to answer. There are infinitely many real numbers and infinitely many rationals, and infinitely many real numbers are not rational. More on this next term!

For the moment, let’s make one important observation: not only are there infinitely many rational numbers, but there are no ‘gaps’ in the rational numbers. If you accept the view of real numbers as (possibly) infinite decimal expansions, then this is quite clear: you can get a very good approximation to any real number by terminating its decimal expansion after a large number of digits. (And we know that a terminating decimal expansion is a rational number.) The following theorem makes sense of the statement that there are no ‘rational-free’ zones in the real numbers. Precisely, between any two rational numbers, no matter how close together they are, there is always another rational number.

Theorem 7.6. *Suppose $q, q' \in \mathbb{Q}$ with $q < q'$. Then there is $r \in \mathbb{Q}$ with $q < r < q'$.*

Proof. Consider $r = (1/2)(q + q')$. Details are left to you! □

Activity 7.4. *Complete this proof.*

7.3 Complex numbers

7.3.1 Introduction

Consider the two quadratic polynomials,

$$p(x) = x^2 - 3x + 2 \qquad \text{and} \qquad q(x) = x^2 + x + 1$$

If you sketch the graph of $p(x)$ you will find that the graph intersects the x-axis at the two real solutions (or roots) of the equation $p(x) = 0$, and that the polynomial factors into the two linear factors,

$$p(x) = x^2 - 3x + 2 = (x - 1)(x - 2)$$

Sketching the graph of $q(x)$, you will find that it does not intersect the x-axis. The equation $q(x) = 0$ has no solution in the real numbers, and it cannot be factorised (or factored) over the reals. Such a polynomial is said to be *irreducible* over the reals. In order to solve this equation, we need to define the complex numbers.

If you met the complex numbers in school, then probably you were told to accept ‘there is a symbol i which means the square root of -1’ and you did arithmetic with it. This isn’t a very satisfactory way of doing things: *why* can we assume there is such a symbol? We could equally well invent a symbol (say E) to be the result of trying to divide 1 by 0 and do arithmetic with it—and if you do, you’ll find you can ‘prove’ $1 = 2$. (Try it!)

What we will do is instead to write down a new number system, explain how to do arithmetic, and then show that we can find a ‘square root of -1’ in this new system.

7.3.2 Complex numbers: a formal approach

To start with, let's formally construct the complex numbers from the real numbers.

We define the set $\mathbb{C}$ of complex numbers to be the set of all ordered pairs (x,y) of real numbers, with addition and multiplication operations defined as follows:

$$(a,b)+(c,d)=(a+c,b+d)\,,\quad (a,b)\times(c,d)=(ac-bd,ad+bc)\,.$$

You should check that these definitions really work, that is, that (for example) the multiplication is commutative, and that the distributive law holds; more generally, that all the usual operations of arithmetic work. Formally, you should check that the complex numbers are a 'field'. (This term hasn't been defined in this course, but you can look it up if you want; it is not very complicated.)

You can also check that the complex numbers of the form $(x,0)$ behave like the real numbers, in other words that $(x,0)+(y,0)=(x+y,0)$, and $(x,0)\times(y,0)=(xy,0)$, which is what you expect for adding and multiplying real numbers. Finally, let's remember why we began this: we wanted to be able to solve the equation $x^2+1=0$. Well, that means we want a complex number (a,b) such that $(a,b)\times(a,b)+(1,0)=(0,0)$. And we can find such a number: $(0,1)\times(0,1)=(-1,0)$, so we are done.

Let's return briefly to the $\frac{1}{0}$ bad example from the last section. Suppose you try to construct a new number system—maybe by taking pairs or triples or whatever of numbers, maybe with some equivalence relation to say when two pairs are 'equivalent' (as we did to construct the rationals). To do arithmetic with your new number system, you need to explain how to add and to multiply, and (if you have some equivalence relation involved) you need to show that the addition and multiplication you wrote down are well-defined. And you would like that there is something like 'subtraction' and 'division' that are inverse operations, and you would like it to be true that addition distributes over multiplication, and so on.

There are in fact lots of things you might come up with that make sense—not just the rational, real and complex numbers—these other things are also fields and they are very important in mathematics (and some of them turn out to be very important in modern technology). What you will *not* find is a field that contains a solution to the equation $0\times x=1$, in the way that the complex numbers we just defined contain a solution to the equation $x^2+1=0$. This is why we cannot invent a symbol $E=\frac{1}{0}$ and do arithmetic with it, but we can invent a symbol $i=\sqrt{-1}$.

7.3.3 Complex numbers: a more usual approach

Rather than the ordered pairs approach outlined above, it is more common to define the complex numbers as follows. We begin by defining the *imaginary* number i which has the property that $i^2=-1$. The term 'imaginary' is historical, and not an indication that this is a figment of someone's imagination—but historically the reason for the name is that some mathematicians didn't believe the complex numbers make sense: 'imaginary' is a term of Descartes, and he meant it as an attack on the idea.

This symbol i is simply a nicer way of writing the pair $(0,1)$ of real numbers; it's easier to write on the board in calculations (in the same way that it's easier to write $\frac{a}{b}$ for the rational rather than the equivalence class $[(a,b)]_R$ of the relation R we defined in Section 6.3.1). We can then say what we mean by the complex numbers.

Definition 7.7. A complex number is a number of the form $z=a+ib$, where a and b are real numbers, and $i^2=-1$. The set of all such numbers is

$$\mathbb{C}=\{a+ib\ :\ a,b\in\mathbb{R}\}\ .$$

If $z = a + ib$ is a complex number, then the real number a is known as the real part of z, denoted $\text{Re}(z)$, and the real number b is the imaginary part of z, denoted $\text{Im}(z)$. Note that $\text{Im}(z)$ is a *real* number.

If $b = 0$, then z is a real number, so $\mathbb{R} \subseteq \mathbb{C}$. If $a = 0$, then z is said to be *purely imaginary.*

The quadratic polynomial $q(z) = x^2 + x + 1$ can be factorised over the complex numbers, because the equation $q(z) = 0$ has two complex solutions. Solving in the usual way, we have

$$x = \frac{-1 \pm \sqrt{-3}}{2}.$$

We write, $\sqrt{-3} = \sqrt{(-1)3} = \sqrt{-1}\ \sqrt{3} = i\sqrt{3}$, so that the solutions are

$$w = -\frac{1}{2} + i\frac{\sqrt{3}}{2} \qquad \text{and} \qquad \overline{w} = -\frac{1}{2} - i\frac{\sqrt{3}}{2}.$$

Notice the form of these two solutions. They are what is called a *conjugate pair.* We have the following definition.

Definition 7.8. If $z = a+ib$ is a complex number, then the *complex conjugate* of z is the complex number $\overline{z} = a - ib$.

We can see by the application of the quadratic formula, that the roots of an irreducible quadratic polynomial with real coefficients will always be a conjugate pair of complex numbers.

Addition, multiplication, division

Addition and *multiplication* of complex numbers are defined as for polynomials in i using $i^2 = -1$.

Example 7.9. If $z = (1 + i)$ and $w = (4 - 2i)$ then

$$z + w = (1 + i) + (4 - 2i) = (1 + 4) + i(1 - 2) = 5 - i$$

and

$$zw = (1 + i)(4 - 2i) = 4 + 4i - 2i - 2i^2 = 6 + 2i$$

You should check that this is really exactly the same as the definitions we gave when we formally constructed the complex numbers: the only difference is the way we're writing complex numbers.

If $z \in \mathbb{C}$, then $z\overline{z}$ is a real number:

$$z\overline{z} = (a + ib)(a - ib) = a^2 + b^2.$$

Activity 7.5. *Carry out the multiplication to verify this: let $z = a + ib$ and calculate $z\overline{z}$.*

Division of complex numbers is then defined by $\dfrac{z}{w} = \dfrac{z\overline{w}}{w\overline{w}}$ since $w\overline{w}$ is real.

Example 7.10.

$$\frac{1+i}{4-2i} = \frac{(1+i)(4+2i)}{(4-2i)(4+2i)} = \frac{2+6i}{16+4} = \frac{1}{10} + \frac{3}{10}i$$

Properties of the complex conjugate

A complex number is real if and only if $z = \overline{z}$. Indeed, if $z = a + ib$, then $z = \overline{z}$ if and only if $b = 0$.

The complex conjugate of a complex number satisfies the following properties:

- $z + \overline{z} = 2\,\mathrm{Re}(z)$ is real
- $z - \overline{z} = 2i\,\mathrm{Im}(z)$ is purely imaginary
- $\overline{\overline{z}} = z$
- $\overline{z + w} = \overline{z} + \overline{w}$
- $\overline{zw} = \overline{z}\,\overline{w}$
- $\overline{\left(\frac{z}{w}\right)} = \frac{\overline{z}}{\overline{w}}$

Activity 7.6. *Let $z = a + ib$, $w = c + id$ and verify all of the above properties.*

7.3.4 Roots of polynomials

Are we really done with construction? We invented the symbol i because we wanted to have a solution to $x^2 + 1 = 0$. But I also want a solution to $x^6 + 10x^2 + 17 = 0$. Do I need a new symbol for that? It turns out the answer is No.

The *Fundamental Theorem of Algebra* asserts that a polynomial of degree n with complex coefficients has n complex roots (not necessarily distinct), and can therefore be factorised into n linear factors. Explicitly, any equation

$$a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0 = 0$$

where $a_i \in \mathbb{C}$ has n solutions $z \in \mathbb{C}$. Contrast this with the difficulty of solving polynomial equations in $\mathbb{R}$. So, the introduction of i enables us to solve **all** polynomial equations: there's no need to introduce anything else. A fancy way of saying this is: 'The field of complex numbers is algebraically closed.'

If the coefficients of the polynomial are restricted to real numbers, the polynomial can be factorised into a product of linear and irreducible quadratic factors over $\mathbb{R}$ and into a product of *linear* factors over $\mathbb{C}$. The proof of the *Fundamental Theorem of Algebra* is beyond the scope of this course (and this time not because it's long and boring, but because it is genuinely quite hard). However, we note the following useful result.

Theorem 7.11. *Complex roots of polynomials with real coefficients appear in conjugate pairs.*

Proof. Let $P(x) = a_0 + a_1 x + \cdots + a_n x^n$, $a_i \in \mathbb{R}$, be a polynomial of degree n. We shall show that if z is a root of $P(x)$, then so is $\overline{z}$.

Let z be a complex number such that $P(z) = 0$, then

$$a_0 + a_1 z + +a_2 z^2 \cdots + a_n z^n = 0$$

Conjugating both sides of this equation,

$$\overline{a_0 + a_1 z + a_2 z^2 + \cdots + a_n z^n} = \overline{0} = 0$$

Since 0 is a real number, it is equal to its complex conjugate. We now use the properties of the complex conjugate: that the complex conjugate of the sum is the sum of the conjugates, and the same is true for the product of complex numbers. We have

$$\overline{a_0} + \overline{a_1 z} + \overline{a_2 z^2} + \cdots + \overline{a_n z^n} = 0,$$

and

$$\overline{a}_0 + \overline{a}_1\overline{z} + \overline{a}_2\overline{z}^2 + \cdots + \overline{a}_n\overline{z}^n = 0.$$

Since the coefficients a_i are real numbers, this becomes

$$a_0 + a_1\overline{z} + a_2\overline{z}^2 + \cdots + a_n\overline{z}^n = 0.$$

That is, $P(\overline{z}) = 0$, so the number $\overline{z}$ is also a root of $P(x)$. □

Example 7.12. Let us consider the polynomial

$$x^3 - 2x^2 - 2x - 3 = (x-3)(x^2+x+1).$$

If $w = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, then

$$x^3 - 2x^2 - 2x - 3 = (x-3)(x-w)(x-\overline{w})$$

Activity 7.7. *Multiply out the last two factors above to check that their product is the irreducible quadratic $x^2 + x + 1$.*

7.3.5 The complex plane

The following theorem shows that a complex number is uniquely determined by its real and imaginary parts.

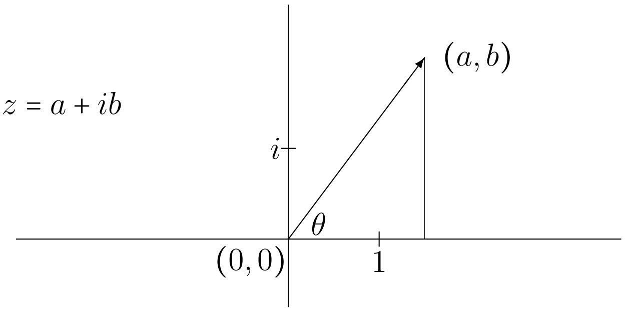
Theorem 7.13. *Two complex numbers are equal if and only if their real and imaginary parts are equal.*

There are two ways to prove this. We can do it directly, using the fact that the complex numbers are a field:

Proof. Two complex numbers with the same real parts and the same imaginary parts are clearly the same complex number, so we only need to prove this statement in one direction. Let $z = a+ib$ and $w = c+id$. If $z = w$, we will show that their real and imaginary parts are equal. We have $a+ib = c+id$, therefore $a-c = i(d-b)$. Squaring both sides, we obtain $(a-c)^2 = i^2(d-b)^2 = -(d-b)^2$. But $a-c$ and $(d-b)$ are real numbers, so their squares are non-negative. The only way this equality can hold is for $a-c = d-b = 0$. That is, $a = c$ and $b = d$. □

The other, much shorter (by now!) way to prove this is simply to observe that the complex numbers are the same as pairs of real numbers (with addition and multiplication as we defined them when we formally constructed the complex numbers) and pairs of real numbers are by definition equal if and only if both parts—which are precisely the real and imaginary parts—are equal.

As a result of this theorem, we can think of the complex numbers geometrically, as points in a plane. For, we can associate the vector $\binom{a}{b}$ uniquely to each complex number $z = a+ib$, and all the properties of a two-dimensional real vector space apply. A complex number $z = a+ib$ is represented as a point (a,b) in the complex plane; we draw two axes, a horizontal axis to represent the real parts of complex numbers, and a vertical axis to represent the imaginary parts of complex numbers. Points on the horizontal axis represent real numbers, and points on the vertical axis represent purely imaginary numbers.



Complex plane or Argand diagram

Activity 7.8. *Plot* $z = 2 + 2i$ *and* $w = 1 - i\sqrt{3}$ *in the complex plane.*

7.3.6 Polar form of z

If the complex number $z = a + ib$ is plotted as a point (a, b) in the complex plane, then we can determine the polar coordinates of this point. We have

$$a = r\cos\theta, \quad b = r\sin\theta$$

where $r = \sqrt{a^2 + b^2}$ is the length of the line joining the origin to the point (a, b) and θ is the angle measured anticlockwise from the real (horizontal) axis to the line joining the origin to the point (a, b). Then we can write $z = a + ib = r\cos\theta + i\,r\sin\theta$.

Definition 7.14. The *polar form* of the complex number z is

$$z = r(\cos\theta + i\sin\theta).$$

The length $r = \sqrt{a^2 + b^2}$ is called the *modulus* of z, denoted $|z|$, and the angle θ is called the *argument* of z.

Note the following properties:

- z and $\overline{z}$ are reflections in the real axis. If θ is the argument of z, then $-\theta$ is the argument of $\overline{z}$.
- $|z|^2 = z\overline{z}$.
- θ and $\theta + 2n\pi$ give the same complex number.

We define the *principal argument* of z to be the argument in the range, $-\pi < \theta \leq \pi$.

Activity 7.9. *Express* $z = 2 + 2i$, $w = 1 - i\sqrt{3}$ *in polar form.*
Describe the following sets of z*: (a)* $|z| = 3$*, (b) argument of* z *is* $\frac{\pi}{4}$.

Multiplication and division using polar coordinates gives

$$\begin{aligned} zw &= r(\cos\theta + i\sin\theta)\cdot\rho(\cos\phi + i\sin\phi) \\ &= r\rho(\cos(\theta+\phi) + i\sin(\theta+\phi)) \end{aligned}$$

$$\frac{z}{w} = \frac{r}{\rho}\Big(\cos(\theta-\phi) + i\sin(\theta-\phi)\Big)$$

Activity 7.10. *Show these by performing the multiplication and the division as defined earlier, and by using the facts that* $\cos(\theta+\phi) = \cos\theta\cos\phi - \sin\theta\sin\phi$ *and* $\sin(\theta+\phi) = \sin\theta\cos\phi + \cos\theta\sin\phi$.

DeMoivre's Theorem

We can consider explictly a special case of the multiplication result above, in which $w = z$. If we apply the multiplication to $z^2 = zz$, we have

$$\begin{aligned} z^2 &= zz \\ &= (r(\cos\theta + i\sin\theta))(r(\cos\theta + i\sin\theta)) \\ &= r^2(\cos^2\theta + i^2\sin^2\theta + 2i\sin\theta\cos\theta) \\ &= r^2(\cos^2\theta - \sin^2\theta + 2i\sin\theta\cos\theta) \\ &= r^2(\cos 2\theta + i\sin 2\theta). \end{aligned}$$

Here we have used the double angle formulae for $\cos 2\theta$ and $\sin 2\theta$.

Applying the product rule n times, where n is a positive integer, we obtain *DeMoivre's Formula*

Theorem 7.15.

$$(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta$$

Proof.

$$\begin{aligned} z^n &= \underbrace{z\cdots z}_{n\text{ times}} = \big(r(\cos\theta + i\sin\theta)\big)^n \\ &= r^n\Big(\cos(\underbrace{\theta + \cdots + \theta}_{n\text{ times}}) + i\sin(\underbrace{\theta + \cdots + \theta}_{n\text{ times}})\Big) \end{aligned}$$

□

7.3.7 Exponential form of z

Functions of complex numbers can be defined by the power series (Taylor expansions) of the functions:

$$e^z = 1 + z + \frac{z^2}{2!} + \frac{z^3}{3!} + \cdots \qquad z \in \mathbb{C}$$

$$\sin z = z - \frac{z^3}{3!} + \frac{z^5}{5!} - \cdots \qquad \cos z = 1 - \frac{z^2}{2!} + \frac{z^4}{4!} - \cdots$$

If we use the expansion for e^z to expand $e^{i\theta}$, and then factor out the real and imaginary parts, we find:

$$\begin{aligned} e^{i\theta} &= 1 + (i\theta) + \frac{(i\theta)^2}{2!} + \frac{(i\theta)^3}{3!} + \frac{(i\theta)^4}{4!} + \frac{(i\theta)^5}{5!} + \cdots \\ &= 1 + i\theta - \frac{\theta^2}{2!} - i\frac{\theta^3}{3!} + \frac{\theta^4}{4!} + i\frac{\theta^5}{5!} - \cdots \\ &= \left(1 - \frac{\theta^2}{2!} + \frac{\theta^4}{4!} - \cdots\right) + i\left(\theta - \frac{\theta^3}{3} + \frac{\theta^5}{5!} - \cdots\right) \end{aligned}$$

From which we conclude:

Euler's Formula: $e^{i\theta} = \cos\theta + i\sin\theta$

If you're being careful, you might notice something a bit strange here—what exactly do I mean by these funny infinite sums? and why am I allowed to rearrange the terms in them?

Sure, I know addition is commutative, but that will only let me change places of *finitely* many terms in the sum (which I don't quite understand anyway), and I still have infinitely many more things which I need to change places. The answer to *that* objection is: we'll explain properly some of it later this term, and some next year in MA203 Real Analysis. For now, take it on faith that it does actually make sense.

Definition 7.16. The *exponential form* of a complex number $z = a + ib$ is

$$z = re^{i\theta}$$

where $r = |z|$ is the modulus of z and θ is the argument of z.

In particular, the following equality is of note because it combines the numbers e, π and i in a single expression: $e^{i\pi} = -1$.

If $z = re^{i\theta}$, then its complex conjugate is given by $\overline{z} = re^{-i\theta}$. This is because, if $z = re^{i\theta} = r(\cos\theta + i\sin\theta)$, then

$$\overline{z} = r(\cos\theta - i\sin\theta) = r(\cos(-\theta) + i\sin(-\theta)) = re^{-i\theta}.$$

We can use either the exponential form, $z = re^{i\theta}$, or the standard form, $z = a + ib$, according to the application or computation we are doing. For example, addition is simplest in the form $z = a + ib$, but multiplication and division are simpler in exponential form. To change a complex number between $re^{i\theta}$ and $a + ib$, use Euler's formula and the complex plane (polar form).

Example 7.17.

$$e^{i\frac{2\pi}{3}} = \cos\tfrac{2\pi}{3} + i\sin\tfrac{2\pi}{3} = -\tfrac{1}{2} + i\tfrac{\sqrt{3}}{2}.$$

$$e^{2+i\sqrt{3}} = e^2 e^{i\sqrt{3}} = e^2\cos\sqrt{3} + ie^2\sin\sqrt{3}.$$

Activity 7.11. *Write each of the following complex numbers in the form $a + ib$:*

$$e^{i\frac{\pi}{2}} \qquad e^{i\frac{3\pi}{2}} \qquad e^{i\frac{3\pi}{4}} \qquad e^{i\frac{11\pi}{3}} \qquad e^{1+i} \qquad e^{-1}$$

Example 7.18. Let $z = 2 + 2i = 2\sqrt{2}\,e^{i\frac{\pi}{4}}$ and $w = 1 - i\sqrt{3} = 2e^{-i\frac{\pi}{3}}$, then

$$w^6 = (1 - i\sqrt{3})^6 = (2e^{-i\frac{\pi}{3}})^6 = 2^6 e^{-i2\pi} = 64$$

$$zw = (2\sqrt{2}e^{i\frac{\pi}{4}})(2e^{-i\frac{\pi}{3}}) = 4\sqrt{2}e^{-i\frac{\pi}{12}}$$

and

$$\frac{z}{w} = \sqrt{2}e^{i\frac{7\pi}{12}}.$$

Notice that in the above example we are using certain properties of the complex exponential function, that if $z, w \in \mathbb{C}$,

$$e^{z+w} = e^z e^w \qquad \text{and} \qquad (e^z)^n = e^{nz} \quad \text{for } n \in \mathbb{Z}.$$

This last property is easily generalised to include the negative integers.

Example 7.19. Solve the equation $z^6 = -1$ to find the 6th roots of -1.

Write $z^6 = (re^{i\theta})^6 = r^6 e^{i6\theta}$, $\quad -1 = e^{i\pi} = e^{i(\pi+2n\pi)}$

Equating these two expressions, and using the fact that r is a real positive number, we have

$$r = 1 \qquad 6\theta = \pi + 2n\pi, \quad \theta = \frac{\pi}{6} + \frac{2n\pi}{6}$$

This will give the six complex roots by taking $n = 0, 1, 2, 3, 4, 5$.

Activity 7.12. *Show this. Write down the six roots of -1 and show that any one raised to the power 6 is equal to -1. Show that $n = 6$ gives the same root as $n = 0$.*

Use this to factor the polynomial $x^6 + 1$ into linear factors over the complex numbers and into irreducible quadratics over the real numbers.

7.4 Sample exercises

Exercise 7.1. *Prove that* $\sqrt{5}$ *is irrational.*

Exercise 7.2. *Express the complex number* $\dfrac{1+2i}{4-5i}$ *in the form* $a+bi$.

Exercise 7.3. *Solve the equation* $x^2-2ix+3=0$.

Exercise 7.4. *Write each of the following complex numbers in the form* $a+ib$*:*

$$e^{i\frac{\pi}{2}} \qquad e^{i\frac{3\pi}{2}} \qquad e^{i\frac{3\pi}{4}} \qquad e^{i\frac{11\pi}{3}} \qquad e^{1+i} \qquad e^{-1}.$$

Exercise 7.5. *Express* $1+\sqrt{3}i$ *in exponential form. Hence find* $(1+\sqrt{3}i)^{30}$.

7.5 Comments on selected activities

Comment on Activity 7.3. The obvious thing to do is to try mimicking the proof that $\sqrt{2}$ is irrational. So let's try. Suppose for a contradiction that there are integers a and b such that $\left(\frac{a}{b}\right)^2 = n$. As before, we can assume n does not divide both a and b. We get

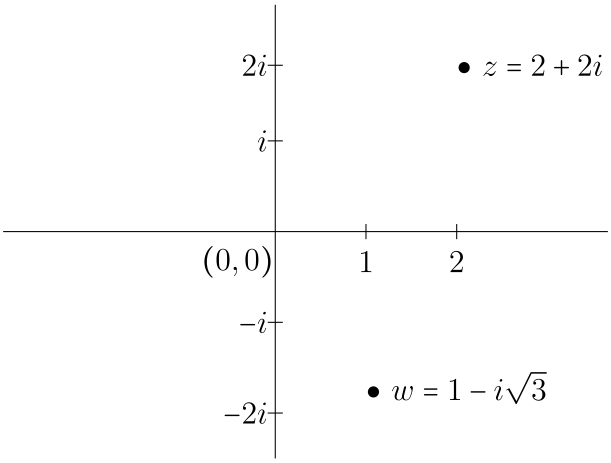
$$a^2 = nb^2$$

and it follows that a^2 is divisible by n. But it *doesn't* follow that a is divisible by n, in general. For example $6^2 = 36$ is divisible by 18, but 6 is certainly not divisible by 18). In order to get further, it helps to think about the prime factorisation of n—this is something we will meet in MA103 next term.

Comment on Activity 7.7. We have

$$(x-w)(x-\overline{w}) = x^2 - (w+\overline{w})x + w\overline{w}.$$

Now, $w+\overline{w} = 2\,\mathrm{Re}(w) = 2(-\frac{1}{2})$ and $w\overline{w} = \frac{1}{4}+\frac{3}{4}$ so the product of the last two factors is x^2+x+1.



Comment on Activity 7.8.

Comment on Activity 7.9. Draw the line from the origin to the point z in the diagram above. Do the same for w. For z, $|z| = 2\sqrt{2}$ and $\theta = \frac{\pi}{4}$, so $z = 2\sqrt{2}\big(\cos(\frac{\pi}{4}) + i\sin(\frac{\pi}{4})\big)$. The modulus of w is $|w| = 2$ and the argument is $-\frac{\pi}{3}$, so that

$$w = 2\Big(\cos(-\frac{\pi}{3}) + i\sin(-\frac{\pi}{3})\Big) = 2\Big(\cos(\frac{\pi}{3}) - i\sin(\frac{\pi}{3})\Big).$$

The set (a) $|z| = 3$, is the circle of radius 3 centered at the origin. The set (b), argument of z is $\frac{\pi}{4}$, is the half line from the origin through the point (1,1).

Comment on Activity 7.12. The roots are:

$$z_1 = 1 \cdot e^{i\frac{\pi}{6}}, \qquad z_2 = 1 \cdot e^{i\frac{3\pi}{6}}, \qquad z_3 = 1 \cdot e^{i\frac{5\pi}{6}},$$

$$z_4 = 1 \cdot e^{i\frac{7\pi}{6}}, \qquad z_5 = 1 \cdot e^{i\frac{9\pi}{6}}, \qquad z_6 = 1 \cdot e^{i\frac{11\pi}{6}}.$$

These roots are in conjugate pairs, and $e^{i\frac{13\pi}{6}} = e^{i\frac{\pi}{6}}$:

$$z_4 = \overline{z}_3 = e^{-i\frac{5\pi}{6}}, \qquad z_5 = \overline{z}_2 = e^{-i\frac{\pi}{2}}, \qquad z_6 = \overline{z}_1 = e^{-i\frac{\pi}{6}}.$$

The polynomial factors as

$$x^6 + 1 = (x - z_1)(x - \overline{z}_1)(x - z_2)(x - \overline{z}_2)(x - z_3)(x - \overline{z}_3),$$

Using the $a + ib$ form of each complex number, for example, $z_1 = \frac{\sqrt{3}}{2} + i\frac{1}{2}$, you can carry out the multiplication of the linear terms pairwise (conjugate pairs) to obtain $x^6 + 1$ as a product of irreducible quadratics with real coefficients:

$$x^6 + 1 = (x^2 - \sqrt{3}\,x + 1)(x^2 + \sqrt{3}\,x + 1)(x^2 + 1).$$

7.6 Solutions to exercises

Solution to Exercise 7.1. Suppose we have $\sqrt{5} = m/n$ where $m, n \in \mathbb{Z}$. Since $\sqrt{5} > 0$, we may assume that $m, n > 0$. (Otherwise, both are negative, and we can multiply each by -1.) We can also suppose that m, n have greatest common divisor 1. (For, we can cancel any common factors.) Then $(m/n)^2 = 5$ means that $m^2 = 5n^2$. So $5 \div m^2$. Now m can, by the Fundamental Theorem of Arithmetic, be written as a product of primes $m = p_1 p_2 \dots p_k$. Then $m^2 = p_1^2 p_2^2 \dots p_k^2$. If no p_i is 5, then 5 does not appear as a factor in m^2 and so 5 does not divide m^2. So some p_i is equal to 5. So $5 \div m$. Now, this means that $m = 5r$ for some $r \in \mathbb{N}$ and hence $m^2 = (5r)^2 = 25r^2$ and so $25r^2 = 5n^2$. Then, $n^2 = 5r^2$, so $5 \div n^2$. Arguing as before, $5 \div n$. So 5 is a common factor if m and n, which contradicts $\gcd(m, n) = 1$. Hence $\sqrt{5}$ is not rational.

Solution to Exercise 7.2. We have

$$\begin{aligned}
\frac{1+2i}{4-5i} &= \frac{1+2i}{4-5i}\frac{4+5i}{4+5i} \\
&= \frac{(1+2i)(4+5i)}{(4-5i)(4+5i)} \\
&= \frac{4+8i+5i+10i^2}{16-25i^2} \\
&= \frac{-6+13i}{41} \\
&= -\frac{6}{41} + \frac{13}{41}i.
\end{aligned}$$

You can *check* that this is the correct answer by calculating the product

$$\left(-\frac{6}{41} + \frac{13}{41}i\right)(4 - 5i)$$

and observing that the answer is $1 + 2i$.

Solution to Exercise 7.3. To solve the equation $x^2 - 2ix + 3 = 0$, we could use the formula for the solutions of a quadratic equation. Or we could note that the equation is equivalent to $(x - i)^2 = -4$, so the solutions are given by $x - i = 2i$ and $x - i = -2i$, so they are $x = 3i$ and $x = -i$.

Solution to Exercise 7.4. We have

$$e^{i\pi/2} = i, \qquad e^{i3\pi/2} = -i, \qquad e^{i3\pi/4} = -\frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}},$$

$$e^{i(11\pi/3)} = e^{-i(\pi/3)} = \frac{1}{2} - i\frac{\sqrt{3}}{2}, \qquad e^{1+i} = e^1 e^i = e\cos(1) + i\,e\sin(1),$$

$$e^{-1} = e^{-1} + 0i \text{ is real, so already in the form } a + ib.$$

Solution to Exercise 7.5. To express $z = 1 + \sqrt{3}i$ in exponential form, we first note that

$$1 + \sqrt{3}i = 2\left(\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)$$

and this is $r(\cos\theta + i\sin\theta)$ when $r = 2, \theta = \pi/3$. So $z = 2e^{\pi i/3}$. Then,

$$(1 + \sqrt{3}i)^{30} = z^{30} = \left(2e^{\pi i/3}\right)^{30} = 2^{30}e^{30\pi i/3} = 2^{30}e^{10\pi i} = 2^{30}.$$

8 Analysis: the real numbers

8.1 What is analysis?

Analysis is the *theory* behind real numbers, sequences, and functions. The word ‘theory’ is important. You might, for example, have a good idea of what we mean by a ‘limit’ of a convergent sequence of numbers, or the notion of a ‘continuous’ function, but in this part of the course we aim to formalise such notions.

8.1.1 Analysis and calculus: the history

Historically, mathematicians did not formalise the concept of a ‘function’ as we have done it until the 1800s. Prior to this, mathematicians generally thought of a function as ‘something defined by a formula’. This is what Isaac Newton and Gottfried Leibniz were thinking of when they independently developed the ‘infinitesimal calculus’. What they did starts with what you learned at school: how to integrate and differentiate, and what those two operations mean. The roots of the calculus are much older—Pierre de Fermat had some systematic ideas in this direction, and in ancient times Eudoxus and Archimedes in Greece, and independently Liu Hui in China, developed geometric methods which are rather close to integration.

As Newton and Leibniz formulated it, the calculus is a collection of rules for calculating things—this collection of rules starts with what you learned at school. You can use the calculus to find a formula for, to take an example, the volume of a sphere of radius 1. Here is one way to do that—it’s an argument due to Archimedes.

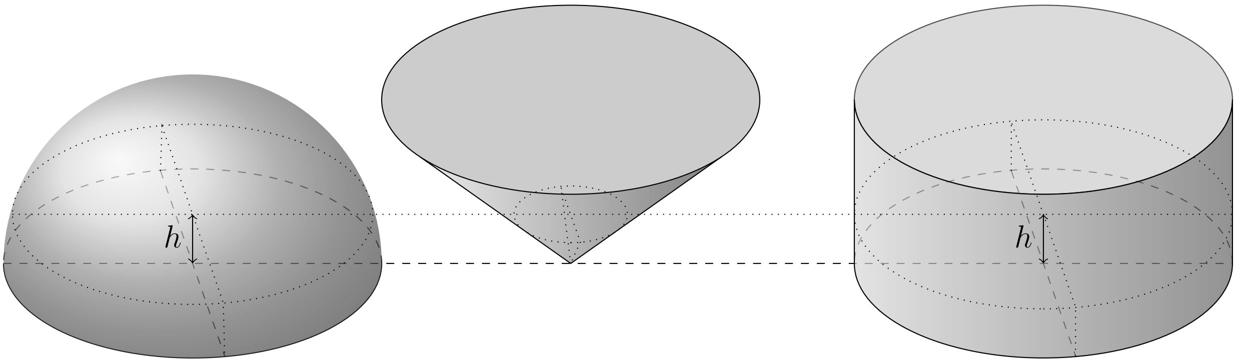


Figure 8.1: A hemisphere, cone and cylinder, with a slice through at height h

Take a sphere of radius 1, and cut in in half through the centre to obtain a hemisphere.

Place the hemisphere with its flat base on the table, and put next to it a cone of height 1, with its base a circle of radius 1, standing vertically on its point. And next to that, put a cylinder of radius and height 1.

Now, the critical observation: if you take a slice through this picture at any height h between 0 and 1, you slice a circle out of each of the hemisphere, cone and cyclinder. The area of the circle sliced from the hemisphere, plus the area of the circle sliced from the cone, is equal to the area of the circle sliced from the cylinder. This is easy to check using the Pythagoras theorem and the formula for the area of a circle (which Archimedes knew). The slice through the hemisphere is a circle of radius $\sqrt{1-h^2}$ for an area $\pi(1-h^2)$; the slice through the cone is again a circle, this time of radius h for an area πh^2; the slice through the cylinder is a circle of radius 1 for an area π.

So, (in modern language) if we integrate we see that the volume of the hemisphere plus the volume of the cone is equal to the volume of the cylinder. Archimedes, of course, did not say 'integrate', but he had a similar conception.

Putting it another way, the volume of the hemisphere is the volume of the cylinder minus the volume of the cone: $\pi - \frac{1}{3}\pi = \frac{2}{3}\pi$. (Archimedes knew the volume of a cone, too.)

So the volume of the sphere is $\frac{4}{3}\pi$.

Why did I go through this argument? Well, because you can try to do something similar to find the surface area of the sphere. Here is one way, which I'll give in terms of modern integration.

Look again at the hemisphere lying on the table, and take a slice through it at height h. That gives us a circle of radius $\sqrt{1-h^2}$, as before, and the length of that circle is $2\pi\sqrt{1-h^2}$.

Integrating, we find the area of the curved bit of the hemisphere is

$$\int_{h=0}^{1} 2\pi\sqrt{1-h^2}\,\mathrm{d}h = \tfrac{1}{2}\pi^2 \,.$$

So the surface area of the whole sphere is π^2.

But you maybe know a formula for the surface area of a sphere—and it doesn't agree with the calculation we just did! The correct answer is slightly larger; it is 4π. Archimedes knew this (he had a different method), and he also knew why the above method does not work.

Activity 8.1. *Why did we underestimate the surface area—what are we missing?*

Liu Hui developed quite a number of methods of this nature in China, and (importantly) he gave intuitive explanations of why certain methods work and others do not; following his ideas, one can solve rather a lot of geometrical problems accurately. But this is an unpleasant situation for a mathematician to find themselves in, with methods which might or might not work.

While mathematicians were using calculus-like methods to find answers to geometrical problems, these intuitive explanations were considered good enough. But Newton and Leibniz, and the mathematicians who came later, were soon using the calculus as you know it to find answers to problems which aren't obviously geometrical. Newton himself did not really trust the calculus (or at least, he didn't expect others to trust it); while he used it to solve problems, once he knew the answer he generally looked for a geometrical proof before publishing. But doing this is hard work (and sometimes you will get completely stuck and be unable to do it at all), and if you trust the calculus, it is a waste of time.

But you cannot always trust the calculus, as we have seen!

The solution to this—developed by Cauchy and Weierstrass in the 1800s—is to formalise all of this properly, remove the appeals to intuition, and provide some clear rules: if you do *this* it will always work, and we can prove it. This is where analysis begins. If that was all there is to it, it would be a small part of mathematics: but in fact, analysis provides us with many surprising tools, going far beyond the calculus of Newton and Leibniz, and it is one of the two major branches of pure mathematics, along with Algebra (which MA103 will introduce you to in Winter Term).

We will not get that far in this course. But we can at least lay the foundations.

8.1.2 Greek letters, conventions and inexact calculation

In mathematics, we often use particular letters for particular things. When you see the letter n in a proof, you probably expect that it is going to be an integer (we always used it that way so far). The letter x, on the other hand, you maybe expect to be some real number, and f is usually a function.

There isn't any rule that says we have to do this; it's perfectly fine to talk about $n = 2.75$, or the function $x : \mathbb{R} \to \mathbb{R}$ defined by $x(f) = f^2$. But it does help to have these conventions—you probably find it hard even to read the function definition!

In analysis, there are two new letters we use from the Greek alphabet: epsilon ε and delta δ. Conventionally, *these are always positive reals* and you should think of them as *tiny*. In the next three chapters, we will always insist that ε and δ are positive real numbers. We will *not* always insist that they are tiny, but the 'interesting case' will always be when they are very small.

In particular, you should think of ε^2 or ε^3 as being much smaller than ε. Why is this relevant? In this part of the course, we *often do not care about exact answers*. This is something you have not seen in maths before: in the past, whenever you were supposed to work something out, you were expected to give an exact answer.

In this bit of the course, you might see a question like 'Find a real number which is bigger than $f(x) = \sin(x) - (x-2)^2$ for all $x \in \mathbb{R}$'. Before turning the page, think about how you can solve this problem.

You probably started thinking about the following: differentiate, set the derivative to zero and solve...

What you are doing, if you do that, is *too much work*. You're trying to find *the maximum* value of $f(x)$ on $\mathbb{R}$. It turns out to be a pain to do this, and it's not what the question asked for. If you do it (correctly!) then you do have a right answer, but you have also spent a lot of time getting it.

It's much easier to observe that $-1 \le \sin x \le 1$ is true for all $x \in \mathbb{R}$ (you know this from school, I hope!), and $-(x-2)^2$ is never positive. So $f(x) \le 1 - 0 = 1$. So we can answer '1 is such a number' and write this very short proof, and we are done. The number 2023, by the way, would have done just as well; there are no points for some 'best possible' answer.

For another example, if you are supposed to 'choose $\varepsilon > 0$ such that $17\varepsilon + 283\varepsilon^2 < 0.1$' then you don't need to start trying to solve a quadratic equation in ε (which is a pain). You can say: I will choose some $\varepsilon \le 1$, so that $\varepsilon^2 \le \varepsilon$. Then I get

$$17\varepsilon + 283\varepsilon^2 \le 17\varepsilon + 283\varepsilon = 300\varepsilon$$

and if I choose $\varepsilon = \frac{1}{6\,000}$ (which is indeed ≤ 1) then I am done.

A final comment: some of you most likely heard something about funny names or symbols like 'infinitesimals' or 'dx' before, and maybe have some idea that ε is 'really' the 'dx'. This is *not true*; ε is a real number and (whatever those funny things are) they are not real numbers.

8.2 The real numbers

The rational number system is inadequate for many purposes. For instance, there is no rational number q such that $q^2 = 2$, and the set

$$S = \left\{ q \in \mathbb{Q} \;\middle|\; q^2 \le 2 \right\}$$

does not have a largest element in $\mathbb{Q}$. So we see that the rational number system has "gaps". The real number system $\mathbb{R}$ includes numbers to fill all of these gaps. Thus the set

$$T = \left\{ x \in \mathbb{R} \;\middle|\; x^2 \le 2 \right\}$$

has a largest element. This is a consequence of a very important property of the real numbers, called the least upper bound property. Before we state this property of $\mathbb{R}$, we need a few definitions.

8.2.1 Bounded sets; least upper bound

Definition 8.1. Let S be a subset of $\mathbb{R}$.

1. An element $u \in \mathbb{R}$ is said to be an *upper bound of* S if, for all $x \in S$, $x \leq u$. If S has an upper bound, then we also say that S is *bounded above.*

2. An element $l \in \mathbb{R}$ is said to be a *lower bound of* S if, for all $x \in S$, $l \leq x$. If S has a lower bound, then we also say that S is *bounded below.*

3. The set S is said to be *bounded* if it is bounded above and bounded below.

Example 8.2.

(i) The set $S = \{x \in \mathbb{R} \mid 0 \leq x < 1\}$ is bounded. Any real number y satisfying $y \geq 1$ (for instance 1, π, or 100) is an upper bound of S, and any real number z satisfying $z \leq 0$ (for instance 0, or -1) is a lower bound of S.

(ii) The set $S = \{n \mid n \in \mathbb{N}\}$ is bounded below; indeed, any real number $x \leq 1$ serves as a lower bound. It has no upper bound—we shall give a formal proof of this shortly—and so it is not bounded above, and therefore also not bounded.

(iii) The set $S = \{(-1)^n \mid n \in \mathbb{N}\}$ is bounded. Note that $S = \{-1, 1\}$. It is bounded above by 1 and bounded below by -1.

More generally, any finite set S is bounded.

(iv) The set $S = \left\{\frac{1}{n} \mid n \in \mathbb{N}\right\}$ is bounded. Any real number x satisfying $1 \leq x$ is an upper bound, and 0 is a lower bound.

(v) The sets $\mathbb{Z}$ and $\mathbb{R}$ are neither bounded above nor bounded below.

(vi) The set $T = \{x \in \mathbb{R} \mid x^2 \leq 2\}$ is bounded. Any real number x satisfying $x^2 \leq 2$ also satisfies $x^2 < 4$. Therefore, $x^2 - 4 < 0$, that is, $(x-2)(x+2) < 0$. It follows that

either $x - 2 < 0$ and $x + 2 > 0$,

or $x - 2 > 0$ and $x + 2 < 0$.

The second case is impossible. Thus the first case has to hold, that is $-2 < x < 2$. It follows that T is bounded above by 2 and bounded below by -2.

(vii) The set $\varnothing$ is bounded. For instance, 1 is an upper bound for $\varnothing$, since the condition "for every element x of $\varnothing$, $x \leq 1$" is satisfied: there is certainly no element x of $\varnothing$ that **doesn't** satisfy $x \leq 1$. Indeed, every real number is an upper bound for $\varnothing$, and similarly every real number is a lower bound for $\varnothing$. □

We now introduce the notions of a least upper bound (also called supremum) and a greatest lower bound (also called infimum) of a subset S of $\mathbb{R}$.

Definition 8.3. Let S be a subset of $\mathbb{R}$.

1. An element $u_* \in \mathbb{R}$ is said to be a *least upper bound of* S (or a *supremum of* S) if

   (a) u_* is an upper bound of S, and

   (b) for each upper bound u of S, it holds that $u_* \leq u$.

2. An element $l_* \in \mathbb{R}$ is said to be a *greatest lower bound of* S (or an *infimum of* S) if

(a) l_* is a lower bound of S, and

(b) for each lower bound l of S, it holds that $l \leq l_*$.

Example 8.4. *Let* $S = \{x \in \mathbb{R} \mid x < 1\}$. *Show that the supremum of* S *is* 1.

Proof. Clearly 1 is an upper bound of S.

Now we show that if u is another upper bound, then $1 \leq u$. Suppose not, that is, suppose that there is an upper bound u of S with $u < 1$. Then we have

$$u < \frac{u+1}{2} < 1,$$

where both inequalities follow using $u < 1$. From the second inequality, it follows that the number $\frac{u+1}{2}$ belongs to S. The first inequality above then shows that u is not an upper bound for S, a contradiction. Hence 1 is a supremum.

Next we show that 1 is the only supremum. Indeed, if u_* is another supremum, then in particular u_* is also an upper bound, and the above argument shows that $1 \leq u_*$. But $1 < u_*$ is not possible, since 1 is an upper bound for S, and as u_* is a supremum, u_* must be less than or equal to the upper bound 1. So it follows that $u_* = 1$. □

In the above example, there was a unique supremum of the set S. In fact, this is always the case and we have the following result.

Theorem 8.5. *If a least upper bound of a subset* S *of* $\mathbb{R}$ *exists, then it is unique.*

Proof. Suppose that S has a least upper bound u_*. Suppose that u'_* is also a least upper bound of S. Then in particular u_* and u'_* are also upper bounds of S. Now since u_* is a least upper bound of S and u'_* is an upper bound of S, it follows that

$$u_* \leq u'_*. \tag{8.1}$$

Furthermore, since u'_* is a least upper bound of S and u_* is an upper bound of S, it follows that

$$u'_* \leq u_*. \tag{8.2}$$

From (8.1) and (8.2) we obtain $u_* = u'_*$. □

Thus it makes sense to talk about *the* least upper bound, or *the* supremum, of a set. Similarly, the infimum of a set S (if it exists) is also unique.

Definition 8.6.

1. The least upper bound of a set S (if it exists) is denoted by $\sup S$.

2. The greatest lower bound of a set S (if it exists) is denoted by $\inf S$.

When the supremum and the infimum of a set belong to the set, we give them the following familiar special names:

Definition 8.7.

1. If $\sup S \in S$, then $\sup S$ is called a *maximum of* S, denoted by $\max S$.

2. If $\inf S \in S$, then $\inf S$ is called a *minimum of* S, denoted by $\min S$.

Example 8.8.

(i) If $S = \{x \in \mathbb{R} \mid 0 \le x < 1\}$, then $\sup S = 1 \notin S$ and so $\max S$ does not exist. But $\inf S = 0 \in S$, and so $\min S = 0$.

(ii) If $S = \mathbb{N}$, then $\sup S$ does not exist, $\inf S = 1$, $\max S$ does not exist, and $\min S = 1$.

(iii) If $S = \{(-1)^n \mid n \in \mathbb{N}\}$, then $\sup S = 1$, $\inf S = -1$, $\max S = 1$, $\min S = -1$.

(iv) If $S = \left\{\frac{1}{n} \,\middle|\, n \in \mathbb{N}\right\}$, then $\sup S = 1$ and $\max S = 1$. We show below (after Theorem 8.12) that $\inf S = 0$. So $\min S$ does not exist.

(v) For the sets $\mathbb{Z}$ and $\mathbb{R}$, none of sup, inf, max, min exist.

(vi) For the set $\varnothing$, none of sup, inf, max, min exist. □

8.2.2 The least upper bound property

In the above examples, we can see that if S is non-empty and bounded above, then its supremum exists. In fact this is a fundamental property of the real numbers, called the *least upper bound property* of the real numbers, which we now state:

The Least Upper Bound Property.
If S is a subset of $\mathbb{R}$ that is non-empty and bounded above, then S has a least upper bound.

In other words, for a subset $S \subseteq \mathbb{R}$, if

1. $S \ne \varnothing$, and

2. S has an upper bound,

then $\sup S$ exists.

While we are formalising the calculus, we want to avoid making more assumptions than we need. So what we are going to assume is very simple. There is a set $\mathbb{R}$ of numbers. We can do arithmetic with these numbers as you are used to (formally, these numbers form a *field*, look it up if you want to know what exactly that means, for our purposes 'arithmetic as normal' is good enough), there is an order $<$ on them which behaves 'as you expect' (again, we could write axioms saying how $<$ interacts with $+$ and $\times$, and formally we should), and the least upper bound property holds.

Everything else we need, we will prove from these assumptions. It's best to avoid thinking about 'what exactly are the real numbers'? If you want something concrete to think about, think about the usual infinite-decimal representation that you learned in school, and we discussed in the last chapter.

But it turns out we will not need to care; we can just work with the assumptions above.

Critical

From this point on, there will be lots of quantifiers. You must use standard strategies to deal with them. Otherwise you will get confused.

Just to see, let's write out 'u is an upper bound of S' in logical notation. It is: $\forall s \in S\,,\ s \le u$. Officially, this is a predicate with two free variables u and S, and one bound variable s. If you don't find that obvious, go back to chapter 3 and re-read.

What about: v is a least upper bound of S? Well:

$$\big(\forall s \in S\,,\ s \le v\big) \wedge \Big(\forall u \in \mathbb{R},\ \big(\forall s \in S\,,\ s \le u\big) \implies v \le u\Big).$$

Again, this is a predicate with free variables v and S; this time s and u are both bound variables (and, actually, we are naughtily re-using the letter s in two different places; we should really use a different letter the second time).

As we get further in to analysis, we'll see more and more complicated statements, in particular ones which look like $\forall \varepsilon > 0\,,\ \exists N \in \mathbb{N}\,,\ \forall n > N\,,\ P(\varepsilon, N, n)$. This is sometimes called *quantifier alternation*; a string of quantifiers swapping between 'for all' and 'there exists'.

Whether you're trying to understand what such a thing means, or to prove it, or to use it, you need to keep the standard strategies clear. You've already seen lots of statements with two quantifiers: 'f is surjective', for example; you know how to work with them. More quantifiers are not really harder, you just need to use the standard strategies more often.

There will be enough difficulty in these Analysis chapters as it is. Understanding will be tricky. Choosing 'the right example' to prove 'there exists' statements, and picking 'the right statement' to use 'for all' statements, will need thought and ideas. You cannot afford to be at the same time struggling with basic logic: if you are not too sure, go back to Chapter 3 and revise.

Let's briefly look at the statement $\forall \varepsilon > 0\,,\ \exists N \in \mathbb{N}\,,\ \forall n > N\,,\ P(\varepsilon, N, n)$. Yes, it doesn't really mean anything when you don't know what the predicate P is. Still: how would you try to prove it?

Well, it is a 'for all' statement, so the proof starts 'Given $\varepsilon > 0$'. Then, what's inside is a 'there exists', so you will need to have an idea how to choose a natural number N. At this stage you probably write 'Let $N =$.' and you'll fill in the blank later. Then, what's inside *that* is a 'for all', so 'Given $n > N$'.

At this point, ε, N and n are all fixed. The predicate $P(\varepsilon, N, n)$, with these fixed numbers in, is now just a true-or-false statement; it's probably something like a calculation or an inequality that is supposed to be true. It might be, for example, '$\frac{1}{n} < \varepsilon$'. In this example—what's missing is to fill in the blank $N =$ with something that will make the calculation work, and here picking any integer N larger than $\frac{1}{\varepsilon}$ would do the job (because $n > N$ we have $\frac{1}{n} < \frac{1}{N} < \varepsilon$). So—proof done.

What you are supposed to notice here is: while you need ideas to write proofs, the same standard strategies as you saw in the last chapters are what you need to figure out how the routine bits of proofs go. The same understanding of basic logic as in the last chapters is what you need to understand these more complicated statements. It is definitely not the case that you need to think in new and different ways to do this part of the course: instead, you need to keep thinking in exactly the same way as worked for you in the last few chapters, you just need to be more persistent (and you will need a few more ideas, because there will be a few more $\exists$ symbols). In the proof above, you already know how it has to start, and where you need an idea (choosing N), without even looking at what this predicate $P(\varepsilon, N, n)$ is; that bit is all routine, standard strategies. You need to look at the predicate only to figure out what the final calculation is, and so you can start thinking about what N should be.

What you can also notice is that if you want to start using proof by contrapositive or contradiction, then you'd better be able to negate statements like the above. You need to realise that

$$\neg \forall \varepsilon > 0\,,\ \exists N \in \mathbb{N}\,,\ \forall n > N\,,\ P(\varepsilon, N, n)$$

is

$$\exists \varepsilon > 0\,,\ \forall N \in \mathbb{N}\,,\ \exists n > N\,,\ \neg P(\varepsilon, N, n)\,.$$

That has to be something you can do automatically—because then you can apply standard strategies to help prove such a thing. There will be enough places where you have to come up with an idea: so you need to be able to do the 'easy bits' without it costing you mental energy.

Example 8.9. Use the least upper bound property to show that there exists a number $s \in \mathbb{R}$ such that $s > 0$ and $s^2 = 2$.

Since the function $x \to x^2$ is increasing on the non-negative reals (i.e. if $x \geq 0$) and it 'doesn't have jumps' (draw the graph!), the intuition is that we trace the number line (the x axis) from 0 upwards, until we reach the desired point $x = s$ where x^2 gets to 2. When $x > s$ we will have $x^2 > 2$.

This is of course not a proof. We don't know what 'doesn't have jumps' means formally (we'll get to that!) and 'trace the number line' is not part of the least upper bound property.

But this idea does suggest something: we can split the reals into two parts: the part $S = \{x \in \mathbb{R} \mid x^2 < 2\}$ of numbers that are 'too small' and the rest. Again, draw the graph and look at where S is on the x axis. We would really like to say that s is the number 'at the end of' S. This informal idea is exactly what 'least upper bound' is supposed to formalise.

So we would like to say that $s = \sup S$ *exists* and that *it satisfies* $s^2 = 2$. Let's now formalise this.

Proof. To begin with, we justify that $x \to x^2$ is an increasing function for $x \geq 0$. That is, if $0 \leq y < z$ then we want to prove $y^2 < z^2$. That is the same as proving $z^2 - y^2 > 0$, and we can factorise $z^2 - y^2 = (z - y)(z + y)$ which is positive because both factors are positive.

Let $S = \{x \in \mathbb{R} \mid x^2 < 2\}$. We now want to show $\sup S$ exists. This is what the least upper bound property is for. We just need to show S is not empty and it has an upper bound.

First, $1 \in S$ (by definition), so S is not empty. And for example 3 is an upper bound for S. This needs some justification: why is it that everything in S is at most 3? In other words, why is everything bigger than 3 *not* in S? Well, $3^2 = 9$, and so (because of the increasing property) if we are given any x with $3 < x$ then $3^2 < x^2$. That means in particular $x^2 > 2$, so x is not in S.

Since we now know S is not empty and has an upper bound, by the least upper bound property $\sup S$ exists. Let $s = \sup S$. We can notice that $s \geq 1$ since $1 \in S$.

Finally, we need to prove $s^2 = 2$. We do this by showing that each of the two alternatives $s^2 > 2$ and $s^2 < 2$ leads to a contradiction.

Suppose first that $s^2 > 2$. Intuitively, s is 'too big'. We should be trying to contradict the 'least' part of 'least upper bound'; we want to find an upper bound of S that is smaller than s.

That is, we want to find some small $\varepsilon > 0$ such that $s - \varepsilon$ is an upper bound for S. By the increasing property, that is the same as finding a small $\varepsilon > 0$ such that $(s - \varepsilon)^2 > 2$.

We choose $\varepsilon = \frac{s^2-2}{2s}$; this formula comes out positive since $s^2 > 2$ and $s \geq 1$. Calculating, we get

$$(s - \varepsilon)^2 = s^2 - 2s\varepsilon + \varepsilon^2 > s^2 - 2s\varepsilon = s^2 - 2s\tfrac{s^2-2}{2s} = 2\,.$$

Here the inequality is since $\varepsilon^2 > 0$. We are done in this case.

Now suppose $s^2 < 2$. Again, intuitively s is 'too small' so we should be trying to contradict the 'upper bound' part of 'least upper bound'; we want to find something in S which is bigger than s.

That is, we want to find some small $\varepsilon > 0$ such that $s + \varepsilon$ is in S, so $(s + \varepsilon)^2 < 2$.

We choose $\varepsilon = \min\left(\frac{1}{2}, \frac{2-s^2}{2s+1}\right)$. That is, ε is whichever is smaller out of $\frac{1}{2}$ and $\frac{2-s^2}{2s+1}$. Again, since $s^2 < 2$ and $s \geq 1$ this formula comes out positive.

Now we can calculate:

$$(s + \varepsilon)^2 = s^2 + 2s\varepsilon + \varepsilon^2 = s^2 + (2s + \varepsilon)\varepsilon < s^2 + (2s + 1)\varepsilon \leq s^2 + (2s + 1)\tfrac{2-s^2}{2s+1} = 2\,.$$

Here the $<$ comes because we replaced ε with 1: we know $\varepsilon \leq \frac{1}{2}$ so in particular $\varepsilon < 1$. And the $\leq$ is since we know $\varepsilon \leq \frac{2-s^2}{2s+1}$. What this calculation says is that $s + \varepsilon \in S$. This case is done.

The only remaining possibility is that $s^2 = 2$. To conclude, we have shown the existence of $s \in \mathbb{R}$ such that $s > 0$ and $s^2 = 2$. □

In the 'checking that $s^2 = 2$' part of this proof, there are two big 'magic steps' where I just pulled a weird formula for ε out of somewhere and it turned out to work. Of course, these steps cannot really be magic. Where does the formula come from?

The first one is easier. We suppose $s^2 > 2$, so s is 'too big' and we can think about removing some tiny $\varepsilon > 0$.

We knew from the start we wanted to get $(s-\varepsilon)^2 > 2$. That's the same as saying $s^2-2s\varepsilon+\varepsilon^2 > 2$. This looks like a quadratic in ε, which is nasty: let's try to avoid solving a quadratic. Let's work backwards.

It's enough to get $s^2 - 2s\varepsilon \geq 2$, because then we can add ε^2 to both sides (and $2 + \varepsilon^2 > 2$). This is now a linear inequality, which is easy. Rearranging, it's enough to get

$$\varepsilon \leq \tfrac{s^2-2}{2s} .$$

Well, but *we can choose* ε, so in particular we can choose ε to satisfy this inequality. Maybe the easiest option was the choice we made; though really any ε satisfying $0 < \varepsilon \leq \frac{s^2-2}{2s}$ would work.

The other calculation needs a bit more explanation. The idea is the same. Since we assume $s^2 < 2$, we think s is 'too small' and we want to look at $s + \varepsilon$: think of ε as being tiny, and work backwards.

We want $(s + \varepsilon)^2 < 2$, or equivalently $s^2 + 2\varepsilon s + \varepsilon^2 < 2$. This time the ε^2 *doesn't* help us. But if ε is tiny, then ε^2 should be even smaller. In particular, we should be able to write $\varepsilon^2 < \varepsilon$. So let's do that.

It's enough to get $s^2 + 2\varepsilon s + \varepsilon \leq 2$, because $\varepsilon^2 < \varepsilon$. But this is (again) linear and we can rearrange it: it's enough to get $\varepsilon \leq \frac{2-s^2}{2s+1}$. And again—*we can choose* ε; we can choose $\varepsilon = \frac{2-s^2}{2s+1}$.

This time, though, we need to be a bit careful. We said ε is tiny so $\varepsilon^2 < \varepsilon$. Our argument relied on it! But what if this funny fraction $\frac{2-s^2}{2s+1}$ isn't tiny? If it is 1 or bigger, then our '$\varepsilon^2 < \varepsilon$' assumption would go wrong and the proof would not work.

This is why we chose $\varepsilon = \min\left(\frac{1}{2}, \frac{2-s^2}{2s+1}\right)$. We insist ε is at most $\frac{1}{2}$ so that we can write $\varepsilon^2 < \varepsilon$. And then we insist ε is at most $\frac{2-s^2}{2s+1}$ so the rest of the argument works.

Example 8.10. Prove the 'greatest lower bound property': if S is a non-empty subset of $\mathbb{R}$ that is bounded below, then S has a greatest lower bound.

This is an exercise.

8.2.3 The Archimedean property of the real numbers

The least upper bound property of the real numbers tells us (intuitively!) that the real numbers don't have 'gaps', which is certainly nice.

But why did we insist on saying that 0.9999... is the same real number as 1? Why don't we say that they are two different numbers, differing by something 'infinitesimal'? It turns out that we can't—it's not compatible with the least upper bound property. This is the content of the next theorem, called the *Archimedean property* of the real numbers.

Remark 8.11. Some mathematicians *do* study number systems which contain 'infinitesimals', but the price to pay is that they do not behave as nicely as we would like. We will not go into this.

Theorem 8.12 (Archimedean property). *For all $x, y \in \mathbb{R}$ with $x > 0$, there exists an $n \in \mathbb{N}$ such that $y < nx$.*

Proof. Given $x, y \in \mathbb{R}$ with $x > 0$, suppose for a contradiction that there does not exist $n \in \mathbb{N}$ such that $y < nx$. This means that for all $n \in \mathbb{N}$, $y \geq nx$. In other words, y is an upper bound of the non-empty set $S = \{nx \mid n \in \mathbb{N}\}$.

By the least upper bound property of the reals, S has a least upper bound u_*. Note that $u_* - x$ is not an upper bound of S, since $u_* - x$ is smaller than u_* (x is positive) and u_* is the *least* upper bound. Hence there exists an element $mx \in S$ (with $m \in \mathbb{N}$) such that $u_* - x < mx$, that is, $u_* < (m+1)x$. But $(m+1)x$ is also an element of S, and we just said $(m+1)x > u_*$: this contradicts the fact that u_* is an upper bound of S. □

Let's see why the Archimedean property tells us that 0.999... = 1. Well, if not, then $x = 1 - 0.999...$ cannot be zero; suppose $x > 0$. (This is the obvious thing to assume, but formally we should consider the 'other' case that it is negative.) And let $y = 1$. Then the Archimedean property says that there is some natural number n such that $1 < nx$, i.e. $x > \frac{1}{n}$. Putting it another way, we have

$$\tfrac{1}{n} + \tfrac{9}{10} + \tfrac{9}{100} + \tfrac{9}{1000} + \cdots < 1$$

for some fixed natural number n. But this is not possible. To see that, observe that

$$\tfrac{1}{n} + \tfrac{9}{10} + \tfrac{9}{100} + \tfrac{9}{1000} + \cdots > \tfrac{1}{n} + \tfrac{9}{10} + \tfrac{9}{100} + \cdots + \tfrac{9}{10^n} = \tfrac{1}{n} + \tfrac{10^n - 1}{10^n}$$

where the first inequality is simply because we're leaving out all the (infinitely many, positive) terms of the series after $\frac{9}{10^n}$, and the equality uses the formula for the sum of a geometric series. But $n < 10^n$ is true for every natural number n, so $\frac{1}{n} > \frac{1}{10^n}$, so the right hand side of the above is bigger than one.

As a consequence of the Archimedean property we are now able to *prove* that the set $\mathbb{N}$ of natural numbers is not bounded above.

Example 8.13. Show that the set $\mathbb{N}$ is not bounded above.

Proof. Suppose that $\mathbb{N}$ is bounded above. Then $\mathbb{N}$ has an upper bound $y \in \mathbb{R}$. Since $1 \in \mathbb{N}$, $1 \leq y$, and in particular, $y > 0$. Let $x = 1$. By the Archimedean property (Theorem 8.12), there exists an $n \in \mathbb{N}$ such that $y < nx = n$. This contradicts the fact that y is an upper bound of $\mathbb{N}$. □

Warning 8.14. It's rather common for students to say 'the natural numbers are bounded above, by ∞'. This is *wrong*. The symbol ∞ is a very convenient thing to use—and we will use it repeatedly in what follows—but it is *not* a real number. Trying to treat ∞ as a real number is one of the quickest ways to get to a wrong answer. Not just wrong in that your proof doesn't make sense, but wrong in that you get the wrong number out of your calculations, you end up calculating things like $3 - 1 = 0$.

Example 8.15. Set $S = \left\{\frac{1}{n} \,\middle|\, n \in \mathbb{N}\right\}$. Show that $\inf S = 0$.

Proof. We know that 0 is a lower bound of S. Suppose that l is a lower bound of S such that $l > 0$. By the Archimedean property (with the real numbers x and y taken as $x = 1$ (> 0) and $y = \frac{1}{l}$), there exists $n \in \mathbb{N}$ such that $\frac{1}{l} = y < nx = n \cdot 1 = n$, and so $\frac{1}{n} < l$, contradicting the fact that l is a lower bound of S. Thus any lower bound of S must be less than or equal to 0. Hence 0 is the infimum of S. □

8.2.4 Intervals and absolute values

Definition 8.16. An *interval* (in $\mathbb{R}$) is a non-empty subset S of $\mathbb{R}$ with the property: if $x, y \in S$ and $x \le z \le y$, then $z \in S$.

For instance, the set $S = \{x \in \mathbb{R} \mid x < 2\}$ is an interval: if x and y are both in S, and $x \le z \le y$, then in particular $z \le y < 2$ so $z \in S$.

An interval may or may not have an upper bound: if it does have an upper bound, then it has a supremum which may or may not be in the interval. Similarly, an interval may or may not have a lower bound: if it does have a lower bound, then it has an infimum which may or may not be in the interval. In the example above, S has an upper bound, and the supremum is not in S, while S has no lower bound. There are thus three possible forms for the "lower" end of an interval, and three possible forms for the "upper end", making nine forms in all. These are listed in the figure below, along with the notation for each type of interval.

$$(a,b) = \{x \in \mathbb{R} \mid a < x < b\}$$

$$[a,b] = \{x \in \mathbb{R} \mid a \le x \le b\}$$

$$(a,b] = \{x \in \mathbb{R} \mid a < x \le b\}$$

$$[a,b) = \{x \in \mathbb{R} \mid a \le x < b\}$$

$$(a,\infty) = \{x \in \mathbb{R} \mid a < x\}$$

$$[a,\infty) = \{x \in \mathbb{R} \mid a \le x\}$$

$$(-\infty,b) = \{x \in \mathbb{R} \mid x < b\}$$

$$(-\infty,b] = \{x \in \mathbb{R} \mid x \le b\}$$

$$(-\infty,\infty) = \mathbb{R}$$

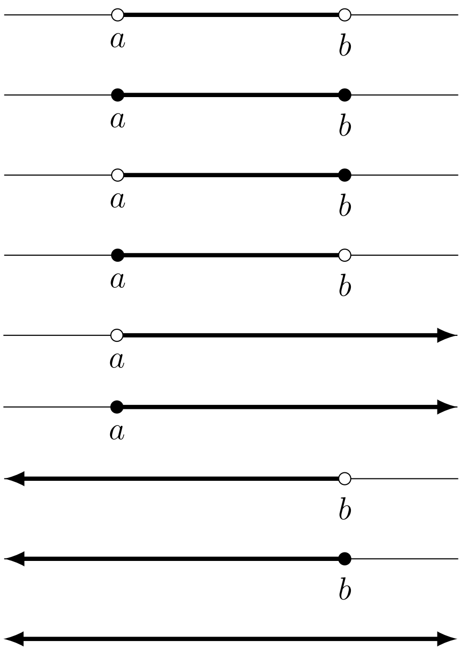


Figure 8.2: Intervals in $\mathbb{R}$

An interval of the form $(-\infty,b)$, (a,b) or (a,∞) is called an *open interval.* An interval of the form $(-\infty,b]$, $[a,b]$ or $[a,\infty)$ is called a *closed interval.*

Thus in the notation for intervals used in Figure 8.2, a parenthesis '(' or ')' means that the respective endpoint is not included, and a square bracket '[' or ']' means that the endpoint is included. For example, $[0,1)$ is the set of all real numbers x such that $0 \le x < 1$. (Note that the use of the symbol ∞ in the notation for intervals is simply a matter of convenience and is not be taken as suggesting that there is a real number ∞.) We do not give any special name to intervals of the form $[a,b)$ or $(a,b]$.

In analysis, in order to talk about notions such as *convergence* and *continuity*, we will need a notion of 'closeness' between real numbers. This is provided by the absolute value $|\cdot|$, and the distance between real numbers x and y is $|x-y|$. We give the definitions below.

Definition 8.17.

1. For a real number x, the *absolute value* $|x|$ of x is defined as follows:

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

2. The *distance* between two real numbers x and y is the absolute value $|x-y|$ of their difference.

Note that $|x| \geq 0$ for all real numbers x, and that $|x| = 0$ if and only if $x = 0$. Thus $|1| = 1$, $|0| = 0$, $|-1| = 1$, and the distance between the real numbers -1 and 1 is equal to $|-1-1| = |-2| = 2$. The distance gives a notion of closeness of two points, which is crucial in the formalization of the notions of analysis.

We can now specify regions comprising points close to a certain point $x_0 \in \mathbb{R}$ in terms of inequalities in absolute values, that is, by demanding that the distance of the points of the region, to the point x_0, is less than a certain positive number δ, say $\delta = 0.01$ or $\delta = 0.0000001$, and so on. See Figure 8.3.

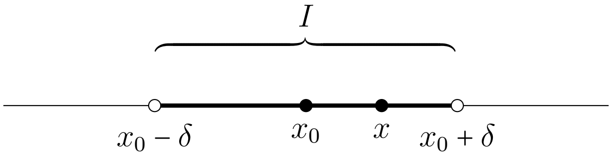


Figure 8.3: The interval $I = (x_0 - \delta, x_0 + \delta) = \{x \in \mathbb{R} \mid \text{we have } |x - x_0| < \delta\}$ is the set of all points in $\mathbb{R}$ whose distance to the point x_0 is strictly less than δ (> 0).

The following properties of the absolute value will be useful.

Theorem 8.18. *If x, y are real numbers, then*

$$|xy| = |x|\,|y| \quad \textit{and} \tag{8.3}$$

$$|x+y| \leq |x| + |y|\,. \tag{8.4}$$

Proof. We prove (8.3) by exhausting all possible cases:

$x = 0$ or $y = 0$.
Then $|x| = 0$ or $|y| = 0$, and so $|x|\,|y| = 0$. On the other hand, as $x = 0$ or $y = 0$, it follows that $xy = 0$ and so $|xy| = 0$.

$x > 0$ and $y > 0$.
Then $|x| = x$ and $|y| = y$, and so $|x|\,|y| = xy$. On the other hand, as $x > 0$ and $y > 0$, it follows that $xy > 0$ and so $|xy| = xy$.

$x > 0$ and $y < 0$.
Then $|x| = x$ and $|y| = -y$, and so $|x|\,|y| = x(-y) = -xy$. On the other hand, as $x > 0$ and $y < 0$, it follows that $xy < 0$ and so $|xy| = -xy$.

$x < 0$ and $y > 0$.
This follows from the previous case by swapping x and y.

$x < 0$ and $y < 0$.

Then $|x| = -x$ and $|y| = -y$, and so $|x|\,|y| = (-x)(-y) = xy$. On the other hand, as $x < 0$ and $y < 0$, it follows that $xy > 0$ and so $|xy| = xy$.

This proves (8.3).

Next we prove (8.4). First observe that from the definition of $|\cdot|$, it follows that for any real $x \in \mathbb{R}$, $|x| \geq x$: indeed if $x \geq 0$, then $|x| = x$, while if $x < 0$, then $-x > 0$, and so $|x| = -x > 0 > x$. From (8.3), we also have $|-x| = |-1\cdot x| = |-1||x| = 1|x| = |x|$, for all $x \in \mathbb{R}$, and so it follows that $|x| = |-x| \geq -x$ for all $x \in \mathbb{R}$. We have the following cases:

$x + y \geq 0$.

Then $|x+y| = x+y$. As $|x| \geq x$ and $|y| \geq y$, we obtain $|x| + |y| \geq x + y = |x+y|$.

$x + y < 0$.

Then $|x+y| = -(x+y)$. Since $|x| \geq -x$ and $|y| \geq -y$, it follows that $|x| + |y| \geq -x + (-y) = -(x+y) = |x+y|$.

This proves (8.4). □

The second of these inequalities, (8.4), is often called the *triangle inequality*. If you draw a triangle in the plane, with sides of length a, b and c, then $c \leq a + b$; to go from one vertex of a triangle to another, it's never longer to go down the side connecting them than *via* the other two sides. The equation $|x+y| \leq |x| + |y|$ is just the special case when all three points of the triangle are on a line.

Remark 8.19. We won't go into it in this course, but this is going in the direction of why analysis is such an important part of mathematics. It's often useful to be able to make precise things like: *this* shape is more like a circle than *that* shape; the distance you have to travel in the *space of shapes* to get to the circle is shorter. Or the same thing with similarity of shapes replaced by similarity of functions, or of many other things. One real-world application: if you use Amazon, it recommends you products which were bought by people whose purchase history is similar to yours. But it would take far too much computing time to find all users on Amazon whose purchase history is similar to yours and look up what they bought that you don't have, every time you log on.

What is much quicker is for Amazon to keep track of a few 'model users' whose purchase histories are fairly different, and for each model user a list of what people similar to the model user bought. Then when you log on, Amazon just has to look up the one or two model users whose purchase history is closest to yours, and output the list of what people similar to them bought (minus the things you already have). Why does that work? Well, because of the triangle inequality. The distance (in purchase history space) between your purchase history and a model user M is maybe 3 units, and the similarity between M and any one of the people they are similar to, say N, is at most 5 units. Why is something that N bought likely to be a good suggestion for you? Well, because you and N cannot be more than $3 + 5 = 8$ units apart: in this 'purchase history space' the triangle inequality holds. You have similar preferences to N, so you might well like something they bought.

In MA203 you can study 'metric spaces'—the abstract idea of a space together with an idea of the distance between two points in the space. All one assumes is that two points are at zero distance if and only if they are the same point (otherwise the distance is positive) and the triangle inequality: the distance between any two points is never more than going *via* a third. Amazingly, you can say quite a lot about these spaces without assuming anything more.

8.3 Sample exercises

Exercise 8.1. *Fill in the following table for each of the sets $S = A, B, .., E$ below.*

An upper bound	*A lower bound*	*Is S bounded?*	$\sup S$	$\inf S$	*If* $\sup S$ *exists, then is* $\sup S$ *in S?*	*If* $\inf S$ *exists, then is* $\inf S$ *in S?*	$\max S$	$\min S$

(a) $A = \{x \in \mathbb{R} \mid 0 \leq x < 1\}$

(b) $B = \{x \in \mathbb{R} \mid 0 \leq x \leq 1\}$

(c) $C = \{x \in \mathbb{R} \mid x \in \mathbb{N} \text{ and } x \text{ prime}\}$

(d) $D = \{0, 2, 5, 2016\}$

(e) $E = \left\{(-1)^n \left(1 + \frac{1}{n}\right) \,\middle|\, n \in \mathbb{N}\right\}$

Exercise 8.2. *Let A and B be non-empty subsets of $\mathbb{R}$ that are bounded above and define*

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

(a) Show that $\sup A + \sup B$ *is an upper bound for $A + B$.*
Deduce that $\sup(A + B)$ *exists and that* $\sup(A + B) \leq \sup A + \sup B$.

(b) For any real number $\varepsilon > 0$, show that $(\sup A - \varepsilon) + (\sup B - \varepsilon)$ *is* ***not*** *an upper bound for $A + B$.*
Deduce that $\sup(A + B) \geq \sup A + \sup B - 2\varepsilon$, *for every $\varepsilon > 0$.*

(c) Show that $\sup(A + B) = \sup A + \sup B$.

Exercise 8.3. *Let S be a non-empty set of positive real numbers, and define $S^{-1} = \left\{\frac{1}{x} \,\middle|\, x \in S\right\}$.*

(a) Show that, if $\inf S = 0$, *then S^{-1} is not bounded above.*

(b) Show that, if $\inf S > 0$, *then S^{-1} is bounded above and* $\sup S^{-1} = \frac{1}{\inf S}$.

Exercise 8.4. *In this exercise we define the* floor *and* ceiling *functions. For any $x \in \mathbb{R}$ define the set $S_x = \{n \in \mathbb{Z} \mid n \leq x\}$.*

(a) Show that, for any $x \in \mathbb{R}$, the set S_x is non-empty and bounded above.

Hint: To show that $S_x \neq \varnothing$, you will need the Archimedean property.

(b) Show that $\sup S_x$ *exists and* $\sup S_x \in S_x$ *for any $x \in \mathbb{R}$. Explain why we obtain as a consequence that the following gives a proper definition of the* floor function $\lfloor\cdot\rfloor : \mathbb{R} \to \mathbb{Z}$

$$\lfloor x \rfloor = \max\{n \in \mathbb{Z} \mid n \leq x\}, \quad x \in \mathbb{R}.$$

(c) Show that $x - 1 < \lfloor x \rfloor \leq x$, for every $x \in \mathbb{R}$.

(d) Adapt (a)) and (b)) to explain why the following gives a proper definition of the ceiling function $\lceil\cdot\rceil : \mathbb{R} \to \mathbb{Z}$

$$\lceil x \rceil = \min\{n \in \mathbb{Z} \mid n \geq x\}, \quad x \in \mathbb{R}.$$

(e) Show that $\lfloor\sqrt{k^2 + k}\rfloor = k$ for all $k \in \mathbb{N}$.

Exercise 8.5. *Let S be a subset of $\mathbb{R}$ that does not have a maximum. Show that, for every $x \in S$, there is $y \in S$ with $y > x$.*

Hint: Deal separately with the two cases: (i) S has a supremum; (ii) S has no supremum.

Exercise 8.6. *Prove that if x, y are real numbers, then $||x| - |y|| \leq |x - y|$.*

8.4 Comments on selected activities

Comment on Activity 8.1. What is missing is that we don't take into account that the surface is slanted. By the logic we used, if we have a flat 1 by 1 sheet, standing vertically, we should estimate its area by integrating from 0 to 1 the length of the line which is a horizontal slice through, namely 1. So the surface area should be $\int_{x=0}^{1} 1\,\mathrm{d}x = 1$, which is correct; this sheet isn't slanted.

But now put the sheet at a $\frac{\pi}{4}$ angle (45 degrees) to the vertical. A horizontal slice through is still a length 1 line, so now (by the logic we used) the surface area should be

$$\int_{x=0}^{1/\sqrt{2}} 1\,\mathrm{d}x = \tfrac{1}{\sqrt{2}}\,,$$

since the vertical height of the sheet is now $1/\sqrt{2}$. Of course this is nonsense; the sheet hasn't really become smaller just because it is slanted. The same error has been made in calculating the area of the sphere.

And now you should decide if you are really convinced by Archimedes' argument for the volume—if so, why?

8.5 Solutions to exercises

Solution to Exercise 8.1.

(a) 1 is one upper bound, and is in fact the supremum of A. 0 is a lower bound, and the infimum of A. The set is bounded. As 0 is an element of A, but 1 is not, the set has a minimum (namely 0), but no maximum.

(b) As (a), except that now the supremum (1) is in B, so B has a maximum.

(c) There is no upper bound (this is equivalent to saying that there are infinitely many prime numbers). There is a lower bound, and the infimum and minimum are both equal to 2, the smallest prime number. The set is not bounded.

(d) Any *finite* set of real numbers has a maximum and a minimum, and the rest of the answer follows. In this case, the maximum is 2016, and the minimum is 0.

(e) It's worth evaluating the first few elements of the sequence $(-1)^n(1+\frac{1}{n})$, to get an idea of what's going on. These elements are $-2, 3/2, -4/3, 5/4, \ldots$. This set E has a minimum and a maximum, namely -2 and $3/2$ respectively, and the answers to all the other questions follow.

Solution to Exercise 8.2.

(a) A general element of $A+B$ is of the form $x+y$ for some $x \in A$ and $y \in B$. For any such pair of elements, we have that $x \le \sup A$ and $y \le \sup B$ (since $\sup A$ is an upper bound for A and $\sup B$ is an upper bound for B) and hence $x+y \le \sup A + \sup B$. Therefore indeed $\sup A + \sup B$ is an upper bound for $A+B$.

This proves that $A+B$ is bounded above, and the set is non-empty since both A and B are. Hence $A+B$ has a supremum, which is certainly at most the upper bound $\sup A + \sup B$.

(b) Since $\sup A - \varepsilon$ is not an upper bound for A, there is some $x \in A$ with $x > \sup A - \varepsilon$. Similarly, there is some $y \in B$ with $y \ge \sup B - \varepsilon$. Now $x+y$ is an element of $A+B$ with $x+y > \sup A - \varepsilon + \sup B - \varepsilon = \sup A + \sup B - 2\varepsilon$. Hence $\sup A + \sup B - 2\varepsilon$ is not an upper bound for $A+B$. Moreover, no real number less than $\sup A + \sup B - 2\varepsilon$ is an upper bound for $A+B$, so the supremum of $A+B$ (which *is* an upper bound for $A+B$) is at least $\sup A + \sup B - 2\varepsilon$.

(c) We have seen in (a) that $\sup(A+B) \le \sup A + \sup B$. If $\sup(A+B) < \sup A + \sup B$, then there is a positive real number ε such that $\sup(A+B) < \sup A + \sup B - 2\varepsilon$ (to be specific, set $\varepsilon = \frac{1}{3}(\sup A + \sup B - \sup(A+B)))$, but this contradicts (b). Hence also $\sup(A+B) \ge \sup A + \sup B$, and the equality follows.

Solution to Exercise 8.3. One key idea is that, provided we stay within the realm of positive real numbers, a larger element of S corresponds to a smaller element of S^{-1}.

(a) We prove the contrapositive: if S^{-1} is bounded above, then $\inf S \neq 0$. Take an upper bound M for S^{-1}. [This is what we gain: we can get our hands on a specific object M, and reason about it.] Note that $M > 0$, as S contains at least one positive real number. Then $x \leq M$ for every element $x \in S^{-1}$, which is equivalent to saying that $1/z \leq M$ for every element $z \in S$. [Because the elements of S^{-1} are exactly the elements of the form $1/z$ for $z \in S$.] In turn, this is equivalent to saying that $z \geq 1/M$ for every $z \in S$. [We use here that both M and z (an element of S) are positive.] This means exactly that the positive real number $1/M$ is a lower bound for S. The infimum of S is then at least $1/M$, and therefore greater than 0.

(b) Suppose now that $s = \inf S > 0$. We claim that $1/s$ is an upper bound for S. [It's important to have an idea of what is going on, so that you can see that this is what is likely to be true.] Indeed, as s is a lower bound for S, we have $s \leq z$ for every $z \in S$, and therefore $1/z \leq 1/s$ for every $z \in S$. This means that $x \leq 1/s$ for every $x \in S^{-1}$, i.e., that indeed $1/s$ is an upper bound for S^{-1}.

What do we have left to prove? We have seen that S^{-1} is bounded above, and that $1/\inf S = 1/s$ is an upper bound for S^{-1}. We still need to show that $1/s$ is the *least* upper bound for S^{-1}. Suppose then that $0 < u < 1/s$, i.e., $1/u > s$. As s is the infimum of S, it follows that $1/u$ is not a lower bound for S, in other words there is some $z \in S$ with $z < 1/u$, or equivalently $u < 1/z$. But now $1/z$ is an element of S^{-1}, so u is not an upper bound for S^{-1}. Hence indeed $1/s$ is the supremum of S^{-1}, as required.

(By the way, normally we do not attach any meaning to S^{-1} when S is a set: sets don't have "inverses". If, in the future, you want the notation to mean what it does here, you either have to define it afresh, or you could say "where, for a set S of positive real numbers, S^{-1} is as in Exercise 8.3".)

Solution to Exercise 8.4.

(a) The set S_x is certainly bounded above by x, so the main issue is to show that S_x is non-empty. If $x \geq 0$, then $0 \in S_x$, so we can assume x is negative. Once you've realised that, you should see that the Archimedean property is exactly what we need: given any (negative) x, there is an integer m such that $-m \geq -x$, and so $m \leq x$. The integer m is then in the set S_x, so S_x is non-empty.

(b) For each x, the set S_x is non-empty and bounded above, so has a supremum $\sup S_x$. Moreover, the set S_x is a set of integers. You have seen in the first half of the course that a set of integers bounded above has a maximum, so the set has a maximum element (which is the same as the supremum). Thus, for every real number x, $\max\{n \in \mathbb{Z} \mid n \leq x\}$ is a well-defined integer.

(c) The fact that $\lfloor x \rfloor \leq x$ is immediate from the definition. To see the other inequality, suppose that $\lfloor x \rfloor \leq x - 1$. Then $m = \lfloor x \rfloor + 1$ is an integer with $m \leq (x-1) + 1 = x$, so m is in the set $\{n \in \mathbb{Z} \mid n \leq x\}$, and $m > \lfloor x \rfloor$, contradicting the choice of $\lfloor x \rfloor$ as the maximum of this set.

(d) Similar to (a) and (b).

(e) Evidently $k \leq \sqrt{k^2+k}$, so $k \in S_{\sqrt{k^2+k}}$. On the other hand, $k + 1 > \sqrt{k^2+k}$: both sides are non-negative, so this inequality is equivalent to $(k+1)^2 > k^2 + k$, which is indeed true. Thus no integer greater than k is in $S_{\sqrt{k^2+k}}$, and hence k is the maximum of $S_{\sqrt{k^2+k}}$, i.e., $k = \lfloor \sqrt{k^2+k} \rfloor$, whenever $k \in \mathbb{N}$.

Solution to Exercise 8.5.

Recall the definition: if S has a supremum s, and $s \in S$, then s is the maximum of S. (Otherwise S has no maximum.)

So there are two ways that S could fail to have a maximum: (i) S has a supremum, s, but s is not a member of S; (ii) S has no supremum.

In case (i), take any element x of S. Then $x \leq s$ because s is an upper bound for S, but $x \neq s$ since x is in S and s isn't. Thus $x < s$, and so x is not an upper bound for S. That means exactly that there is some $y \in S$ with $x < y$.

In case (ii), either S is empty or S is not bounded above. In the first case there is nothing to check (i.e., there is no element x in S that could possibly be a counterexample). In the second case, any element x of S is not an upper bound for S, and this again means that there is some $y \in S$ with $x < y$.

Actually, you don't need to divide into cases: you can argue as follows. Suppose S has no maximum, and let x be any element of S. Then x is not a supremum of S. Certainly x is less than any upper bounds of S, so it must be that x is not itself an upper bound of S. This means exactly that there is some $y \in S$ with $x < y$.

Solution to Exercise 8.6.

One can do this by breaking into cases, depending on the signs of x and y. Here's an alternative approach, based on the inequality $|a + b| \le |a| + |b|$, valid for all real numbers a and b, that we proved in lectures. Applying this with $a = x - y$ and $b = y$ gives $|x| \le |x - y| + |y|$, and so $|x| - |y| \le |x - y|$. Similarly $|y| - |x| \le |y - x| = |x - y|$. Now, $||x| - |y||$ is equal to either $|x| - |y|$ or $-(|x| - |y|) = |y| - |x|$, and so it follows that $||x| - |y|| \le |x - y|$.

9 Analysis: Sequences and limits

If we have a function $f : \mathbb{R} \to \mathbb{R}$, what does $f'(0)$, the derivative of f at 0, *mean*? You probably would say something like 'the slope of the tangent to $f(x)$ at $x = 0$'. Well, yes—but how can we find what that is, or even say if it exists? If the function has some funny kink at zero, like $f(x) = |x|$, then this phrase 'the tangent..' doesn't make much sense. Any line you draw doesn't look much like a tangent.

One way is to imagine drawing a line from $\big(0, f(0)\big)$ to $\big(h, f(h)\big)$ where h is 'small'. Intuitively, the slope of this line—which is $\frac{f(h)-f(0)}{h-0}$—should be more or less what we want. If we make h smaller and smaller, we should get closer to the right answer. That is, basically, the definition of 'derivative'. But in order to make sense of it, we need to formalise what it means to 'get closer to the right answer'. In other words, we need to say what it means for a 'sequence' of real numbers to 'converge to a limit'.

9.1 Sequences

The notion of a sequence occurs in ordinary conversation. An example is the phrase "an unfortunate sequence of events". In this case, we envision one event causing another, which in turn causes another event and so on. We can identify a *first* event, a *second* event, etcetera.

A sequence of real numbers is a list

$$(a_1, a_2, a_3, \dots)$$

of real numbers, where there is the *first* number (namely a_1), the *second* number (namely a_2), and so on. For example,

$$(1, \tfrac{1}{2}, \tfrac{1}{3}, \dots)$$

is a sequence of real numbers. The first number is 1, the second number is $\frac{1}{2}$ and so on. (There may not be a connection between the numbers appearing in a sequence.) If we think of a_1 as $f(1)$, a_2 as $f(2)$, and so on, then it becomes clear that a sequence of real numbers is a special type of function, namely one with domain $\mathbb{N}$ and co-domain $\mathbb{R}$. This leads to the following formal definition.

Definition 9.1. A *sequence* of real numbers is a function $f : \mathbb{N} \to \mathbb{R}$.

Only the notation is somewhat unusual. Instead of writing $f(n)$ for the value of f at a natural number n, we write a_n. The entire sequence is then written in any one of the following ways:

$$(a_n)_{n\in\mathbb{N}}, \ (a_n)_{n=1}^{\infty}, \ (a_n)_{n\geq 1}, \ (a_n).$$

In $(a_n)_{n=1}^{\infty}$, the ∞ symbol indicates that the assignment process $1 \mapsto a_1, 2 \mapsto a_2, \dots$ continues indefinitely. In these notes, we shall normally use the notation $(a_n)_{n\in\mathbb{N}}$. In general, the terms of a sequence need not be real numbers, but in these notes we shall only be dealing with sequences whose entries are real numbers, so we shall simply refer to them as *sequences* from now on.

The n-th term a_n of a sequence may be defined explicitly by a formula involving n, as in the example given above:

$$a_n = \tfrac{1}{n}, \quad n \in \mathbb{N}.$$

It might also sometimes be defined recursively. For example,

$$a_1 = 1, \quad a_{n+1} = \tfrac{n}{n+1} a_n \text{ for } n \in \mathbb{N}.$$

(Write down the first few terms of this sequence.)

Example 9.2.

(i) $\left(\frac{1}{n}\right)_{n\in\mathbb{N}}$ is a sequence with the n-th term given by $\frac{1}{n}$, for $n \in \mathbb{N}$. This is the sequence

$$\left(1,\ \tfrac{1}{2},\ \tfrac{1}{3},\ \dots\right).$$

(ii) $\left(1 + \frac{1}{n}\right)_{n\in\mathbb{N}}$ is a sequence with the n-th term given by $1 + \frac{1}{n}$, for $n \in \mathbb{N}$. This is the sequence

$$\left(2,\ \tfrac{3}{2},\ \tfrac{4}{3},\ \tfrac{5}{4},\ \tfrac{6}{5},\ \tfrac{7}{6},\ \dots\right).$$

(iii) $\left((-1)^n\left(1 + \frac{1}{n}\right)\right)_{n\in\mathbb{N}}$ is a sequence with the n-th term given by $(-1)^n\left(1 + \frac{1}{n}\right)$, for $n \in \mathbb{N}$. This is the sequence

$$\left(-2,\ \tfrac{3}{2},\ -\tfrac{4}{3},\ \tfrac{5}{4},\ -\tfrac{6}{5},\ \tfrac{7}{6},\ \dots\right).$$

(iv) $\left((-1)^n\right)_{n\in\mathbb{N}}$ is a sequence with the n-th term given by $(-1)^n$, for $n \in \mathbb{N}$. This sequence is simply

$$(-1,\ 1,\ -1,\ 1,\ -1,\ 1,\ \dots)$$

with the n-th term equal to -1 if n is odd, and 1 if n is even.

(v) $(1)_{n\in\mathbb{N}}$ is a sequence with the n-th term given by 1, for $n \in \mathbb{N}$. This is the constant sequence

$$(1,\ 1,\ 1,\ \dots).$$

(vi) $(n)_{n\in\mathbb{N}}$ is a sequence with the n-th term given by n, for $n \in \mathbb{N}$. This is the strictly increasing sequence

$$(1,\ 2,\ 3,\ \dots).$$

(vii) $\left(\frac{1}{1^1} + \frac{1}{2^2} + \frac{1}{3^3} + \dots + \frac{1}{n^n}\right)_{n\in\mathbb{N}}$ is a sequence with the n-th term given by $\frac{1}{1^1} + \frac{1}{2^2} + \frac{1}{3^3} + \dots + \frac{1}{n^n}$, for $n \in \mathbb{N}$. This is the sequence of 'partial sums'

$$\left(\frac{1}{1^1},\quad \frac{1}{1^1} + \frac{1}{2^2},\quad \frac{1}{1^1} + \frac{1}{2^2} + \frac{1}{3^3},\quad \dots\right).$$

(viii) $\left(n^{1\,000\,000}2^{-n}\right)_{n\in\mathbb{N}}$ is the sequence whose nth term is $n^{1\,000\,000}2^{-n}$. Its first term is $\frac{1}{2}$, its second term is a huge integer with about 30 000 decimal digits, its third term is even bigger, and if you keep calculating, the terms will just keep getting bigger and bigger as long as you have patience to keep going.

(ix) $\left(\frac{2}{n} + \frac{(-1)^n}{n}\right)_{n\in\mathbb{N}}$ is the sequence whose terms are

$$\left(\tfrac{1}{1},\ \tfrac{3}{2},\ \tfrac{1}{3},\ \tfrac{3}{4},\ \tfrac{1}{5},\ \tfrac{3}{6}, \dots\right).$$

9.2 Limit of a convergent sequence

A sequence can be graphed. For instance, the first 7 points of the graph of the sequence $\left(\frac{1}{n}\right)_{n\in\mathbb{N}}$ are displayed in Figure 9.1.

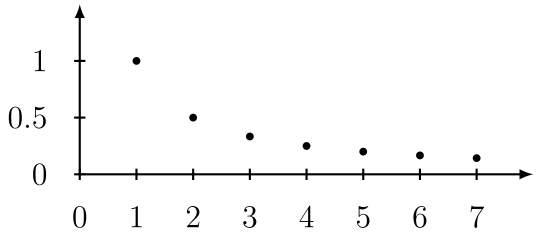


Figure 9.1: First 7 points of the graph of the sequence $\left(\frac{1}{n}\right)_{n\in\mathbb{N}}$.

This portion of the graph suggests that the terms of the sequence $\left(\frac{1}{n}\right)_{n\in\mathbb{N}}$ "tend toward 0" as n increases. This is consistent with the idea of convergence that you might have encountered before: a sequence $(a_n)_{n\in\mathbb{N}}$ converges to some real number L, if the terms a_n get "closer and closer" to L as n "increases without bound". Symbolically, this is represented using the notation

$$\lim_{n\to\infty} a_n = L,$$

where L denotes the limit of the sequence. If there is no such finite number L to which the terms of the sequence get arbitrarily close, then the sequence is said to diverge.

The problem with this characterization is its imprecision. Exactly what does it mean for the terms of a sequence to get "closer and closer", or "as close as we like", or "arbitrarily close" to some number L? Even if we accept this apparent ambiguity, how would one use the definition given in the preceding paragraph to prove theorems that involve sequences? Since sequences are used throughout analysis, the concepts of their convergence and divergence must be carefully defined.

For example, the terms of $\left(1+\frac{1}{n}\right)_{n\in\mathbb{N}}$ get "closer and closer" to 0 (indeed the distance to 0 keeps decreasing), but its limit is 1:

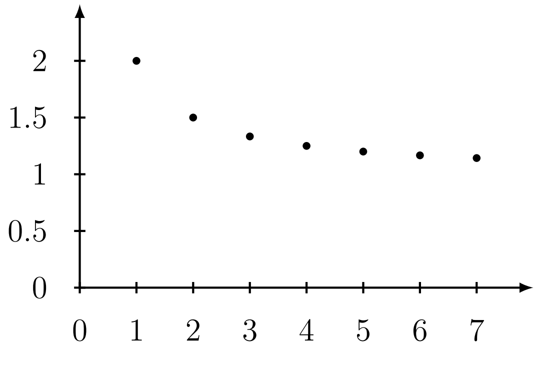


Figure 9.2: First 7 points of the graph of the sequence $\left(1+\frac{1}{n}\right)_{n\in\mathbb{N}}$.

Some of the terms of $\left((-1)^n\left(1+\frac{1}{n}\right)\right)_{n\in\mathbb{N}}$ get "as close as we like" or "arbitrarily close" to 1, but the sequence has no limit:

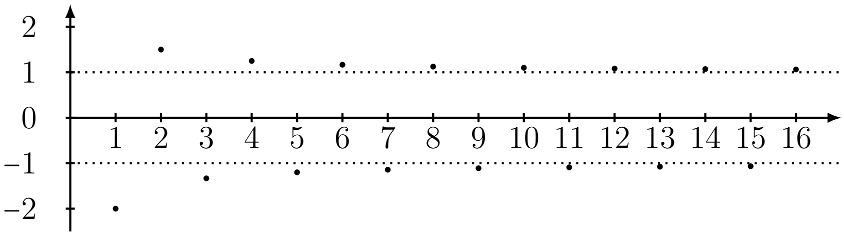


Figure 9.3: First sixteen points of the graph of the sequence $\left((-1)^n\left(1+\frac{1}{n}\right)\right)_{n\in\mathbb{N}}$.

The terms of $\left(n^{1\,000\,000}2^{-n}\right)_{n\in\mathbb{N}}$, despite all appearances, do eventually get smaller. The first few terms—indeed, the first few million terms—are enormous. But eventually (when n is very large) the nth term is guaranteed to be very close to 0.

Finally, the terms of $\left(\frac{2}{n}+\frac{(-1)^n}{n}\right)_{n\in\mathbb{N}}$ don't always get closer to 0. If you look at the nth term where n is very large, that term will be very tiny—it will be either $\frac{1}{n}$ or $\frac{3}{n}$ depending on whether n is odd or even—but the even-numbered terms are almost three times as big as the odd-numbered term before: it keeps on getting *further* from 0:

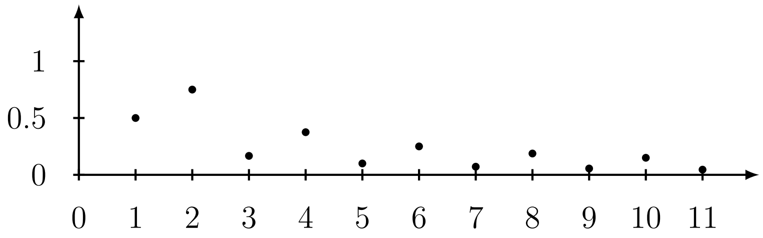


Figure 9.4: First 11 points of the graph of the sequence $\left(\frac{2}{n}+\frac{(-1)^n}{n}\right)_{n\in\mathbb{N}}$.

So which of the sequences from Example 9.2 converge to 0? The answer is: the ones where (eventually, maybe when n is very large) the terms are guaranteed to be close to 0. These are examples (i), (viii) (even though the first few terms are enormous and growing), and (ix) (even though each even term is further from 0 than the previous odd term). Sequence (ii) does converge, but to the limit 1 not 0 (even though the terms are always getting closer to 0). Sequence (iii) doesn't converge to any limit (even though lots of terms are very close to 1, and lots more to −1). The same is true for sequence (iv). The sequence (v) (obviously!) converges to 1.

The sequence (vi) 'obviously' doesn't converge; it just keeps getting bigger, so it can't possibly stay close to any fixed real number (whatever candidate limit you pick, when n is large enough the nth term of the sequence is going to be much bigger than your candidate limit). And finally the sequence (vii) does converge, but to a number bigger than 1. It's obvious the terms are all at least 1—but how do I know it converges? More on that later.

More generally, we want to say a sequence $\big(a_n\big)_{n\in\mathbb{N}}$ converges to the real number L if, when n is very large, a_n is guaranteed to be close to L. The following, which formalises that idea, is the key definition for this chapter.

Definition 9.3. The sequence $(a_n)_{n\in\mathbb{N}}$ is said to *converge to* L if for every real number $\varepsilon > 0$, there exists an $N \in \mathbb{N}$ (possibly depending on ε) such that for all $n > N$,

$$|a_n - L| < \varepsilon.$$

Then we say that $(a_n)_{n\in\mathbb{N}}$ is *convergent with limit* L and write

$$\lim_{n\to\infty} a_n = L\,.$$

We may also say that $(a_n)_{n\in\mathbb{N}}$ *tends to* L.

If there does not exist a number L such that $\lim\limits_{n\to\infty} a_n = L$, then the sequence $(a_n)_{n\in\mathbb{N}}$ is said to be *divergent*.

This definition is complicated; there are several quantifiers to deal with. Written in logical notation, we say $\big(a_n\big)_{n\in\mathbb{N}}$ converges to L if

$$\forall\varepsilon > 0\,, \exists N \in \mathbb{N} \text{ such that } \forall n > N\,, |a_n - L| < \varepsilon\,.$$

Remember, you need to *understand* this definition not just memorise it—and the English text version is easier to understand!

Warning 9.4. As we saw back in Chapter 3, if you swap around the order of quantifiers you can change the meaning of a logical statement. This is the case here: if you change around the order of the quantifiers in 'converges to L' then you will get a statement which means *something*, but *not* any more what you want!

You can try to prove a sequence converges by following the standard strategies. That is, the first quantifier in the definition is $\forall\varepsilon > 0$, a universal statement. So the first line of the proof should be 'Given $\varepsilon > 0$' and then you need to prove the statement

$$\exists N \in \mathbb{N} \text{ such that } \forall n > N\,, |a_n - L| < \varepsilon\,.$$

where now you know that ε is some fixed positive real number. Now, this statement is an existential statement: the easiest way to prove it is to *find an* N *which works.* In other words, the next line of the proof is going to be something like 'We choose $N = ..$'. Having chosen N, you need to prove

$$\forall n > N\,, |a_n - L| < \varepsilon\,.$$

Back to a universal statement! So: 'Given $n > N$.' And finally you need to prove

$$|a_n - L| < \varepsilon$$

which is just a calculation.

The obvious question is: But how should we choose N..? The answer is pretty similar to what we saw in the proof of Exercise 8.9. That is, you need it to be big enough that the final calculation works. At some point when you are proving $|a_n - L| < \varepsilon$, you will say 'because $n > N$ and we chose $N = ...$'. You will *not* be able to write in the value for N until you try to do this calculation: you'll need to work backwards.

Activity 9.1. *Try to prove, for each of the sequences in Example 9.2, that the comment above is accurate, i.e. (i) converges to* 0*, and so on.*

Some of these sequences are harder to work with than others. If you couldn't do any of them, the worked examples that follow should help. If you could do all of them except (vii) and (viii), you're doing very well. (If you think you have proofs for (vii) and (viii), then either you are doing exceptionally well, or you saw this material before, or you assumed something unjustified!)

Note that $|a_n - L| < \varepsilon$ if and only if $a_n \in (L - \varepsilon, L + \varepsilon)$. Hence pictorially, for a convergent sequence with limit L, this definition means the following, as illustrated in Figure 9.5.

Pick any $\varepsilon > 0$, and consider the shaded strip of width ε around the horizontal line passing through L. Then one can find an $N \in \mathbb{N}$, large enough, such that all the terms a_n of the sequence, for $n > N$, lie in the shaded strip.

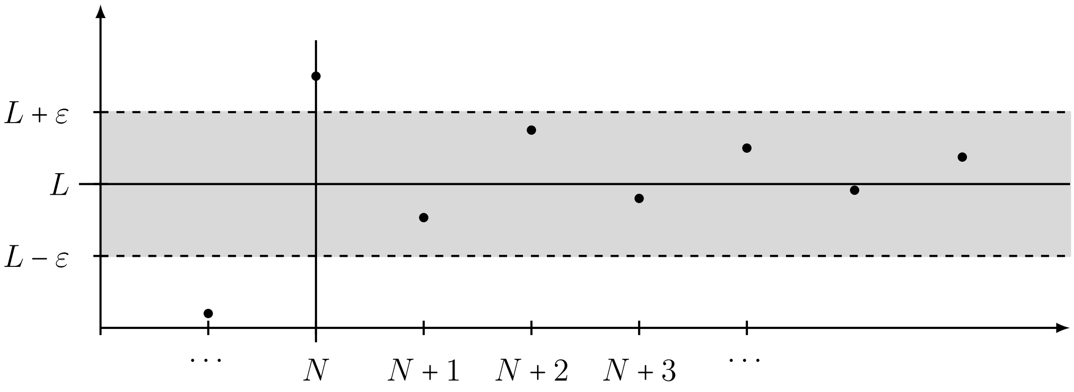


Figure 9.5: Convergence of a sequence with limit L.

It is *definitely* worth keeping this picture in mind for the rest of the chapter. Of course you can do everything in Analysis just by sticking to the algebra and logic without ever drawing a picture, but (at least for most people) trying to do this is a good way to get confused and make errors.

Critical

A sequence is a list of numbers. $(1, 2, 3, 1, 17, \dots)$ is a sequence. So is $(a_1, a_2, a_3, \dots)$ (even if we don't know what the number a_3 actually is).
a_n is not a sequence: first, I don't know what n should be, second, even if you tell me, a_n is one number, one number is not a list.
You should neither think, nor write, as if one number converges. When we write $|a_n - L| < \varepsilon$, this is not 'one statement that eventually gets true if the sequence converges'. A statement is either true or false, it doesn't change over time. This is a predicate, it might be true or false depending on the value of n that we put in. In the definition of convergence, the idea is: if we put any sufficiently large n in, then we will get a true statement.
The picture above is a good picture. In particular, you should notice that the points we plotted aren't moving, nothing is 'getting closer to the line L'. Yes, we will write 'the sequence tends to L' sometimes, because this is standard, but it is bad language. The sequence converges.

9.2.1 Proving convergence of a sequence

Example 9.5. Show that $\exists N\,,\ \forall n > N\,,\ \left|\frac{1}{2n+5\sin n} - 0\right| < \frac{1}{1000}$.

This example is what we would have to show in a proof of convergence if we happened to be given $\varepsilon = \frac{1}{1000}$; of course, if you want to prove convergence, your proof needs to work for *every* $\varepsilon > 0$ you might be given; your choice of N would depend on the ε you were given.

Proof. The denominator $2n + 5\sin n$ is painful to work with. But $\sin n$ is always between 1 and -1, so if $n \geq 5$ then we have $n + 5\sin n \geq 0$.

Adding n to both sides, we see that if $n \geq 5$ then we have $2n + 5\sin n \geq n$, so $\frac{1}{2n+5\sin n} \leq \frac{1}{n}$. So (finally) we should choose $N = 1000$. Then for each $n > N$ we have

$$\left|\frac{1}{2n+5\sin n} - 0\right| = \frac{1}{2n+5\sin n} \leq \frac{1}{n} < \frac{1}{N} = \frac{1}{1000}$$

which is what we wanted. □

Let's notice two things about this proof. One, it is quite short and easy. It does not find 'the best' N, which (in fact) is about 500. But that is irrelevant: it works, that is all we need, and finding 'the best' N is *a waste of time* because you're not asked to find it.

Two, we don't actually know what N we should choose until we do some calculations. So even though a 'model' proof of 'there exists N such that...' should start with 'Let N be..' and then go on to check that this particular choice works, we're never going to come up with a proof in that order. The 'model proof' is:

Proof. Let $N = 1000$.

Then for all $n > N$, we have $n + 5\sin n \geq 0$, so $2n + 5\sin n \geq n$, so

$$\left|\frac{1}{2n+5\sin n} - 0\right| = \frac{1}{2n+5\sin n} \leq \frac{1}{n} < \frac{1}{N} = \frac{1}{1000}$$

which is what we wanted. □

If you want to write a proof that looks like this—and you do—the only way to do it is to leave a blank space to fill in the 'Let $N = ...$' later, then start thinking about the calculation. That will be a feature of all our proofs of convergence.

Let's now prove that some sequences converge (and that some other ones do not). These proofs will look a bit complicated at first: but when we want to prove a sequence $(a_n)_{n\in\mathbb{N}}$ converges to a limit L, the proof structure will be what is outlined above. It will start 'Given $\varepsilon > 0$', and then there will be a choice of N as in the model proof above, and the rest of the proof will look like the model proof: it will argue that $|a_n - L| < \varepsilon$ is true for all $n > N$. Usually, the choice of N will depend on the real number ε you are given.

Example 9.6. Show that $\left(\frac{1}{2n+5\sin n}\right)_{n\in\mathbb{N}}$ converges to 0.

We'll prove this by starting with the model proof above, and changing it so that it works for any $\varepsilon > 0$ and not just $\frac{1}{1000}$.

Proof. Given $\varepsilon > 0$, choose N to be the smallest integer which is at least as big as both 5 and $\frac{1}{\varepsilon}$.

Then for all $n > N$, we have $n + 5\sin n \geq 0$, so $2n + 5\sin n \geq n$, so

$$\left|\frac{1}{2n+5\sin n} - 0\right| = \frac{1}{2n+5\sin n} \leq \frac{1}{n} < \frac{1}{N} \leq \varepsilon$$

which is what we wanted. □

One important thing to notice here is that, while you should generally think of the ε you are given at the start of the proof as 'a very small number', it doesn't *have* to be. You might be given $\varepsilon = 100$, and your proof has to work in that situation. We need to say that N should be at least 5 in order to deal with this situation—to make sure $n + 5\sin n \geq 0$ is true—even though 'usually' $\frac{1}{\varepsilon}$ is much bigger than 5.

In order to avoid complicated phrases like 'the smallest integer which is at least as big as both 5 and $\frac{1}{\varepsilon}$' we make the following definitions.

Definition 9.7. The *ceiling* of a real number x, written $\lceil x \rceil$, is the smallest integer at least as big as than x; the *floor* of x, written $\lfloor x \rfloor$, is the largest integer which is not bigger than x.

Given a collection of real numbers $s_1, s_2, \dots, s_t$, we write $\max(s_1, ..., s_t)$ for the largest of them, and $\min(s_1, ..., s_t)$ for the smallest.

So 'the smallest integer which is at least as big as both 5 and $\frac{1}{\varepsilon}$' is simply $\max\left(5, \lceil \frac{1}{\varepsilon} \rceil\right)$.

You should now be able to do the following.

Activity 9.2. *Use the definition of the limit of a sequence to show that* $\left(\frac{1}{n}\right)_{n\in\mathbb{N}}$ *is a convergent sequence with limit* 0*.*

Here are some slightly harder worked examples.

Example 9.8. Use the definition of the limit of a sequence to show that $\left(1 + \frac{1}{2n^2-n}\right)_{n\in\mathbb{N}}$ is a convergent sequence with limit 1.

Proof. Given $\varepsilon > 0$, we choose $N = \lceil \frac{1}{\varepsilon} \rceil$.

Suppose $n > N$. We notice that whatever natural number n is, we have $2n^2 - n \geq n$. So we can write

$$\left|1 + \frac{1}{2n^2 - n} - 1\right| = \frac{1}{2n^2 - n} \leq \frac{1}{n} < \tfrac{1}{N} < \varepsilon \,,$$

which is what we wanted. □

Let's point out that (again) we get to this proof in a different order to the way it's written on paper. We know we want to eventually write down

$$\left|1 + \frac{1}{2n^2 - n} - 1\right| \leq \ldots < \varepsilon \,,$$

and we need to figure out what the ... steps in the middle are. We can simplify the left-hand-side, so we do that. We get something which is still not very simple, $\frac{1}{2n^2-n}$, but we notice that we can replace that with something bigger that still gets small when n is large, namely $\frac{1}{n}$. That is why we write that $2n^2 - n \geq n$ is true for all natural numbers n—to justify that indeed $\frac{1}{2n^2-n} \leq \frac{1}{n}$. And we know $\frac{1}{n} < \frac{1}{N}$ because we supposed that $n > N$. Finally, we choose N (really at this time, even though we write it at the top of the proof) so that we can write $\frac{1}{N} \leq \varepsilon$ and be done.

The critical step here is to notice that we can get rid of the complicated $\frac{1}{2n^2-n}$ by replacing it with something bigger that we can still show is smaller than ε in the end. There are lots of different choices we could have make; none is 'best', and this one is just the first one I happened to think of.

In Analysis, there are generally several 'right answers' and your job is just to pick one of them. In the proof above, we could just as well have noticed that $n^2 - n \geq 0$ is true for all natural numbers, and so $\frac{1}{2n^2-n} \leq \frac{1}{n^2}$. If we'd done that, most likely we would have chosen $N = \left\lceil \frac{1}{\sqrt{\varepsilon}} \right\rceil$ in order to get our ε at the end. That's also fine; it's not better or worse, it is an equally good different proof.

So how do you make the choice? Think about it and try something. There are three possibilities.
One, you find that what you tried isn't actually bigger (or you can't see how to prove it). Well, then you chose something too small, go back and try something bigger.
Two, you find that no matter how you calculate you cannot get the ε out at the end, you keep getting something big (like 1). Well, then you chose something too big, go back and try something smaller.
Three, your proof works. You don't need to care about whether you could've made another choice, you're done.

Example 9.9. Use the definition to show that $(a_n)_{n\in\mathbb{N}} = \left((-1)^n\left(1+\frac{1}{n}\right)\right)_{n\in\mathbb{N}}$ is a divergent sequence.

There is only one reason why a sequence might converge: the terms get close to a limit and stay there as you look at larger and larger n. But there are a few different ways a sequence $(a_n)_{n\in\mathbb{N}}$ can fail to converge. It might be that a_n bounces around crazily all over the place, sometimes very big and sometimes very small, no matter how big you make n. It might be that it just keeps getting bigger and bigger and eventually gets too big for any candidate limit (or the same thing but in the negative direction). It might be that the sequence doesn't look too crazy, but it jumps between being close to different real numbers. This (see Figure 9.3) is an example of the last: the odd-numbered terms get close to -1, and the even-numbered terms get close to 1.

It's very tempting to say 'we prove that -1 is not a limit. Then we prove that 1 is not a limit. And now we are done'. But this is *not enough.* If you say this, you didn't rule out the possibility that 0 is a limit, or π, or any other real number; you need to rule out *all* the real numbers.

So the proof has to start 'Given a real number L..' and then go on to show that L cannot be a limit. Let's see how that goes.

Proof. Given a real number L, we need to show that $\forall\varepsilon>0\,,\ \exists N\in\mathbb{N}\,,\ \forall n>N\,,\ |a_n-L|<\varepsilon$ is a false statement. That is, we need to prove the negation

$$\neg\forall\varepsilon>0\,,\ \exists N\in\mathbb{N}\,,\ \forall n>N\,,\ |a_n-L|<\varepsilon$$

which is

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

It turns out (you might want to plot the sequence: pictures help..!) that $\varepsilon=1$ is a good example.

Now we need to show that $\forall N\in\mathbb{N}\,,\ \exists n>N\,,\ |a_n-L|\geq 1$ is true. So: given any $N\in\mathbb{N}$, we need to show $\exists n>N\,,\ |a_n-L|\geq 1$. We need an example; a particular $n>N$.

At this point, we need to look at the terms a_n and what L is.

Case 1: $L\geq 0$. Choose n to be any odd integer greater than N, then we have

$$|a_n-L| = |L-a_n| = L-(-1)^n\left(1+\tfrac{1}{n}\right) = L+1+\tfrac{1}{n}$$

and since $L\geq 0$, this is strictly bigger than 1.

Case 2: $L<0$. Choose n to be any even integer greater than N. Then we have

$$|a_n-L| = (-1)^n\left(1+\tfrac{1}{n}\right)-L = 1+\tfrac{1}{n}-L$$

and since $L<0$ this is strictly bigger than 1.

Since these two cases are exhaustive, whatever L is given we proved that it is not a limit. So the sequence has no limit: it is divergent. □

Again, this proof is not written in the order we think of it. I got to this proof by staring at Figure 9.3 and noticing that all the odd-numbered terms are smaller than -1 (so they're not within distance one of any number L which is ≥ 0) and all the even-numbered terms are bigger than 1 (so they're not with distance one of any L which is ≥ 0). For this part, it really helps to look at the picture.

Well, but any L is either ≥ 0 or ≤ 0 (or both, if $L = 0$). So (whatever L is) we can choose $\varepsilon = 1$. Anything less than 1 would work too. (But anything bigger than 1 would not work: we would run into trouble with $L = 0$ and some other numbers.)

Activity 9.3. *Check that for any real number L, any sequence $(a_n)_{n\in\mathbb{N}}$, and any $\varepsilon > 0$, we have: '$\exists N \in \mathbb{N}\,,\ \forall n > N\,,\ |a_n - L| < \varepsilon$ is a false statement' if and only if 'there are infinitely many n such that $|a_n - L| \geq \varepsilon$'.*

We can (and generally we would) shorten the proof of Example 9.9 a bit:

Proof. Given a real number L, we choose $\varepsilon = 1$. We want to show there are infinitely many n such that $|a_n - L| \geq 1$.

Case 1: $L \geq 0$. For every odd integer n, we have

$$|a_n - L| = |L - a_n| = L - (-1)^n\big(1 + \tfrac{1}{n}\big) = L + 1 + \tfrac{1}{n}$$

and since $L \geq 0$, this is strictly bigger than 1.

Case 2: $L < 0$. For every even integer n, we have

$$|a_n - L| = (-1)^n\big(1 + \tfrac{1}{n}\big) - L = 1 + \tfrac{1}{n} - L$$

and since $L < 0$ this is strictly bigger than 1.

Since these two cases are exhaustive, whatever L is given we proved that it is not a limit. So the sequence has no limit: it is divergent. □

Try one yourself. Hint: in this case, any $\varepsilon > 0$ you choose will work.

Activity 9.4. *Prove that $(n)_{n\in\mathbb{N}}$ is divergent.*

We should also remember (from Chapter 3) that when we want to *use* a 'for all' statement, what we will do generally doesn't look like *proving* a 'for all' statement. As we've just seen, the first line of proving the statement $\lim\limits_{n\to\infty} a_n = L$ is generally going to be 'Given $\varepsilon > 0, \dots$'. What do we do if we are given that $(a_n)_{n\in\mathbb{N}}$ is a convergent sequence with limit L, and we want to prove something about (say) L?

The notation $\lim\limits_{n\to\infty} a_n$ suggests that the limit is unique. But is this actually well-defined, or could it be that there is a convergent sequence with two different limits?

Warning 9.10. We saw the sequence $\big((-1)^n(1 + \frac{1}{n})\big)_{n\in\mathbb{N}}$ before. It's tempting to say 'yes, this sequence has two limits, 1 and -1'. But this is false: this sequence doesn't tend to any limit at all; it is divergent, as we just proved.

Theorem 9.11. *A convergent sequence has a unique limit.*

The proof of this is a good example of how we can *use* the fact that a given sequence is convergent with a certain limit.

Proof. Formally, to prove 'a convergent sequence has a unique limit', we need to show two things:

(i) A convergent sequence has a limit;

(ii) A convergent sequence cannot have two different limits.

Here, (i) is true by the definition of convergence, so we only have to prove (ii).

In other words, if $\lim_{n\to\infty} a_n = L_1$ and $\lim_{n\to\infty} a_n = L_2$, then we have to prove $L_1 = L_2$.

Suppose that $(a_n)_{n\in\mathbb{N}}$ is a sequence which is convergent with limit both L_1 and L_2.

If $L_1 = L_2$, then there is nothing to prove. So suppose for a contradiction that this is not the case.

We choose $\varepsilon = \frac{1}{3}|L_2 - L_1|$, which is positive since $L_2 \neq L_1$.

Because $\lim_{n\to\infty} a_n = L_1$, there is some $N_1 \in \mathbb{N}$ such that if $n > N_1$ then a_n is guaranteed to be within ε of L_1. And since $\lim_{n\to\infty} a_n = L_2$ there is a (maybe different) $N_2 \in \mathbb{N}$ such that if $n > N_2$ then a_n is guaranteed to be within ε of L_2.

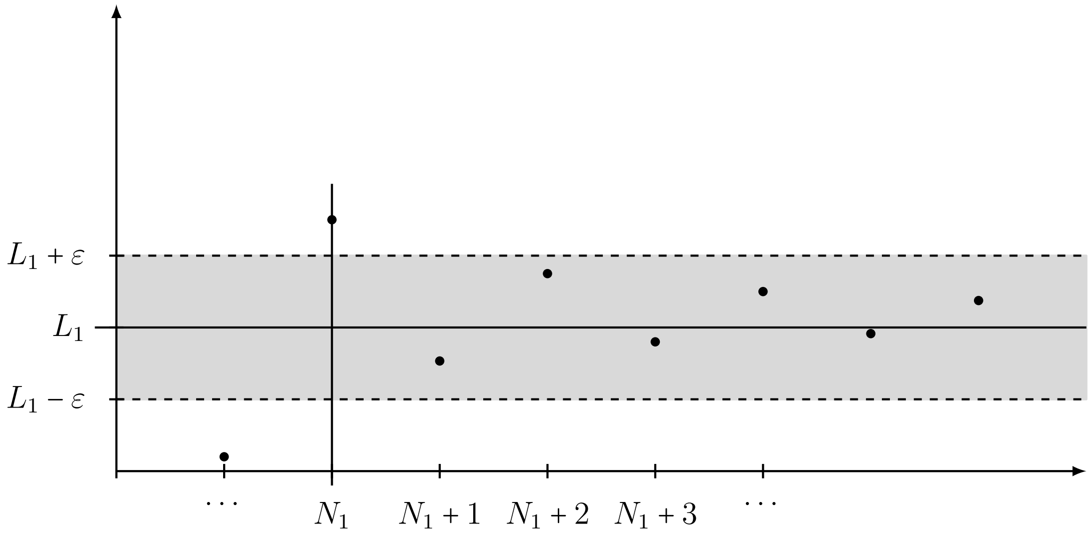
Now pick an n which is bigger than both N_1 and N_2 (for example $n = N_1 + N_2 + 1$). Then we have $|a_n - L_1| < \varepsilon$ and $|a_n - L_2| < \varepsilon$. So by the triangle inequality, we have

$$|L_2 - L_1| \le |L_2 - a_n| + |a_n - L_1| < 2\varepsilon = \tfrac{2}{3}|L_2 - L_1| < |L_2 - L_1|\,.$$

But this is a contradiction—$|L_2 - L_1|$ cannot be smaller than itself. □

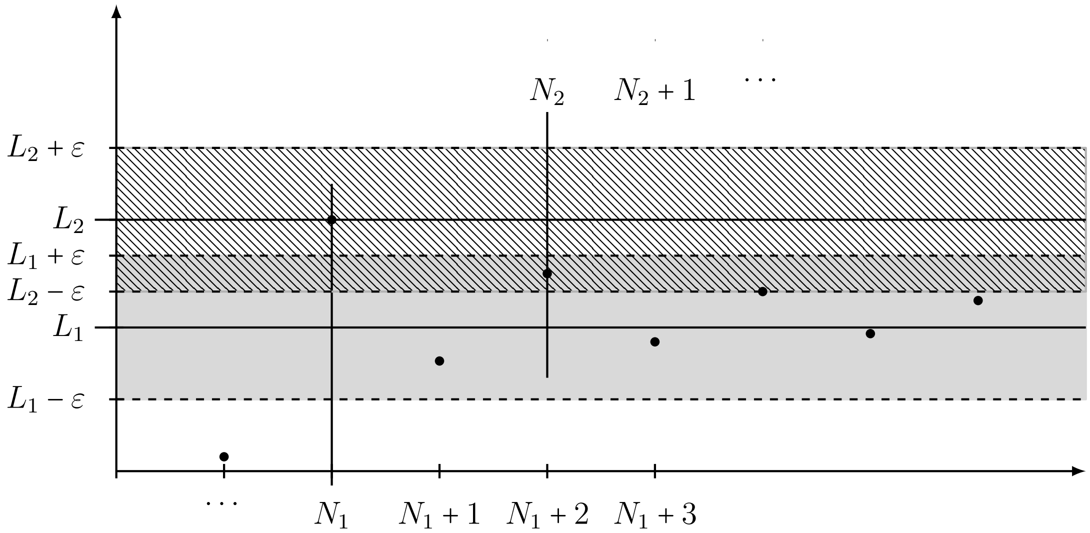
You should notice that this proof, where we *use* the assumption that a sequence tends to a limit, looks nothing like *proving that* a sequence tends to a limit. We get to choose our favourite $\varepsilon > 0$, and then we are given N_1 and N_2. I want to stress that the choice we made, $\varepsilon = \frac{1}{3}|L_2 - L_1|$, isn't 'obvious' at the point in the proof where we write 'we choose...'. Again, if you were not just reading this proof but trying to think it up, you'd leave a blank space here to fill in later, once you see (at the second to last line) what you actually need: 2ε shouldn't be bigger than $|L_2 - L_1|$. If you think a bit, in fact $\varepsilon = \frac{1}{2}|L_2 - L_1|$ would actually work as well (because we have *strict* inequalities) but it is better to write something which 'works easily'; you're less likely to make a mistake.

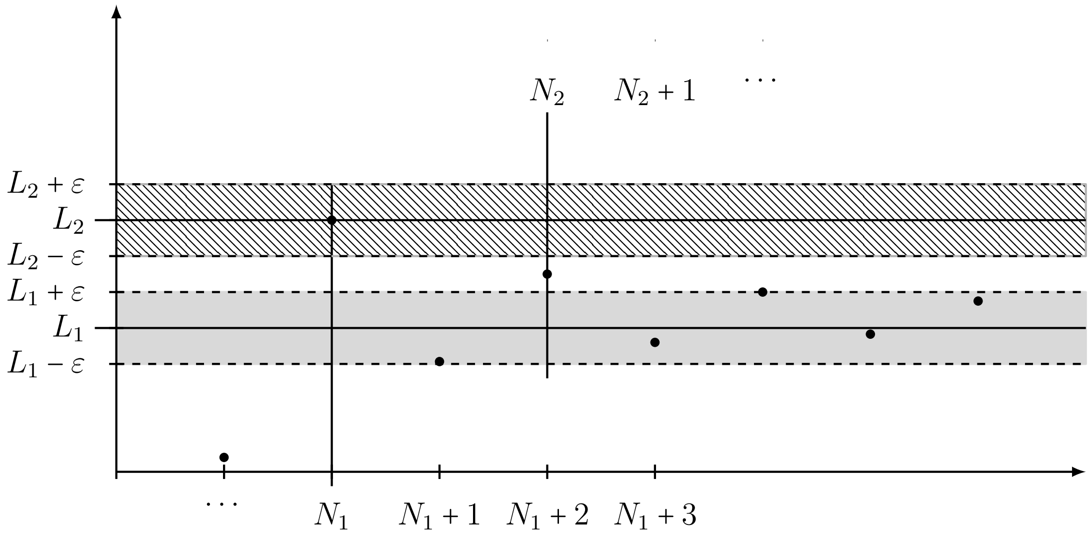
Again, it's not too easy to see where this proof comes from just by looking at the algebra. How did I find it? Well, I drew Figure 9.5, with the 'first' limit L_1:



Then I drew in L_2 on the y axis with its ε-sized band and N_2.

Now, what does this picture mean? In order for $\lim_{n\to\infty} a_n = L_1$ to be true, all the points after N_1 have to be in the grey box, which they are. And for $\lim_{n\to\infty} a_n = L_2$ to be true, all the points have to be in the hashed box after N_2. Which they are not in this picture—but they *could have been*:





they could have all been in the grey-hashed overlap. We want to get rid of that possibility—we chose ε too big, we should choose a smaller value so the boxes don't overlap:

And now we are happy: if N is at least as big as both N_1 and N_2, for $\lim\limits_{n\to\infty} a_n = L_1$ to be true all the points a_n with $n > N$ need to be in the grey box; but for $\lim\limits_{n\to\infty} a_n = L_2$ to be true all the points a_n with $n > N$ need to be in the hashed box. That can't be: the boxes don't overlap!

The proof we saw really came from drawing this final picture. It tells us how we need to choose $\varepsilon > 0$. Then N_1 and N_2 are given to us by the definition of 'converges to L_1' and 'converges to L_2' respectively. Then the picture tells us to choose $N = \max(N_1, N_2)$.

An important fact about sequences is that changing the first few terms of a sequence does not change whether the sequence converges or the value of the limit if it exists. This is made precise by the following theorem.

Theorem 9.12. *Let $(a_n)_{n\in\mathbb{N}}$ and $(b_n)_{n\in\mathbb{N}}$ be two sequences, let M be a natural number, and let L be a real number. Suppose that $a_n = b_n$ for all $n > M$. Then $\lim_{n\to\infty} a_n = L$ is True if and only if $\lim_{n\to\infty} b_n = L$ is True.*

The proof of this theorem is an exercise.

Let's finally prove one important fact about limits of sequences: if all the terms of a convergent sequence are contained in a closed interval $[a,b]$, then so is the limit.

Theorem 9.13. *Suppose $[a,b]$ is any closed interval, and $(x_n)_{n\in\mathbb{N}}$ be a convergent sequence with limit L, where $x_n \in [a,b]$ for all $n \in \mathbb{N}$. Then L is also in $[a,b]$.*

Proof. We prove this theorem by contradiction. Suppose for a contradiction that $L \notin [a,b]$. Then either $L > b$, or $L < a$.
Case 1: Suppose $L > b$. Choose $\varepsilon = \frac{L-b}{2}$, which is positive. Since $(x_n)_{n\in\mathbb{N}}$ converges to L, there exists $N \in \mathbb{N}$ such that for all $n > N$ we have

$$|x_n - L| < \varepsilon = \tfrac{L-b}{2} \quad \text{so} \quad x_n > L - \varepsilon = \tfrac{L+b}{2} > b\,,$$

where the final inequality is since $L > b$. In particular, for $n = N+1$ we have $x_n > b$. But this is a contradiction to our assumption $x_n \in [a,b]$.

The second case is very similar.
Case 2: Suppose $L < a$. Choose $\varepsilon = \frac{a-L}{2}$, which is positive. Since $(x_n)_{n\in\mathbb{N}}$ converges to L, there exists $N \in \mathbb{N}$ such that for all $n > N$ we have

$$|x_n - L| < \varepsilon = \tfrac{a-L}{2} \quad \text{so} \quad x_n < L + \varepsilon = \tfrac{L+a}{2} < a\,,$$

where the final inequality is since $L < a$. In particular, for $n = N+1$ we have $x_n < a$. But this is a contradiction to our assumption $x_n \in [a,b]$.

In either case, we found a contradiction, so the theorem is proved. □

It's worth noticing that this theorem would be false for an open interval; we've already seen that $\left(\frac{1}{n}\right)_{n\in\mathbb{N}}$ is a convergent sequence with limit 0. All the terms of this sequence are in $(0,2)$, but the limit is not.

9.2.2 Standard strategies and Analysis

I know this has been said before, but it bears repetition. What you should notice from the above proofs is: you need to use standard strategies to help you get started with proofs, to keep the logic straight, to make it clear where you need an idea. In all the proofs we just saw, a good deal of the writing has come from applying one standard strategy after another: in short, basic logic. If you don't see where the standard strategies came in, go back to the list, and use it to work through the proof until you get stuck—this is probably the first place where an idea is needed.

What we have also just seen is that sometimes—often—the ideas we need are not so obvious. This is where Analysis is 'supposed' to be difficult: you need to come up with these ideas.

It is *not* supposed to be difficult to understand the definitions, or to write the standard bits of the proof. That will only be difficult if you write sloppily, or you are not clear about the basic logic. But, if you are not clear on the basic logic: well, those bits will be difficult too, you most likely will not really understand definitions like 'converges to L' that you have seen. In this case, you should stop reading further, return to Chapters 2 and 3, and get up to speed on logic and quantifiers. If you read further without the basic logic competence, you will actively be making it harder to learn this material: you will misunderstand things, and it will be harder to correct that once you learn logic than it is to learn logic first then understand Analysis.

9.2.3 Writing analysis proofs: formal versus informal

There are two styles for writing analysis proofs.

One, the classical formal style, is: write down the choices of all the constants at the beginning, and then complete the proof. This is what the proofs above did. Here is another example. We want to prove the sequence $\big(a_n\big)_{n\in\mathbb{N}}$ given by $a_n = 1 + \frac{1}{\sqrt{n}-\pi}$ tends to the limit 1.

Proof. Given $\varepsilon > 0$, let $N = \max\big(400, \lceil 4\varepsilon^{-2}\rceil\big)$.

Suppose $n > N$. Then we have

$$|a_n - 1| = \left|\frac{1}{\sqrt{n}-\pi}\right| = \left|\frac{1}{2\sqrt{\frac{n}{4}}-\pi}\right| \le \left|\frac{1}{\sqrt{\frac{n}{4}}+\sqrt{100}-\pi}\right| < \left|\frac{1}{\sqrt{\frac{n}{4}}}\right| < \left|\frac{1}{\sqrt{\frac{4\varepsilon^{-2}}{4}}}\right| = \varepsilon$$

which is what we wanted. □

Let's quickly notice where this long sequence of inequalities above comes from. The first equality is just putting in the definition of a_n and noticing that the 1s cancel. For the next, we just take a factor of 2 out of the square root. The reason we do this is that we can notice that, since N is bigger than 400, and n is bigger than N, so $\sqrt{\frac{n}{4}}$ is bigger than $\sqrt{\frac{400}{4}} = \sqrt{100}$. So when we replace a $\sqrt{\frac{n}{4}}$ with $\sqrt{100}$ in the denominator, we make the denominator smaller, and that makes the fraction bigger. Why do we do this? Well, because π is about 3, in particular it's less than $\sqrt{100} = 10$. So again, we can make the denominator smaller by taking out the $\sqrt{100} - \pi$, and again that makes the fraction bigger. Finally, we notice that n is bigger than N which is bigger than $4\varepsilon^{-2}$, so (yet again!) we can replace n with $4\varepsilon^{-2}$ to make the denominator smaller and the fraction bigger. And simplifying we have the ε we wanted: we proved $|a_n - 1| < \varepsilon$.

This proof works fine. It's easy to check. It is not obvious how to *think of it.* We make a 'magical' choice of N at the beginning, and it just happens to be exactly what we need to get a pretty ε at the end.

Of course, the truth is that I didn't really make this choice of N at the beginning. I left a blank space, and filled it in later after realising what I needed. Later on, we'll see proofs which are more complicated, and there you might have several 'magical' choices made at the beginning of the proof.

Some people (and some textbooks too) prefer a more informal style, where we don't choose N at the beginning, but simply write down that it is to be chosen later and then write down what we need as we go. Here's the same proof, written that way.

Proof. Given $\varepsilon > 0$, we will choose an integer N later.

Suppose $n > N$. Then we have

$$|a_n - 1| = \left|\frac{1}{\sqrt{n}-\pi}\right| = \left|\frac{1}{2\sqrt{\frac{n}{4}}-\pi}\right|$$

We will need $N \ge 400$ in order to write $2\sqrt{\frac{n}{4}} - \pi < \sqrt{\frac{n}{4}} + \sqrt{100} - \pi < \sqrt{\frac{n}{4}}$. Putting this in, we get

$$|a_n - 1| < \left|\frac{1}{\sqrt{\frac{n}{4}}}\right|.$$

We need the right side of this to be less than ε, so we need $N \ge 4\varepsilon^{-2}$ for that to work. Putting this in, we get

$$|a_n - 1| < \left|\frac{1}{\sqrt{\frac{4\varepsilon^{-2}}{4}}}\right| = \varepsilon$$

which is what we wanted. So we should choose $N = \max\big(400, \lceil 4\varepsilon^{-2} \rceil\big)$. □

This proof is a bit longer, but that's fine. It is certainly more obvious why we made this particular choice of N. In general, I don't like 'magical choices' in proofs; it feels like the lecturer showing off, and, worse, it probably makes some students think they will never be able to come up with these proofs themselves (which is false).

However, I am going to stick to the formal style for the rest of these notes, and the reason is that if you choose the informal style, you need to pay attention to the following.

Warning 9.14. If you choose N as you go in a proof, you might end up writing something like 'we choose N bigger than $(7-\varepsilon)(n-\pi)$'. This looks all fine, and there certainly *is* an integer n all over the place in the proof: why not, if it makes the inequalities come out the way you want?

Let's try to prove that $\left(\frac{n}{n-\pi}\right)_{n\in\mathbb{N}}$ tends to 7.

Proof. Given $\varepsilon > 0$, we will choose an integer N later.

Suppose $n > N$. When $n > 5$, we have $6n > 30 > 7\pi$, so $6n - 7\pi > 0$, so $7(n-\pi) > n$, so $\frac{n}{n-\pi} < 7$. We want this last inequality, so we will choose $N > 5$. Then we have

$$\left|\frac{n}{n-\pi} - 7\right| = 7 - \frac{n}{n-\pi}\,.$$

We should choose N bigger than $(7-\varepsilon)(n-\pi)$, because then we can make the numerator smaller (and so the RHS becomes larger) by writing

$$\left|\frac{n}{n-\pi} - 7\right| = 7 - \frac{n}{n-\pi} < 7 - \frac{N}{n-\pi} < 7 - \frac{(7-\varepsilon)(n-\pi)}{n-\pi} = 7 - (7-\varepsilon) = \varepsilon\,,$$

which is what we wanted. So we should choose $N = \max\big(5, \lceil (7-\varepsilon)(n-\pi) \rceil\big)$. □

If you try writing this proof in the formal style, you'll see something is fishy rather fast:
Proof. Given $\varepsilon > 0$, choose $N = \max\big(5, \lceil (7-\varepsilon)(n-\pi) \rceil\big)$.

Wait—what is n? Something is wrong.

When you read the formal proof (as when you read any proof) one thing you should be thinking is: do I know what each quantity is as it comes? With 'given $\varepsilon > 0$' there is no problem; that means that ε is allowed to be any positive real number, from this point on we fix one particular choice, and the rest of the proof should work whatever positive real number it happens to be. Then 'choose N to be..' means that we are trying to define a quantity N. We want it bigger than 5; no problem. And bigger than a formula. Well, the formula contains ε—we know what that is, we just fixed it. And it contains π—that's about 3.14. And it contains n. What is n? We haven't seen it before, we don't know what it is—how should we work out what this formula *is*? `ERROR ERROR! COMPUTER SAYS NO!`

What is wrong is not just a formality; this is not me being picky for the sake of it. The sequence $\left(\frac{n}{n-\pi}\right)_{n\in\mathbb{N}}$ *does not* tend to 7, in fact (as you can convince yourself by working out a few values, and as you will be able to prove easily by the end of this chapter) the sequence tends to 1. If you want to use the informal style of writing a proof, you need to check that *if* you would write it out in the formal style, *then* you wouldn't ever try to use some letter in a formula before you actually say what that letter is. If you're trying to prove a sequence converges to a limit, that means that when you choose N you can refer to ε, but not to n (or to anything that depends on n!). Otherwise, you may 'prove' completely wrong statements, like the one above.

9.3 Bernoulli's inequality and the sequence $(x^n)_{n\in\mathbb{N}}$.

In this section, we prove that, whenever $|x| < 1$, the sequence $(x^n)_{n\in\mathbb{N}}$ is convergent, with limit 0. This is a basic, and perhaps "obvious" result, but we will want to use it repeatedly: let's prove it.

We proceed by first proving a useful result known as *Bernoulli's Inequality.*

Theorem 9.15. *For all real $x \geq -1$ and all $n \in \mathbb{N}$,*

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

Proof. We prove this result by induction on n. Note first that, for $n = 1$, the inequality states that $1 + x \geq 1 + x$, which is certainly true.

Suppose now that, for some $n \in \mathbb{N}$, $(1 + x)^n \geq 1 + nx$. Now we have

$$(1 + x)^{n+1} = (1 + x)(1 + x)^n \geq (1 + x)(1 + nx) = 1 + nx + x + nx^2 \geq 1 + (n + 1)x\,.$$

So the inequality holds for $n + 1$. Hence, by induction, the inequality holds for all $n \in \mathbb{N}$. □

You might wonder where we used the assumption $x \geq -1$ in this proof. The answer is: we multiplied the induction hypothesis $(1 + x)^n \geq 1 + nx$ through by $1 + x$ *and didn't change the direction of the inequality because* $x + 1 \geq 0$.

Now we use Bernoulli's Inequality to show that, whenever $|x| < 1$, $(x_n)_{n\in\mathbb{N}}$ is convergent with limit 0.

Theorem 9.16. *Let x be any real number with $-1 < x < 1$. Then $(x^n)_{n\in\mathbb{N}}$ is a convergent sequence with limit* 0.

Proof. Given x with $|x| < 1$, we separate two cases.

First note that, if $x = 0$, then $x^n = 0$ for every $n \in \mathbb{N}$, and so certainly $\lim_{n\to\infty} x^n = 0$. So we may assume that $x \neq 0$.

In this case, we have that $1 < \frac{1}{|x|}$, and so $h = \frac{1}{|x|} - 1 > 0$. Now, by Bernoulli's Inequality, Theorem 9.15, for any natural number n we have

$$\frac{1}{|x|^n} = (1 + h)^n \geq 1 + nh > nh,$$

and so

$$0 \leq |x|^n \leq \frac{1}{nh}\,.$$

Remembering this inequality, let's begin the proof of convergence.

Given any $\varepsilon > 0$, we take $N = \left\lceil \frac{1}{\varepsilon h} \right\rceil$. Now, for $n > N$, we have

$$|x^n - 0| = |x|^n \leq \frac{1}{nh} < \frac{1}{Nh} \leq \varepsilon\,.$$

Hence $\lim\limits_{n\to\infty} x^n = 0$. □

Let's check quickly that we did not fall into the 'trap' of Warning 9.14. We chose $N = \left\lceil \frac{1}{\varepsilon h} \right\rceil$. That depends on ε, which is fine: we were given ε already. And it depends on h—what is h? We defined it to be $\frac{1}{|x|} - 1$. What is x? That was given to us at the start of the proof too, so that's fine. What is important is that the choice of N we make doesn't depend on n (because we don't know what n is yet, we only introduce it on the next line).

Example 9.17. Use Bernoulli's Inequality to show that $\lim_{n\to\infty} 2^{\frac{1}{n}} = 1$.

Proof. $2 > 1$ and so $2^{\frac{1}{n}} > 1$ (for otherwise $2 = (2^{\frac{1}{n}})^n \le 1$, a contradiction). Let $a_n := 2^{\frac{1}{n}} - 1 \ge 0$. Then Bernoulli's inequality says $2 = (1 + a_n)^n \ge 1 + na_n$, and so

$$0 \le a_n \le \frac{1}{n}.$$

Now, given any $\varepsilon > 0$, choose $N = \lceil 1/\varepsilon \rceil$. Then, for $n > N$,

$$|2^{\frac{1}{n}} - 1| = |a_n| = a_n \le \frac{1}{n} < \frac{1}{N} \le \varepsilon.$$

Therefore the sequence $2, \sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \sqrt[5]{2}, \dots$ is convergent with limit 1. □

I've so far been rather careful to make sure N is always chosen to be an integer (because that's what it is declared to be in Definition 9.3, the definition of convergence). This is why I've put in these $\lceil\cdot\rceil$ symbols 'the smallest integer at least..'.

However, it's rather common to simply write 'choose $N \ge 1/\varepsilon$' rather than 'choose $N = \lceil 1/\varepsilon \rceil$', and leave it implicit that N is *supposed* to be an integer. I'll be happy with you producing either.

You might wonder why we don't simply change the definition of convergence and allow N to be any real number to avoid these issues. The answer to that is that it often *is* convenient to assume N is a natural number in proofs; we can write things like a_N and be assured that that is actually a term of our sequence.

9.4 Bounded and monotone sequences

It is cumbersome to check from the definition if a sequence is convergent or not. Furthermore, it's very hard to use the definition to show that a sequence is convergent if we don't already know what the limit is. This is one reason why it's hard to show sequence (vii) from Example 9.2 converges to a limit—we don't have any idea what the limit might be, and looking at the terms of the sequence doesn't suggest any nice number that might be the answer (because the answer is, as far as we know, not a nice number!).

In this section, we will study a condition under which we can conclude that a sequence is convergent even without knowing its limit! We will prove that if a sequence is both 'bounded' as well as 'monotone', then it is always convergent.

Definition 9.18. A sequence $(a_n)_{n\in\mathbb{N}}$ is said to be *bounded* if there exists a real number $M > 0$ such that

$$\text{for all } n \in \mathbb{N}, \quad |a_n| \le M. \tag{9.1}$$

Note that a sequence is bounded if and only if the set $S = \{a_n \mid n \in \mathbb{N}\}$ is bounded (this is an exercise).

Example 9.19.

(i) $(1)_{n\in\mathbb{N}}$ is bounded, since $|1| = 1 \le 1$ for all $n \in \mathbb{N}$.

(ii) $\left(\frac{1}{n}\right)_{n\in\mathbb{N}}$ is bounded, since $\left|\frac{1}{n}\right| = \frac{1}{n} \le 1$ for all $n \in \mathbb{N}$.

(iii) $\left(1+\frac{1}{n}\right)_{n\in\mathbb{N}}$ is bounded, since $\left|1+\frac{1}{n}\right| = 1+\frac{1}{n} \le 2$ for all $n \in \mathbb{N}$.

(iv) $\left((-1)^n\left(1+\frac{1}{n}\right)\right)_{n\in\mathbb{N}}$ is bounded, since $\left|(-1)^n\left(1+\frac{1}{n}\right)\right| = 1+\frac{1}{n} \le 2$ for all $n \in \mathbb{N}$.

Example 9.20. Show that the sequence $(a_n)_{n\in\mathbb{N}}$ defined by

$$a_n = \frac{1}{1^1}+\frac{1}{2^2}+\frac{1}{3^3}+\cdots+\frac{1}{n^n}, \quad n \in \mathbb{N}$$

is bounded. (This is sequence (vii) from Example 9.2.)

Proof. We will prove that $|a_n| \le \frac{3}{2}$ is true for all $n \in \mathbb{N}$. Since all the terms of this sequence are positive, we can write:

$$\begin{aligned}
|a_n| &= a_n \\
&= \frac{1}{1^1}+\frac{1}{2^2}+\frac{1}{3^3}+\cdots+\frac{1}{n^n} \\
&< \frac{1}{1^1}+\frac{1}{2^2}+\frac{1}{2^3}+\cdots+\frac{1}{2^n} \\
&= \frac{1}{1^1}+\frac{1}{2}\left(1-\frac{1}{2}\right)+\frac{1}{2^2}\left(1-\frac{1}{2}\right)+\cdots+\frac{1}{2^{n-1}}\left(1-\frac{1}{2}\right) \\
&= 1+\frac{1}{2}-\frac{1}{2^2}+\frac{1}{2^2}-\frac{1}{2^3}+\frac{1}{2^3}-\frac{1}{2^4}+\cdots+\frac{1}{2^{n-1}}-\frac{1}{2^n} \\
&= 1+\frac{1}{2}-\frac{1}{2^n} \\
&< \frac{3}{2}.
\end{aligned}$$

Thus all the terms are bounded by $\frac{3}{2}$, and so the sequence is bounded. □

As usual, I did not know $\frac{3}{2}$ would turn out to be an upper bound at the start of the proof; I left a blank space and filled it in once I found it at the end. As with convergence, what's important is that whatever number I write for an upper bound has to be a number which does not depend on n.

You might be a bit unhappy with the proof above. If so:

Activity 9.5. *Write down a detailed proof that* $|a_n| \le 1+\dfrac{1}{2}-\dfrac{1}{2^n}$ *using induction on* n.

Example 9.21. Show that the sequence $(a_n)_{n\in\mathbb{N}}$ given by $a_n = n$ for $n \in \mathbb{N}$, is not bounded.

Proof. Given any $M > 0$, there exists an $N \in \mathbb{N}$ such that $M < N$ (Archimedean property with $y = M$ and $x = 1$). Thus

$$\neg\left[\exists M > 0 \text{ such that for all } n \in \mathbb{N},\ |a_n| = |n| = n \le M\right],$$

and so $(n)_{n\in\mathbb{N}}$ is not bounded. □

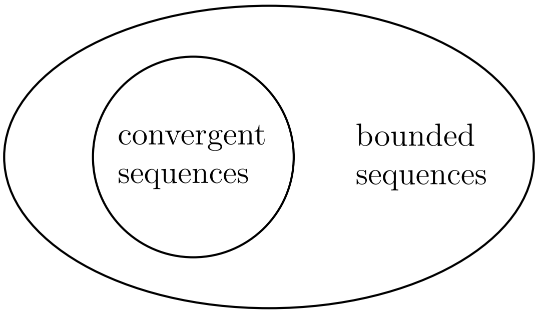


Figure 9.6: All convergent sequences are bounded.

The sequences $(1)_{n\in\mathbb{N}}$, $\left(\frac{1}{n}\right)_{n\in\mathbb{N}}$, $\left(1+\frac{1}{n}\right)_{n\in\mathbb{N}}$ are all convergent, and we have shown above that these are also bounded. This is not a coincidence, and in the next theorem we show that the set of all convergent sequences is contained in the set of all bounded sequences, as illustrated in Figure 9.6.

Theorem 9.22. *If a sequence is convergent, then it is bounded.*

Proof. Let $(a_n)_{n\in\mathbb{N}}$ be a convergent sequence with limit L. Set $\varepsilon = 1$. Then, using the definition of convergence for this value of ε, we see that there exists $N \in \mathbb{N}$ such that, for all $n > N$,

$$|a_n - L| < 1.$$

Hence for all $n > N$,

$$|a_n| = |a_n - L + L| \le |a_n - L| + |L| < 1 + |L|.$$

Let $M = \max\big(|a_1|, \dots, |a_N|, 1 + |L|\big)$. Then for all $n \in \mathbb{N}$

$$|a_n| \le M$$

and so $(a_n)_{n\in\mathbb{N}}$ is bounded. □

The above theorem can be used to prove the *divergence* of a sequence. Indeed, in contrapositive form it asserts that unbounded sequences are not convergent. Thus, one way to prove that a sequence is divergent is to prove that it is unbounded.

Example 9.23. Show that the sequence $(n)_{n\in\mathbb{N}}$ is divergent.

Proof. We have seen above that $(n)_{n\in\mathbb{N}}$ is unbounded. It follows from Theorem 9.22 that $(n)_{n\in\mathbb{N}}$ is not convergent. □

Keep in mind that *some* divergent sequences are not bounded, but some other divergent sequences are bounded, such as sequence (iv) of Example 9.2.

Definition 9.24. A sequence $(a_n)_{n\in\mathbb{N}}$ is said to be

monotonically increasing (or simply **increasing**) if for all $n \in \mathbb{N}$, $a_n \le a_{n+1}$,

strictly increasing if for all $n \in \mathbb{N}$, $a_n < a_{n+1}$,

monotonically decreasing (or simply **decreasing**) if for all $n \in \mathbb{N}$, $a_n \ge a_{n+1}$,

strictly decreasing if for all $n \in \mathbb{N}$, $a_n > a_{n+1}$,

monotone if it is either monotonically increasing or monotonically decreasing.

$$\begin{aligned}
\text{Thus a sequence } (a_n)_{n\in\mathbb{N}} \text{ is monotonically increasing if} \quad & a_1 \le a_2 \le a_3 \le \dots, \\
\text{strictly increasing if} \quad & a_1 < a_2 < a_3 < \dots, \\
\text{monotonically decreasing if} \quad & a_1 \ge a_2 \ge a_3 \ge \dots, \\
\text{and strictly decreasing if} \quad & a_1 > a_2 > a_3 > \dots.
\end{aligned}$$

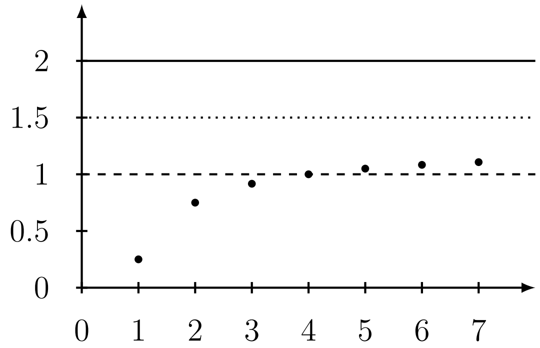
Example 9.25.

Sequence	monotonically increasing?	strictly increasing?	monotonically decreasing?	strictly decreasing?	monotone?
$\left(\frac{1}{n}\right)_{n\in\mathbb{N}}$	No	No	Yes	Yes	Yes
$\left(1+\frac{1}{n}\right)_{n\in\mathbb{N}}$	No	No	Yes	Yes	Yes
$\left((-1)^n\left(1+\frac{1}{n}\right)\right)_{n\in\mathbb{N}}$	No	No	No	No	No
$(1)_{n\in\mathbb{N}}$	Yes	No	Yes	No	Yes
$(n)_{n\in\mathbb{N}}$	Yes	Yes	No	No	Yes
$\left(\frac{1}{1^1}+\frac{1}{2^2}+\frac{1}{3^3}+\dots+\frac{1}{n^n}\right)_{n\in\mathbb{N}}$	Yes	Yes	No	No	Yes

The following theorem can be useful for showing that sequences converge without knowing the limit beforehand (or with less work than using the definition).

Theorem 9.26. *If a sequence is monotone and bounded, then it is convergent.*

Again, to see how to prove this it helps to draw a picture. We'll draw the picture for the case 'monotonically increasing'.



The black line at 2 is an upper bound for the sequence. But it doesn't look like 2 is a good candidate for the limit: it's too big.

The dashed line at 1 isn't an upper bound for the sequence. This *proves* 1 can't be the limit, it is too small (because the sequence is increasing, it can never go back down from above 1 to get arbitrarily close to 1).

The dotted line at 1.5 looks like a better candidate for the limit. It is an upper bound for the sequence, and this *proves* that 2 can't be the limit: the sequence can never get above 1.5 so it cannot get arbitrarily close to 2.

But if there is a smaller upper bound than 1.5 then that would *prove* 1.5 cannot be the limit.

What we are looking for is the *least upper bound* of the set $\{a_n \mid n \in \mathbb{N}\}$. Since this is a non-empty, bounded set of real numbers, the least upper bound property says that $L = \sup\{a_n \mid n \in \mathbb{N}\}$ exists. We just need to prove it *is* the limit. Let's formalise that.

Proof. We first consider the case that our sequence is monotone increasing, then do the monotone decreasing case.

Let $(a_n)_{n\in\mathbb{N}}$ be a monotonically increasing sequence. Since $(a_n)_{n\in\mathbb{N}}$ is bounded, it follows that the set

$$S = \{a_n \mid n \in \mathbb{N}\}$$

has an upper bound and so $L = \sup S$ exists. We show that in fact $(a_n)_{n\in\mathbb{N}}$ converges to L.

Given $\varepsilon > 0$, we want to find N such that $L - \varepsilon < a_n < L + \varepsilon$ for all $n > N$. The right-hand inequality is going to be easy: by definition of 'upper bound', $a_n \le L < L + \varepsilon$ is true for all $n \in \mathbb{N}$. So the difficulty is to get $L - \varepsilon < a_n$.

Because L is the *least* upper bound of S, it follows $L - \varepsilon$ is *not* an upper bound of S. That means there exists some N such that $a_N > L - \varepsilon$.

But because the sequence is increasing, we have for any $n > N$ the fact

$$L - \varepsilon < a_N \le a_{N+1} \le a_{N+2} \le \cdots \le a_n$$

which is what we wanted. □

We should really write the 'convergence' part of this proof formally:
Given $\varepsilon > 0$, choose N such that $a_N > L - \varepsilon$ (because $L - \varepsilon$ is not an upper bound of S). Then if $n > N$ we have

$$L - \varepsilon < a_N \le a_{N+1} \le \cdots \le a_n \le L < L + \varepsilon$$

so in particular $L - \varepsilon < a_n < L + \varepsilon$ as desired.

Written like this, it's clear the choice of N *doesn't* depend on n: we don't even mention n until after we chose N.

Warning 9.27. Rather often, students read the above theorem as 'if and only if'. This is false. Any bounded monotone sequence is convergent, *but* in the other direction all we can say is that a convergent sequence is bounded (Theorem 9.22). There are sequences which are convergent (and so bounded) but not monotone, such as sequence (ix) of Example 9.2.

Example 9.28. The following table gives a summary of the valid implications, and gives counterexamples to implications which are not true.

Question	Answer	Reason/Counterexample
Is every convergent sequence bounded?	Yes	Theorem 9.22
Is every bounded sequence convergent?	No	$((-1)^n)_{n\in\mathbb{N}}$ is bounded, but not convergent.
Is every convergent sequence monotone?	No	$\left(\frac{(-1)^n}{n}\right)_{n\in\mathbb{N}}$ is convergent, but not monotone: $-1 < \frac{1}{2}$ and $\frac{1}{2} > -\frac{1}{3}$.
Is every monotone sequence convergent?	No	$(n)_{n\in\mathbb{N}}$ is not convergent.
Is every bounded AND monotone sequence convergent?	Yes	Theorem 9.26

The following activity is slightly tricky: think about how to put together the theorems you already saw in order to prove it.

Activity 9.6. *Let* $(a_n)_{n\in\mathbb{N}}$ *be a sequence. We say it is a* Cauchy sequence *if the following is true: For every* $\delta > 0$*, there is an* $M \in \mathbb{N}$ *such that if* $m, m' > M$ *then we have* $|a_m - a_{m'}| < \delta$.

Prove that a sequence is convergent if and only if it is a Cauchy sequence.

Let's finally give an example of how to use Theorem 9.26.

Example 9.29. Prove that the sequence $(a_n)_{n\in\mathbb{N}}$ defined by

$$a_n = \frac{1}{1^1} + \frac{1}{2^2} + \frac{1}{3^3} + \cdots + \frac{1}{n^n}, \quad n \in \mathbb{N}$$

is convergent.

Proof. We showed in Example 9.20 that this sequence is bounded. It is strictly increasing since

$$a_{n+1} - a_n = \frac{1}{(n+1)^{(n+1)}} > 0$$

for all $n \in \mathbb{N}$.

So by Theorem 9.26, this sequence is convergent. □

9.4.1 Series

We won't really talk about *series* in this course, but it is worth giving the definition.

Given real numbers $a_1, a_2, \ldots$, when we write the 'series'

$$\sum_{n=1}^{\infty} a_n$$

what we mean is the limit of the sequence of *partial sums*, that is

$$\sum_{n=1}^{\infty} a_n = \lim_{n\to\infty} \sum_{i=1}^{n} a_i \,.$$

As we've seen, some sequences converge and other sequences diverge; that's equally true for sequences of partial sums. So some series converge (we can write down a real number which is the 'infinite sum') and some diverge (the 'infinite sum' doesn't make sense).

What Example 9.29 shows, in this language, is that

$$\sum_{n=1}^{\infty} \frac{1}{n^n}$$

is a convergent series; it makes sense to say that this 'infinite sum' is a real number.

It would be reasonable to guess that there is perhaps some nice formula for the limit of this series that lets us find out what it is more easily than adding up infinitely many terms. But we don't know any such formula. Not only that, we don't even know if the limit is a rational number or not! This is a long open problem: in 1697, Johann Bernoulli proved that

$$\sum_{n=1}^{\infty} \frac{1}{n^n} = \int_0^1 \frac{1}{x^x} dx \,,$$

but this doesn't help us, either with calculating the limit or finding out if it is rational.

One can fairly easily (with a computer) find out what the first few (or few million) digits of the limit are, and from this calculation we can show that if the limit is rational, then the fraction $\frac{p}{q}$ which is the limit needs to have a very large denominator: q has to be into the millions. So our best guess is that no such fraction exists: probably the limit is irrational.

This is about all I want to say about series in this course. If you take MA203, you'll return to the topic there. The only thing I have left to say is a warning. There is a reason that we invented the new word 'series' rather than just say 'infinite sum'. The reason is that 'infinite sum' sounds friendly and well-behaved. You can do all kinds of things in a sum, like rearrange the terms (because addition is commutative).

Series are not friendly and well-behaved. If you rearrange the terms you get a different series, which might have a completely different limit.

9.5 Algebra of limits

It's 'obvious' that if you have a couple of sequences $(a_n)_{n\in\mathbb{N}}$ and $(b_n)_{n\in\mathbb{N}}$, both of which are convergent with limits respectively A and B, then $(a_n+b_n)_{n\in\mathbb{N}}$ should be a convergent sequence too, with limit $A+B$. Why is it 'obvious'? Well, if n is large then we are guaranteed $|a_n-A|$ is very close to 0, and $|b_n-B|$ is very close to 0, so $|a_n+b_n-A-B|$ must still be pretty close to 0 (by the triangle inequality).

The above is a good way to think about limits of sequences: try to keep in mind the intuitive meaning, without having to write down all the quantifiers in the definition all the time. But you also need to be able to go from this kind of intuitive idea to a formal proof, which means you need to figure out how to use the definition with all the quantifiers.

Activity 9.7. *Prove that if $(a_n)_{n\in\mathbb{N}}$ and $(b_n)_{n\in\mathbb{N}}$ are both are convergent, with limits respectively A and B, then $(a_n+b_n)_{n\in\mathbb{N}}$ is a convergent sequence too, with limit $A+B$.*

However, once you have done this once, you will not learn much from doing the same thing for (say) $(a_n-b_n)_{n\in\mathbb{N}}$ or $(a_nb_n)_{n\in\mathbb{N}}$. The purpose of this section is to do that work for you. We'll see that a sequence which looks 'complicated' can often be broken down into 'simple' sequences by algebraic operations like addition and subtraction, and we can find the limit of the complicated sequences by doing the same algebra with the limits of the simple sequences (which we will hopefully already know or be able to look up). This work-saving device is called the *Algebra of Limits*.

Example 9.30. Show that the sequence $(a_n)_{n\in\mathbb{N}}$ defined by

$$a_n=\frac{4n^2+9}{3n^2+7n+11}$$

converges to $\frac{4}{3}$.

Proof. We could do this by going back to the definition of convergence, and writing half a page of algebra.

But it is much easier to write:

$$a_n=\frac{n^2\left(4+\frac{9}{n^2}\right)}{n^2\left(3+\frac{7}{n}+\frac{11}{n^2}\right)}=\frac{4+\frac{9}{n^2}}{3+\frac{7}{n}+\frac{11}{n^2}}.$$

Now, the sequences $\left(\frac{9}{n^2}\right)_{n\in\mathbb{N}}$, $\left(\frac{7}{n}\right)_{n\in\mathbb{N}}$, $\left(\frac{11}{n^2}\right)_{n\in\mathbb{N}}$ all have limit 0, and by a repeated application of Theorem 9.31 given below, we obtain that

$$\lim_{n\to\infty}a_n=\frac{\lim\limits_{n\to\infty}\left(4+\dfrac{9}{n^2}\right)}{\lim\limits_{n\to\infty}\left(3+\dfrac{7}{n}+\dfrac{11}{n^2}\right)}=\frac{\lim\limits_{n\to\infty}4+\lim\limits_{n\to\infty}\dfrac{9}{n^2}}{\lim\limits_{n\to\infty}3+\lim\limits_{n\to\infty}\dfrac{7}{n}+\lim\limits_{n\to\infty}\dfrac{11}{n^2}}=\frac{4+0}{3+0+0}=\frac{4}{3}.\qquad\square$$

Theorem 9.31 (Algebra of Limits). *If $(a_n)_{n\in\mathbb{N}}$ and $(b_n)_{n\in\mathbb{N}}$ are convergent sequences, then the following hold:*

(a) For all $\alpha \in \mathbb{R}$, $(\alpha a_n)_{n\in\mathbb{N}}$ is a convergent sequence and $\lim\limits_{n\to\infty} \alpha a_n = \alpha \lim\limits_{n\to\infty} a_n$.

(b) $(|a_n|)_{n\in\mathbb{N}}$ is a convergent sequence and $\lim\limits_{n\to\infty} |a_n| = \left|\lim\limits_{n\to\infty} a_n\right|$.

(c) $(a_n + b_n)_{n\in\mathbb{N}}$ is a convergent sequence and $\lim\limits_{n\to\infty}(a_n + b_n) = \lim\limits_{n\to\infty} a_n + \lim\limits_{n\to\infty} b_n$.

(d) $(a_n b_n)_{n\in\mathbb{N}}$ is a convergent sequence and $\lim\limits_{n\to\infty} a_n b_n = \left(\lim\limits_{n\to\infty} a_n\right)\left(\lim\limits_{n\to\infty} b_n\right)$.

(e) For all $k \in \mathbb{N}$, $(a_n^k)_{n\in\mathbb{N}}$ is a convergent sequence and $\lim\limits_{n\to\infty} a_n^k = \left(\lim\limits_{n\to\infty} a_n\right)^k$.

(f) If for all $n \in \mathbb{N}$, $b_n \neq 0$ and $\lim\limits_{n\to\infty} b_n \neq 0$, then $\left(\frac{1}{b_n}\right)_{n\in\mathbb{N}}$ is convergent and moreover, $\lim\limits_{n\to\infty} \frac{1}{b_n} = \frac{1}{\lim\limits_{n\to\infty} b_n}$.

(g) For all $k \in \mathbb{N}$, $(a_{n+k})_{n\in\mathbb{N}}$ is convergent and $\lim\limits_{n\to\infty} a_{n+k} = \lim\limits_{n\to\infty} a_n$.

(h) If for all $n \in \mathbb{N}$, $a_n \geq 0$, then $\left(\sqrt{a_n}\right)_{n\in\mathbb{N}}$ is convergent and $\lim\limits_{n\to\infty} \sqrt{a_n} = \sqrt{\lim\limits_{n\to\infty} a_n}$.

That was a long theorem—which you should think of as good: there are lots of algebraic operations you *can* do and you are guaranteed to get the right answer.

Before proving it (the proof comes in eight parts, so it is long, but no part is hard) it's probably best to highlight what the Algebra of Limits does *not* let you do.

Warning 9.32. The Algebra of Limits *only* works if the sequences $(a_n)_{n\in\mathbb{N}}$ and $(b_n)_{n\in\mathbb{N}}$ are *convergent.* If they are not, sometimes you will end up with a nonsensical answer (like 'infinity minus infinity', and at least you know something is wrong. Sometimes you will get a nice real number, but it happens to be the wrong real number.

The Algebra of Limits lets you add up (or subtract, multiply, et cetera) *two* sequences. By using it repeatedly, you can also add up three sequences, or four, and so on. We'll normally do that without comment (as we did in Example 9.30). But let's recall that $(1)_{n\in\mathbb{N}}$ converges to 1, and $\left(\frac{1}{n}\right)_{n\in\mathbb{N}}$ converges to 0. So can we write

$$\lim_{n\to\infty} 1 = \lim_{n\to\infty} \underbrace{\tfrac{1}{n} + \cdots + \tfrac{1}{n}}_{n \text{ times}} = \underbrace{\lim_{n\to\infty} \tfrac{1}{n} + \cdots + \lim_{n\to\infty} \tfrac{1}{n}}_{n \text{ times}} = \underbrace{0 + \cdots + 0}_{n \text{ times}} = 0 \quad ..?$$

Of course not, because that would say $1 = 0$. The problem is the second equality, which looks like the Algebra of Limits. It's not. This is not a fixed number of sequences, and we've just seen a way to misuse the Algebra of Limits to get the wrong answer. If you're paying attention, you will notice that the next two formulae don't make sense: what should the n under the bracket at the bottom actually *be*? n is supposed to be some natural number, but which one?

What I mean by this is that in the first two formulae, n is a bound variable—that is, it is a placeholder, it only makes sense inside of the 'lim' symbol. So for example, the formula $\lim\limits_{n\to\infty} \frac{1}{n}$ means exactly the same as $\lim\limits_{z\to\infty} \frac{1}{z}$, which means the same as 'the limit of the sequence whose terms are 1, $\frac{1}{2}$, $\frac{1}{3}$, $\frac{1}{4}$, ...'. Any time you start a sequence of statements or equations with an n (or some other letter) as a bound variable (inside a limit, or a quantifier) and at the end it's popped out to become a free variable (summing up n lots of zero) you can be fairly confident that you have made a mistake.

Proof of Theorem 9.31. Throughout this proof, we assume $(a_n)_{n\in\mathbb{N}}$ and $(b_n)_{n\in\mathbb{N}}$ are convergent sequences, and their limits are L_a and L_b, respectively.

(a) If $\alpha = 0$, then $\lim\limits_{n\to\infty} \alpha a_n = \lim\limits_{n\to\infty} 0 = 0$. So we can now assume $\alpha \neq 0$.

Let $\varepsilon > 0$ be given. By the definition of $\lim\limits_{n\to\infty} a_n = L_a$, there exists an $N \in \mathbb{N}$ such that for all $n > N$,

$$|a_n - L_a| < \frac{\varepsilon}{|\alpha|}.$$

Then

$$|\alpha a_n - \alpha L_a| = |\alpha|\,|a_n - L_a| \leq |\alpha|\frac{\varepsilon}{|\alpha|} = \varepsilon\,,$$

and (again by the definition of a convergent sequence) $(\alpha a_n)_{n\in\mathbb{N}}$ is convergent with limit αL_a, that is,

$$\lim_{n\to\infty} \alpha a_n = \alpha L_a = \alpha \lim_{n\to\infty} a_n.$$

(b) Given $\varepsilon > 0$, let $N \in \mathbb{N}$ be such that for all $n > N$,

$$|a_n - L_a| < \varepsilon.$$

Then (as you will prove in an exercise) we have for all $n > N$:

$$\big||a_n| - |L_a|\big| \leq |a_n - L_a| < \varepsilon.$$

Hence $(|a_n|)_{n\in\mathbb{N}}$ is convergent with limit $|L_a|$, that is,

$$\lim_{n\to\infty} |a_n| = |L_a| = \left|\lim_{n\to\infty} a_n\right|.$$

(c) You should have already proved this, in Activity 9.7.

(d) Before beginning this, let's quickly notice why it is a bit tricky. We want to argue that if a_n is close to L_a, and b_n is close to L_b, then $a_n b_n$ is close to $L_a L_b$.

The easiest way to do this is to argue in two steps: first, $a_n b_n$ is close to $L_a b_n$, then second $L_a b_n$ is close to $L_a L_b$. If we can do that, then the triangle inequality tells us $a_n b_n$ is close to $L_a L_b$.

The second part is about the same as what we already did in (a), and we can copy the proof over. For the first part, the difficulty is that if b_n is huge, then a_n might be close to L_a but still $a_n b_n$ is not very close to $L_a b_n$. To deal with this, we use Theorem 9.22 to say that $(b_n)_{n\in\mathbb{N}}$ is bounded, which gives us an upper bound on how huge b_n can be.

First, since $(b_n)_{n\in\mathbb{N}}$ is a convergent sequence, by Theorem 9.22 it is bounded. Let $M > 0$ be[1] such that $|b_n| \leq M$ for every $n \in \mathbb{N}$.

[1] Even if $b_n = 0$ for all n, the definition of 'bounded' insists that we choose a bound which is strictly positive—for example we could set $M = 1$ in this situation.

Given $\varepsilon > 0$, we choose N_a such that for all $n > N_a$ we have $|a_n - L_a| < \frac{\varepsilon}{2M}$, which we can do since $(a_n)_{n\in\mathbb{N}}$ converges to L_a. We choose N_b such that for all $n > N_b$ we have $|b_n - L_b| < \frac{\varepsilon}{2|L_a|+1}$. And finally we let $N = \max(N_a, N_b)$.

Now suppose $n > N$.

Step 1: We want to show $|a_n b_n - L_a b_n| < \frac{\varepsilon}{2}$.

We have $|a_n - L_a| < \frac{\varepsilon}{2M}$, so multiplying both sides by $|b_n|$ we get

$$|b_n||a_n - L_a| < \tfrac{\varepsilon}{2M}|b_n| \le \tfrac{\varepsilon}{2M}M = \tfrac{\varepsilon}{2}\,.$$

Since $|b_n||a_n - L_a| = |a_n b_n - L_a b_n|$ by Theorem 8.18, that's what we wanted for Step 1.

Step 2: We want to show $|L_a b_n - L_a L_b| < \frac{\varepsilon}{2}$.

We have $|b_n - L_b| < \frac{\varepsilon}{2|L_a|+1}$, so multiplying both sides by $|L_a|$ we get

$$|L_a||b_n - L_b| < \tfrac{\varepsilon}{2|L_a|+1}|L_a| = \tfrac{\varepsilon}{2}\cdot\tfrac{|L_a|}{|L_a|+1/2} < \tfrac{\varepsilon}{2}\,,$$

which again is what we want for Step 2.

Putting the two Steps together, and using the triangle inequality (Theorem 8.18) we have

$$|a_n b_n - L_a L_b| \le |a_n b_n - L_a b_n| + |L_a b_n - L_a L_b| < \tfrac{\varepsilon}{2} + \tfrac{\varepsilon}{2} = \varepsilon\,,$$

which is what we needed to verify to show $\lim\limits_{n\to\infty} a_n b_n = L_a L_b$.

Remark 9.33. There are some more 'magical choices' in this proof. Why do we aim for $< \frac{\varepsilon}{2}$ in each of Steps 1 and 2? Well, because we're going to add these up to get ε.

How did I know to ask for $|a_n - L_a| < \frac{\varepsilon}{2M}$; why this particular funny number on the right hand side that (by the end of the proof) just turns out to be exactly what we need? The answer is, of course, I didn't know. I originally wrote $|a_n - L_a| < \delta$ and[2] did some algebra with δ in it, until at the end of Step 1 I got to $|a_n b_n - L_a b_n| < \delta M$. Then I saw that I should choose $\delta = \frac{\varepsilon}{2M}$, and went back and replaced all my δs with this quantity.

Finally, how did I end up with $|b_n - L_b| < \frac{\varepsilon}{2|L_a|+1}$? Some logic similar to what I just said (working things through with a δ) got me to the idea that $\frac{\varepsilon}{2|L_a|}$ looks good. But what if $L_a = 0$? I don't want to divide by zero, so add one to the denominator. That makes the denominator bigger, so the fraction a bit smaller; it's insisting that b_n is a bit closer to L_b. That can only help. It doesn't really matter what we add; 1, or 42, or 0.001.

(e) This can be shown by using induction on k and from part (d) above. It is trivially true with $k = 1$. Suppose that it holds for some k, then $(a_n^k)_{n\in\mathbb{N}}$ is convergent and

$$\lim_{n\to\infty} a_n^k = \left(\lim_{n\to\infty} a_n\right)^k.$$

Hence by part (d) above applied to the sequences $(a_n)_{n\in\mathbb{N}}$ and $(a_n^k)_{n\in\mathbb{N}}$, we obtain that the sequence $(a_n \cdot a_n^k)_{n\in\mathbb{N}}$ is convergent and

$$\lim_{n\to\infty} a_n a_n^k = \left(\lim_{n\to\infty} a_n\right)\left(\lim_{n\to\infty} a_n^k\right) = \left(\lim_{n\to\infty} a_n\right)\left(\lim_{n\to\infty} a_n\right)^k = \left(\lim_{n\to\infty} a_n\right)^{k+1}.$$

Thus $(a_n^{k+1})_{n\in\mathbb{N}}$ is convergent and

$$\lim_{n\to\infty} a_n^{k+1} = \left(\lim_{n\to\infty} a_n\right)^{k+1}.$$

[2] delta, δ is another Greek letter traditionally used for small quantities.

(f) This time, what could be tricky is if b_n is very close to 0. To avoid that, let $N_1 \in \mathbb{N}$ be such that, for all $n > N_1$,

$$|b_n - L_b| < \frac{|L_b|}{2},$$

which we can do since $(b_n)_{n\in\mathbb{N}}$ converges to L_b.

For all $n > N_1$, we have

$$|L_b| - |b_n| \le \big||L_b| - |b_n|\big| \le |b_n - L_b| < \frac{|L_b|}{2},$$

and so $|b_n| \ge \frac{|L_b|}{2}$. This is our '$b_n$ is not close to 0' guarantee.

Given $\varepsilon > 0$, let $N_2 \in \mathbb{N}$ be such that for all $n > N_2$,

$$|b_n - L_b| < \frac{\varepsilon|L_b|^2}{2},$$

which exists since $(b_n)_{n\in\mathbb{N}}$ converges to L_b. Now we let $N = \max\{N_1, N_2\}$.

Suppose $n > N$. Then we have

$$\left|\frac{1}{b_n} - \frac{1}{L_b}\right| = \frac{|b_n - L_b|}{|b_n|\,|L_b|} = |b_n - L_b| \cdot |b_n|^{-1}|L_b|^{-1} < \frac{\varepsilon|L_b|^2}{2}\frac{2}{|L_b|}\frac{1}{|L_b|} = \varepsilon.$$

So $\left(\frac{1}{b_n}\right)_{n\in\mathbb{N}}$ is convergent and $\lim\limits_{n\to\infty} \frac{1}{b_n} = \frac{1}{L_b} = \frac{1}{\lim\limits_{n\to\infty} b_n}$.

Remark 9.34. Of course the funny number $\frac{\varepsilon|L_b|^2}{2}$ is something we got to by saying 'choose N_2 such that if $n > N_2$ then $|b_n - L_b| < \delta$', then doing algebra with δ (as in (d) to figure out how we should choose δ). We get to

$$\left|\tfrac{1}{b_n} - \tfrac{1}{L_b}\right| \le |b_n - L_b| \cdot |b_n|^{-1}|L_b|^{-1} < \delta|b_n|^{-1}|L_b|^{-1}$$

and we know we need the right hand side of this to be at most ε.

A standard mistake at this point is to choose $\delta = \frac{\varepsilon}{2|b_n||L_b|}$. What's the problem?—the algebra works.

The problem is that δ needs to be a quantity that doesn't depend on n—so it can't have a b_n in it. At the point where we first use it in the proof, there *is no n* around, we only say what n should be on the next line, 'Suppose $n > N$'. This is again what we saw in Warning 9.14.

When you're figuring out a proof like this, and you get to needing $\delta|b_n|^{-1}|L_b|^{-1} \le \varepsilon$, what you should think is: *whatever* $n > N$ we happen to be given, we need the left side to be guaranteed small. This would be a problem if $|b_n|^{-1}$ was huge for some values of n—we need to show that $|b_n|^{-1}$ cannot be too big, whatever $n > N$ is. So we need to show $|b_n|$ cannot be too close to 0.

And at this point (and not, despite the way it's written above, at the start!) we realise that we need N to be big enough that we can be sure $|b_n| \ge \frac{|L_b|}{2}$ if $n > N$.

(g) This is homework.

(h) Since $a_n \geq 0$ for each n, from Theorem 9.13 we have $L_a \geq 0$.

The case $L_a = 0$ is an exercise.

In the case $L_a > 0$, we use a technique called "rationalising the numerator": note that

$$\sqrt{a_n} - \sqrt{L_a} = (\sqrt{a_n} - \sqrt{L_a})\frac{\sqrt{a_n} + \sqrt{L_a}}{\sqrt{a_n} + \sqrt{L_a}} = \frac{a_n - L_a}{\sqrt{a_n} + \sqrt{L_a}}.$$

Now, given $\varepsilon > 0$, choose $N \in \mathbb{N}$ so that, for $n > N$, $|a_n - L| < \varepsilon\sqrt{L_a}$. Then we have, for $n > N$,

$$|\sqrt{a_n} - \sqrt{L_a}| = \frac{|a_n - L_a|}{\sqrt{a_n} + \sqrt{L_a}} < \frac{\varepsilon\sqrt{L_a}}{\sqrt{L_a}} = \varepsilon.$$

Thus $(\sqrt{a_n})_{n\in\mathbb{N}}$ is convergent, with limit $\sqrt{L_a}$. □

Activity 9.8. *Show the remaining part of (h), i.e. that if $(a_n)_{n\in\mathbb{N}}$ is a sequence of nonnegative reals, converging to* 0*, then*

$$\lim_{n\to\infty} \sqrt{a_n} = 0\,.$$

Example 9.35. Determine whether the following sequence is convergent and find its limit.

$$\left(\frac{n^2 - 24n^3 + 3n^4 - 12}{1 + 7n + 21n^4}\right)_{n\in\mathbb{N}}$$

Proof. By Activity 9.2 on page 148 we know that $\lim\limits_{n\to\infty} \dfrac{1}{n} = 0$. We now use Theorem 9.31 after first factorizing out n^4 in both the numerator and denominator:

$$\begin{aligned}
\lim_{n\to\infty} \frac{n^2 - 24n^3 + 3n^4 - 12}{1 + 7n + 21n^4} &= \lim_{n\to\infty} \frac{n^4}{n^4} \cdot \frac{\frac{1}{n^2} - \frac{24}{n} + 3 - \frac{12}{n^4}}{\frac{1}{n^4} + \frac{7}{n^3} + 21} \\
&= \frac{\left(\lim\limits_{n\to\infty}\frac{1}{n}\right)^2 - 24\lim\limits_{n\to\infty}\frac{1}{n} + 3 - 12\left(\lim\limits_{n\to\infty}\frac{1}{n}\right)^4}{\left(\lim\limits_{n\to\infty}\frac{1}{n}\right)^4 + 7\left(\lim\limits_{n\to\infty}\frac{1}{n}\right)^3 + 21} \\
&= \frac{0^2 - 24\cdot 0 + 3 - 12\cdot 0^4}{0^4 + 7\cdot 0^3 + 21} \\
&= \frac{3}{21} = \frac{1}{7}.
\end{aligned}$$

□

Example 9.36. Determine whether the following sequence is convergent and find its limit.

$$\left(\frac{2^n + 3^n + 1}{3^{n+1} + 3}\right)_{n\in\mathbb{N}}$$

Proof. Divide numerator and denominator by the fastest growing term appearing, which is 3^n, and use that $\lim_{n\to\infty} x^n = 0$ for $|x| < 1$:

$$\begin{aligned}
\lim_{n\to\infty} \frac{2^n + 3^n + 1}{3^{n+1} + 3} &= \lim_{n\to\infty} \frac{(2/3)^n + 1 + (1/3)^n}{3 + 3(1/3)^n} \\
&= \frac{\lim\limits_{n\to\infty}(2/3)^n + \lim\limits_{n\to\infty} 1 + \lim\limits_{n\to\infty}(1/3)^n}{\lim\limits_{n\to\infty} 3 + 3\lim\limits_{n\to\infty}(1/3)^n} \\
&= \frac{0 + 1 + 0}{3 + 0} = \frac{1}{3}.
\end{aligned}$$

□

Remark 9.37. It follows from Theorem 9.31.(c) that if we have three convergent sequences $(a_n)_{n\in\mathbb{N}}$, $(b_n)_{n\in\mathbb{N}}$, $(c_n)_{n\in\mathbb{N}}$, then their sum $(a_n + b_n + c_n)_{n\in\mathbb{N}}$ is also convergent with limit

$$\lim_{n\to\infty}(a_n + b_n + c_n) = \lim_{n\to\infty} a_n + \lim_{n\to\infty} b_n + \lim_{n\to\infty} c_n.$$

This is also true for the sum of four convergent sequences, the sum of five convergent sequences, and by an easy induction proof, the sum of any fixed number of convergent sequences.

In general, we can apply any fixed number of algebraic operations *via* the Algebra of Limits, as indeed we did in Example 9.36 (three additions and one division, all in one step).

But remember (Warning 9.32) that it doesn't work (or make sense) for n (or anything not fixed) sequences.

9.6 The Sandwich Theorem

Another theorem that is useful in proving that sequences are convergent and in determining their limits is the so-called Sandwich theorem. Roughly speaking, it says that if a sequence is sandwiched between two convergent limits with the *same* limit, then the sandwiched sequence is also convergent with the same limit.

Theorem 9.38 (Sandwich theorem). *Let $(a_n)_{n\in\mathbb{N}}$, $(b_n)_{n\in\mathbb{N}}$ be convergent sequences with the same limit, that is,*

$$\lim_{n\to\infty} a_n = \lim_{n\to\infty} b_n.$$

If $(c_n)_{n\in\mathbb{N}}$ is a third sequence such that

$$\textit{for all } n \in \mathbb{N},\ \ a_n \le c_n \le b_n,$$

then $(c_n)_{n\in\mathbb{N}}$ is also convergent with the same limit, that is,

$$\lim_{n\to\infty} a_n = \lim_{n\to\infty} c_n = \lim_{n\to\infty} b_n.$$

Proof. Let L denote the common limit of $(a_n)_{n\in\mathbb{N}}$ and $(b_n)_{n\in\mathbb{N}}$:

$$\lim_{n\to\infty} a_n = L = \lim_{n\to\infty} b_n.$$

Given $\varepsilon > 0$, let $N_1 \in \mathbb{N}$ be such that for all $n > N_1$, $|a_n - L| < \varepsilon$. Hence for $n > N_1$,

$$L - a_n \le |L - a_n| = |a_n - L| < \varepsilon,$$

and so $L - a_n < \varepsilon$, that is,

$$L - \varepsilon < a_n.$$

Still for the same given $\varepsilon > 0$, let $N_2 \in \mathbb{N}$ be such that for all $n > N_2$, $|b_n - L| < \varepsilon$. So for $n > N_2$, $b_n - L < \varepsilon$, that is,

$$b_n < L + \varepsilon.$$

Thus for $n > N := \max\{N_1, N_2\}$, we have

$$L - \varepsilon < a_n \le c_n \le b_n < L + \varepsilon,$$

and so $L - \varepsilon < c_n < L + \varepsilon$. Consequently, $c_n - L < \varepsilon$ and $-(c_n - L) < \varepsilon$, and so

$$|c_n - L| < \varepsilon.$$

This proves that $(c_n)_{n\in\mathbb{N}}$ is convergent with limit L. □

Example 9.39. Use the Sandwich theorem to show that $\lim_{n\to\infty} \frac{n}{10^n} = 0$.

Proof. It can be shown by induction that for all $n \in \mathbb{N}$, $n^2 < 10^n$.

Consequently, we have

$$0 \le \frac{n}{10^n} \le \frac{n}{n^2} = \frac{1}{n}.$$

Since $\lim_{n\to\infty} 0 = 0 = \lim_{n\to\infty} \frac{1}{n}$, from the Sandwich theorem it follows that the sequence $\left(\frac{n}{10^n}\right)_{n\in\mathbb{N}}$ is convergent and

$$\lim_{n\to\infty} \frac{n}{10^n} = 0.$$

Thus the sequence $\frac{1}{10}, \frac{2}{100}, \frac{3}{1000}, \frac{4}{10000}, \dots$ is convergent with limit 0. □

Example 9.40. Use the Sandwich theorem to show that for any $a, b \in \mathbb{R}$, $\lim_{n\to\infty} (|a|^n + |b|^n)^{\frac{1}{n}} = \max(|a|, |b|)$.

Proof. Without loss of generality, suppose $\max(|a|,|b|) = |a|$. (That is, $0 \le |b| \le |a|$ holds.)

We have $|a|^n \le |a|^n + |b|^n \le |a|^n + |a|^n = 2|a|^n$. Taking nth roots of this, we see that for all n,

$$|a| \le \left(|a|^n + |b|^n\right)^{1/n} \le 2^{1/n}|a|.$$

Now $\left(|a|\right)_{n\in\mathbb{N}}$ converges to $|a|$, and $\left(2^{1/n}|a|\right)_{n\in\mathbb{N}}$ converges to $|a|$ as well, by Example 9.17 and the Algebra of Limits.

So using the Sandwich theorem, it follows that

$$\lim_{n\to\infty} (|a|^n + |b|^n)^{\frac{1}{n}} = |a| = \max(|a|, |b|).$$

In particular, with $a = 24$ and $b = 2005$, we have that $\lim_{n\to\infty} (24^n + 2005^n)^{\frac{1}{n}} = 2005$, that is, the sequence

$$2029, 2005.1436, 2005.001146260873, \dots$$

is convergent with limit 2005. □

Example 9.41. Show that $\lim_{n\to\infty} \left(\frac{n}{n^2+1} + \frac{n}{n^2+2} + \cdots + \frac{n}{n^2+n}\right) = 1$.

Proof. There are n terms in the sum: the smallest is $\frac{n}{n^2+n}$ and the largest is $\frac{n}{n^2+1}$. Thus, for all $n \in \mathbb{N}$, we have

$$\frac{n^2}{n^2+n} \le \frac{n}{n^2+1} + \frac{n}{n^2+2} + \cdots + \frac{n}{n^2+n} \le \frac{n^2}{n^2+1},$$

and since

$$\lim_{n\to\infty} \frac{n^2}{n^2+n} = 1 = \lim_{n\to\infty} \frac{n^2}{n^2+1}.$$

it follows from the Sandwich theorem that

$$\lim_{n\to\infty} \left(\frac{n}{n^2+1} + \frac{n}{n^2+2} + \cdots + \frac{n}{n^2+n}\right) = 1.$$ □

This last is an example where you might want to try to use the Algebra of Limits somehow to split up the limit of the sum of n terms into n separate limits. If you do that... you will get zero as the answer, which is wrong. See (again) Warning 9.32.

As you can see from the examples above, to use the Sandwich theorem to show a sequence $(c_n)_{n\in\mathbb{N}}$ converges to a limit L, what we want to do is to find a couple of 'nice' sequences $(a_n)_{n\in\mathbb{N}}$

and $(b_n)_{n\in\mathbb{N}}$. What 'nice' here often means is: defined by some simple formula, or for whatever other reason, easy to show they both converge to L, but at the same time satisfying $a_n \le c_n \le b_n$ for every $n \in \mathbb{N}$.

In practice, this is often not quite as easy to do as you would like: it can happen that there are two obvious 'simple formulae' that give you sequences both converging to L, but the inequality $a_n \le c_n \le b_n$ can go wrong when n is small. It's always possible to 'fix' this by picking some slightly less simple formulae. But this is annoying to do, and it 'shouldn't matter', because the first few terms of a sequence don't affect the limit. So to avoid needing this 'fix', we prove the following slightly stronger result, which we will also call Sandwich theorem.

Theorem 9.42 (Sandwich theorem). *Let $(a_n)_{n\in\mathbb{N}}$, $(b_n)_{n\in\mathbb{N}}$ be convergent sequences with the same limit, that is,*

$$\lim_{n\to\infty} a_n = \lim_{n\to\infty} b_n .$$

Let N_0 be a natural number. If $(c_n)_{n\in\mathbb{N}}$ is a third sequence such that

$$\text{for all } n \in \mathbb{N} \text{ with } n > N_0 \ , \ \ a_n \le c_n \le b_n,$$

then $(c_n)_{n\in\mathbb{N}}$ is also convergent with the same limit, that is,

$$\lim_{n\to\infty} a_n = \lim_{n\to\infty} c_n = \lim_{n\to\infty} b_n .$$

The point here is that if you write down your two 'simple formulae', verify happily that they both converge to L, and then discover when trying to prove $a_n \le c_n \le b_n$ holds that in fact it doesn't always; it only holds if $n > 1000$, then you can simply say 'let $N_0 = 1000$, then we verified $a_n \le c_n \le b_n$ for all $n \in \mathbb{N}$ with $n > N_0$ so the Sandwich theorem applies' and you are done.

Proof of Theorem 9.42. We will deduce this from Theorem 9.38.

Given the three sequences $(a_n)_{n\in\mathbb{N}}$, $(b_n)_{n\in\mathbb{N}}$ and $(c_n)_{n\in\mathbb{N}}$, and the number N_0, we define two new sequences $(a'_n)_{n\in\mathbb{N}}$ and $(b'_n)_{n\in\mathbb{N}}$ as follows:

$$a'_n = \begin{cases} c_n & \text{if } n \le N_0 \\ a_n & \text{if } n > N_0 \end{cases} \quad \text{and} \quad b'_n = \begin{cases} c_n & \text{if } n \le N_0 \\ b_n & \text{if } n > N_0 \end{cases} .$$

By definition we have $a'_n \le c_n \le b'_n$ for every natural number n. Furthermore, $\lim_{n\to\infty} a'_n = \lim_{n\to\infty} a_n$ and $\lim_{n\to\infty} b'_n = \lim_{n\to\infty} b_n$ by Theorem 9.12. So applying Theorem 9.38 with the sequences $(a'_n)_{n\in\mathbb{N}}$, $(b'_n)_{n\in\mathbb{N}}$ and $(c_n)_{n\in\mathbb{N}}$, we see $\lim_{n\to\infty} c_n$ exists and equals $\lim_{n\to\infty} a'_n = \lim_{n\to\infty} a_n$, as desired. □

9.7 Subsequences and the Bolzano-Weierstrass theorem

In this section we prove an important result in analysis, known as the Bolzano–Weierstrass theorem, which says that every bounded sequence has a convergent 'subsequence'. We begin this section by defining what we mean by a subsequence of a sequence.

Definition 9.43. Let $(a_n)_{n\in\mathbb{N}}$ be a sequence and let $(n_k)_{k\in\mathbb{N}}$ be a strictly increasing sequence of natural numbers. Then $(a_{n_k})_{k\in\mathbb{N}}$ is called a *subsequence of* $(a_n)_{n\in\mathbb{N}}$.

Another way to think about this is: a subsequence is what you get from a sequence by crossing out some terms (but not rearranging anything).

Example 9.44.

(i) $\left(\frac{1}{2n}\right)_{n\in\mathbb{N}}$, $\left(\frac{1}{n^2}\right)_{n\in\mathbb{N}}$, $\left(\frac{1}{n!}\right)_{n\in\mathbb{N}}$ and $\left(\frac{1}{n^n}\right)_{n\in\mathbb{N}}$ are all subsequences of $\left(\frac{1}{n}\right)_{n\in\mathbb{N}}$.

(ii) Let p_n be the n-th prime number. (Thus $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, etc.) Then the sequence $(a_n)_{n\in\mathbb{N}}$ defined by $a_n = \frac{1}{p_n}$ is a subsequence of $\left(\frac{1}{n}\right)_{n\in\mathbb{N}}$.

(iii) The sequence

$$\tfrac{1}{2},\ 1,\ \tfrac{1}{3},\ \tfrac{1}{4},\ \dots$$

is not a subsequence of $\left(\frac{1}{n}\right)_{n\in\mathbb{N}}$.

(iv) The sequence $\left((-1)^{2n}\right)_{n\in\mathbb{N}}$, that is, the constant sequence

$$1,\ 1,\ 1,\ \dots$$

and the sequence $\left((-1)^{2n-1}\right)_{n\in\mathbb{N}}$, that is, the constant sequence

$$-1,\ -1,\ -1,\ \dots$$

are both subsequences of $\left((-1)^n\right)_{n\in\mathbb{N}}$. □

Theorem 9.45. *If $(a_n)_{n\in\mathbb{N}}$ is a convergent sequence with limit L, then any subsequence of $(a_n)_{n\in\mathbb{N}}$ is also convergent with the limit L.*

Proof. Let $(a_{n_k})_{k\in\mathbb{N}}$ be a subsequence of $(a_n)_{n\in\mathbb{N}}$.

Given $\varepsilon > 0$, let $N \in \mathbb{N}$ be such that for all $n > N$, $|a_n - L| < \varepsilon$.

Since $1 \le n_1 < n_2 < \dots$ and all the n_k are integers, we have $n_k \ge k$ for each integer k.

Suppose $k > N$. Then $n_k \ge k > N$, so $|a_{n_k} - L| < \varepsilon$. This gives us, by definition,

$$\lim_{k\to\infty} a_{n_k} = L\,.$$ □

This theorem lets us build new convergent sequences from old ones; it also gives us a new way to prove divergence of sequences.

Example 9.46.

(i) $\left(\frac{1}{2n}\right)_{n\in\mathbb{N}}$, $\left(\frac{1}{n^2}\right)_{n\in\mathbb{N}}$, $(2^{-n})_{n\in\mathbb{N}}$, $\left(\frac{1}{n!}\right)_{n\in\mathbb{N}}$ and $\left(\frac{1}{n^n}\right)_{n\in\mathbb{N}}$ are convergent sequences with limit 0.

(ii) The sequence $\left((-1)^n\right)_{n\in\mathbb{N}}$ is divergent, since the subsequence $1, 1, 1, \dots$ has limit 1, while the subsequence $-1, -1, -1, \dots$ has limit -1.

Let's now state the Bolzano-Weierstrass theorem.

Theorem 9.47. (Bolzano[3]–Weierstrass[4] theorem.) *Every bounded sequence has a convergent subsequence.*

It probably isn't at all obvious *why* this is an interesting result at this point. But we will see later that it is very useful.

There are several different ways to prove this theorem. We'll give maybe the easiest, which lets the theorems we already proved do most of the work.

The idea is the following. We start with an interval $[-M, M]$ which contains all the terms of the sequence (which we can, because the sequence is bounded). We'll write $s_1 = -M$ and $t_1 = M$.

Then we look at the two intervals $[-M, 0]$ and $[0, M]$, which together cover $[-M, M] = [s_1, t_1]$. One of these two intervals has to contain infinitely many terms of the sequence, call it $[s_2, t_2]$. (It might be both; then pick the first half).

Then we similarly split $[s_2, t_2]$ into two halves, and pick one, $[s_3, t_3]$ that contains infinitely many terms of the sequence. And so on.

Now $(s_k)_{k\in\mathbb{N}}$ is a monotone increasing bounded sequence. So by Theorem 9.26, this sequence converges to a limit L. It's not hard to believe (since the intervals get shorter and shorter) that also the sequence $(t_k)_{k\in\mathbb{N}}$ converges to L.

Finally, we can construct the subsequence of $(a_n)_{n\in\mathbb{N}}$ that we want. Choose $n_1 = 1$, then a_{n_1} is in $[s_1, t_1]$. Now choose $n_2 > n_1$ such that a_{n_2} is in $[s_2, t_2]$. This is possible because infinitely many terms of the sequence are in $[s_2, t_2]$. And so on; in general we choose $n_k > n_{k-1}$ such that a_{n_k} is in $[s_k, t_k]$.

Now for each $k \in \mathbb{N}$, we have $a_{n_k} \in [s_k, t_k]$, i.e. $s_k \le a_{n_k} \le t_k$. That means the sequences $(s_k)_{k\in\mathbb{N}}$ and $(t_k)_{k\in\mathbb{N}}$ sandwich $(a_{n_k})_{k\in\mathbb{N}}$, and by the Sandwich Theorem, $(a_{n_k})_{n\in\mathbb{N}}$ is convergent with limit L—and we're done!

Let's now fill in the details of a formal proof.

Proof. Given a bounded sequence $(a_n)_{n\in\mathbb{N}}$, by definition there is a real number $M > 0$ such that $[-M, M]$ contains each a_n with $n \in \mathbb{N}$.

Step 1: We let $s_1 = -M$ and $t_1 = M$, so infinitely many terms of $(a_n)_{n\in\mathbb{N}}$ are in $[s_1, t_1]$ and $t_1 - s_1 = 2M$.

We now start defining real numbers s_k and t_k such that infinitely many terms of $(a_n)_{n\in\mathbb{N}}$ are in $[s_k, t_k]$, and $t_k - s_k = 2^{2-k}M$, and $s_{k-1} \le s_k < t_k \le t_{k-1}$, recursively, for each $k \ge 2$ as follows.

If there are infinitely many terms of $(a_n)_{n\in\mathbb{N}}$ in $\left[s_{k-1}, \frac{1}{2}(s_{k-1} + t_{k-1})\right]$, we choose $s_k = s_{k-1}$ and $t_k = \frac{1}{2}(s_{k-1} + t_{k-1})$.

Otherwise, there are only finitely many terms of $(a_n)_{n\in\mathbb{N}}$ in $\left[s_{k-1}, \frac{1}{2}(s_{k-1} + t_{k-1})\right]$, but there are infinitely many terms in $[s_{k-1}, t_{k-1}]$, so there must be infinitely many terms of $(a_n)_{n\in\mathbb{N}}$ in $\left[\frac{1}{2}(s_{k-1} + t_{k-1}), t_{k-1}\right]$. So we choose $s_k = \frac{1}{2}(s_{k-1} + t_{k-1})$ and $t_k = t_{k-1}$.

Note that in both cases, $t_k - s_k = \frac{1}{2}(t_{k-1} - s_{k-1}) = \frac{1}{2}\cdot 2^{2-(k-1)}M = 2^{2-k}M$ and $s_{k-1} \le s_k < t_k \le t_{k-1}$.

Step 2: By construction, the sequence of real numbers $(s_k)_{k\in\mathbb{N}}$ is monotone increasing, and it is bounded (with bound M). So by Theorem 9.26, there is a number L such that $\lim_{k\to\infty} s_k = L$. We now show that also $\lim_{k\to\infty} t_k = L$.

Given $\varepsilon > 0$, let $K_1 \in \mathbb{N}$ be such that for all $k > K_1$ we have $|s_k - L| < \frac{\varepsilon}{2}$; this exists since $\lim_{k\to\infty} s_k = L$. Let $K_2 \in \mathbb{N}$ be such that for all $k > K_2$ we have $2^{2-k}M < \frac{\varepsilon}{2}$; this exists since $\lim_{k\to\infty} 2^{-k} = 0$ (Example 9.46) and the Algebra of Limits. Now let $K = \max(K_1, K_2)$.

Suppose $k > K$. Then we have

$$|t_k - L| \le |t_k - s_k| + |s_k - L| < 2^{2-k}M + \tfrac{\varepsilon}{2} < \tfrac{\varepsilon}{2} + \tfrac{\varepsilon}{2} = \varepsilon$$

[3] Bernhard Bolzano (1781–1848)

[4] Karl Weierstrass (1815–1897)

which is what we need for the definition of $\lim_{k\to\infty} t_k = L$.

Step 3: Let $n_1 = 1$. Note that $a_{n_1} \in [s_1, t_1] = [-M, M]$ by definition of M. Now for each $k \geq 2$, recursively, we choose $n_k > n_{k-1}$ such that $a_{n_k} \in [s_k, t_k]$. For each k, we can do this because there are infinitely many terms of $(a_n)_{n\in\mathbb{N}}$ within $[s_k, t_k]$, and at most n_{k-1} of them have index n_{k-1} or smaller.

By definition, we have $s_k \leq a_{n_k} \leq t_k$ for each $k \in \mathbb{N}$. So by the Sandwich Theorem (Theorem 9.38) we have $\lim_{k\to\infty} a_{n_k} = L$, and this is our desired convergent subsequence. □

Example 9.48. Consider the sequence $(a_n)_{n\in\mathbb{N}}$ of fractional parts of integral multiples of $\sqrt{2}$, defined by

$$a_n = n\sqrt{2} - \lfloor n\sqrt{2} \rfloor, \text{ for } n \in \mathbb{N},$$

where, for $x \in \mathbb{R}$, $\lfloor x \rfloor$ is the *floor function* of x. Show that this sequence has a convergent subsequence.

The terms of the sequence $(a_n)_{n\in\mathbb{N}}$ are as follows:

$$\begin{aligned}
\sqrt{2} &= 1.414213\ldots & &\text{so} & a_1 &= 0.414213\ldots\\
2\sqrt{2} &= 2.828427\ldots & &\text{so} & a_2 &= 0.828427\ldots\\
3\sqrt{2} &= 4.242640\ldots & &\text{so} & a_3 &= 0.242640\ldots\\
4\sqrt{2} &= 5.656854\ldots & &\text{so} & a_4 &= 0.656854\ldots\\
5\sqrt{2} &= 7.071067\ldots & &\text{so} & a_5 &= 0.071067\ldots\\
6\sqrt{2} &= 8.485281\ldots & &\text{so} & a_6 &= 0.485281\ldots\\
& & &\vdots & &
\end{aligned}$$

Proof. The sequence $(a_n)_{n\in\mathbb{N}}$ is bounded: indeed, $0 \leq a_n < 1$ for every $n \in \mathbb{N}$. So by the Bolzano–Weierstrass theorem this sequence has a convergent subsequence. □

We have seen that if $(a_n)_{n\in\mathbb{N}}$ is convergent with limit L, then any subsequence also converges to L (Theorem 9.45). We've also seen examples of divergent sequences $(a_n)_{n\in\mathbb{N}}$ for which there are exactly two *limit points*, that is numbers $p \in \mathbb{R}$ such that there is a subsequence of $(a_n)_{n\in\mathbb{N}}$ converging to p. Both sequences (iii) and (iv) from Example 9.2 have limit points 1 and −1, and nothing else. It's easy to give (in both cases) a subsequence which converges to 1, and another one that converges to −1. Why are there no other limit points?

Activity 9.9. *Show that, if $p \in \mathbb{R}$ is not equal to 1 or −1 then there is no subsequence of either $\big((-1)^n\big)_{n\in\mathbb{N}}$ or of $\big((-1)^n(1 + 1/n)\big)_{n\in\mathbb{N}}$ that converges to p.*

A sequence which is not bounded doesn't have to have a convergent subsequence (because the condition of the Bolzano-Weierstrass theorem isn't satisfied).

Activity 9.10. *Find a sequence $(a_n)_{n\in\mathbb{N}}$ which is not bounded and which has no convergent subsequence.*

Find another sequence $(b_n)_{n\in\mathbb{N}}$ which is not bounded and which does have a convergent subsequence.

It's not too hard to come up with sequences which have two, or three, or ten, different limit points. But there can be many more.

Activity 9.11. *Show that for any real number x and any $\varepsilon > 0$, there are infinitely many rational numbers in the interval $(x - \varepsilon, x)$.*

Suppose that $(a_n)_{n\in\mathbb{N}}$ is any sequence such that every rational number is a term of the sequence. Prove that for every real number x, there is a subsequence of $(a_n)_{n\in\mathbb{N}}$ which converges to x.

You could reasonably object to the above: but maybe there isn't any such sequence $(a_n)_{n\in\mathbb{N}}$? But there are in fact such sequences. Here is an example. For any rational number $\frac{p}{q}$ written in lowest terms (i.e. q is positive, and p and q have no common factor bigger than 1) say the *weight* of $\frac{p}{q}$ is $|p| + q$. For any $w \in \mathbb{N}$, there are at most $2w$ rational numbers of weight w: we have to choose $1 \le q \le w$, and then we are left with two possibilities, either $p = w - q$ or $p = -(w - q)$.

So we can make a sequence listing all the rational numbers by first writing down all the ones with weight 1 (there is only one, $\frac{0}{1}$) and then weight 2, weight 3, and so on.

In fact, the sequence from Example 9.48 has a similar property: for any $x \in [0, 1]$, there is a subsequence converging to x. This is rather harder to prove, though!

9.7.1 Non-examinable: another proof of Bolzano-Weierstrass

The proof we gave of the Bolzano-Weierstrass theorem is not the only way to prove it. Another very natural approach is to notice that if $(a_n)_{n\in\mathbb{N}}$ is bounded, so is any subsequence. And we already know that any monotone bounded sequence converges—so it is enough to prove the following.

Theorem 9.49. *Every sequence has a monotone subsequence.*

The proof of this splits up into the following two activities.

Activity 9.12. *Given a sequence $(a_n)_{n\in\mathbb{N}}$, let n_1 be an index such that $a_{n_1} = \max(a_1, a_2, \dots)$, if it exists. Let n_2 be an index such that $a_{n_2} = \max(a_{n_1+1}, a_{n_1+2}, \dots)$, if it exists, and so on: given $k \ge 3$ and n_{k-1}, let n_k be an index such that $a_{n_k} = \max(a_{n_{k-1}+1}, a_{n_{k-1}+2}, \dots)$ if it exists.*

Prove that either we obtain a monotone decreasing subsequence $(a_{n_k})_{k\in\mathbb{N}}$ of $(a_n)_{n\in\mathbb{N}}$, or there is some $K \in \mathbb{N}$ such that $(a_K, a_{K+1}, a_{K+2}, \dots)$ has no biggest term.

Activity 9.13. *Given a sequence $(b_n)_{n\in\mathbb{N}}$ which has no biggest term, let $n_1 = 1$ and for each $k \ge 2$, given n_{k-1}, let n_k be the smallest index such that $b_{n_k} > b_{n_{k-1}}$, if it exists. Prove that this gives a subsequence $(b_{n_k})_{k\in\mathbb{N}}$ which is strictly increasing.*

Finally—and this is easier—put the pieces together.

Activity 9.14. *Use the statements you proved in Activities 9.12 and 9.13 to prove Theorem 9.49. Use Theorems 9.26 and 9.49 to prove Theorem 9.47.*

9.8 Sample exercises

Exercise 9.1. *Prove, directly from the definition, that the sequence $\left(\frac{3n-1}{n+2}\right)_{n\in\mathbb{N}}$ is convergent, and find its limit.*

Exercise 9.2. *(a) Let $(a_n)_{n\in\mathbb{N}}$ be a convergent sequence with limit L, and let M be some real number with $M \ne L$. Show that the set $\{n \in \mathbb{N} \mid a_n = M\}$ is bounded above.*

(b) Prove that the sequence $((-1)^n)_{n\in\mathbb{N}}$ is divergent.

Exercise 9.3. *Use the definition of limit to prove directly that 1 is not a limit of the sequence $(1/n)_{n\in\mathbb{N}}$.*

Exercise 9.4. *In each of the cases listed below, give an example of a divergent sequence $(a_n)_{n\in\mathbb{N}}$ that satisfies the given conditions.*

(a) For every $\varepsilon > 0$, there exists an N such that, for infinitely many $n > N$, $|a_n - 1| < \varepsilon$.

(b) There exists an $\varepsilon > 0$ *and an* $N \in \mathbb{N}$ *such that for all* $n > N$, $|a_n - 1| < \varepsilon$.

Exercise 9.5. *Let* $(a_n)_{n\in\mathbb{N}}$ *be a sequence defined by*

$$a_1 = 1 \text{ and } a_n = \frac{2n+1}{3n} a_{n-1} \text{ for } n \geq 2.$$

Prove that $(a_n)_{n\in\mathbb{N}}$ *is convergent.*

Exercise 9.6. *Suppose that the sequence* $(a_n)_{n\in\mathbb{N}}$ *is bounded. Prove that the sequence* $(c_n)_{n\in\mathbb{N}}$ *defined by*

$$c_n = \frac{a_n^3 + 5n}{a_n^2 + n}$$

is convergent, and find its limit.

Exercise 9.7. ***Sample Exam Question. 2007 Q5.***

(a) What does it mean to say that a sequence $(a_n)_{n\geq 1}$ *is convergent? Use this definition to show that if* $(a_n)_{n\geq 1}$ *is convergent, then* $(a_{n+1})_{n\geq 1}$ *is also a convergent sequence and* $\lim_{n\to\infty} a_n = \lim_{n\to\infty} a_{n+1}$.

Let b *be a real number with* $2 < b < 3$. *We define a sequence* $(b_n)_{n\geq 1}$ *by*

$$b_1 = b \text{ and } b_{n+1} = b_n^2 - 4b_n + 6 \text{ for every } n \in \mathbb{N}.$$

(b) Show that $2 < b_n < 3$ *for every* $n \in \mathbb{N}$.

(c) Prove that $(b_n)_{n\geq 1}$ *is a monotone sequence.*

(d) Explain why $\lim_{n\to\infty} b_n$ *exists and find its value.*

(e) Let $S = \{b_n \mid n \in \mathbb{N}\}$. *Find* $\sup S, \inf S, \max S, \min S$. *Justify your answers.*

9.9 Comments on selected activities

Comment on Activity 9.1.

(i) For this, you should find that given $\varepsilon > 0$, choosing $N = \lceil 1/\varepsilon \rceil$, or anything bigger, will work. If your N is smaller, then your proof is wrong.

(ii) As (i).

(iii) You need to consider all possible values of $L \in \mathbb{R}$, and rule out all of them. If you only consider $L = 1$ and $L = -1$, the 'obvious' limits, then you haven't shown that (for example) this sequence doesn't converge to 0. Whatever L is, you should find that the definition of convergence, with $\varepsilon = 1$, fails. Any smaller ε will also fail (but you only need to show that some one ε is a counterexample). If you tried to use $\varepsilon > 1$, then your proof will not work for $L = 0$.

(iv) As (iii).

(v) For any $\varepsilon > 0$, you can simply choose $N = 1$. But if you wrote something bigger (e.g. that $N = \lceil \frac{1}{\varepsilon} \rceil$) your proof works, it's just a bit more complicated than necessary.

(vi) This is a bit tricky. Given $L \in \mathbb{R}$, we want to rule out that $(n)_{n\in\mathbb{N}}$ converges to L. We will use $\varepsilon = 1$. This is a counterexample to the definition of convergence to L for the following reason.

Whatever N is given, it is not true that for all $n > N$ we have $|n - L| < 1$. Indeed, we can choose $n = \max(N + 1, \lceil |L| \rceil + 1)$. Now by definition we have $n > N$, and by definition we have $n \geq |L| + 1$, so $|n - L| \geq 1$. □

(vii) This is really the 'wrong time' to try to prove that this sequence is convergent; we will prove it after we develop some tools that help us find when sequences are convergent.

(viii) Again, this is really the wrong time to look at this sequence. The idea is that (eventually!) the exponential will tend to zero much faster than the polynomial grows, so it will win in the long run. But formally proving this needs a bit of algebra, and it helps to know Bernoulli's Inequality.

(ix) For this, you should find that given $\varepsilon > 0$, choosing $N = \lceil 3/\varepsilon \rceil$, or anything bigger, will work. If your choice of N tries to take into account whether N is odd or even, then probably your proof is wrong. If it takes into account whether n is odd or even, then your proof is definitely wrong: see Warning 9.14.

Comment on Activity 9.2. Given $\varepsilon > 0$, we choose $N = \left\lceil \frac{1}{\varepsilon} \right\rceil$.

Given $n > N$, we have

$$\left|\tfrac{1}{n} - 0\right| = \tfrac{1}{n} < \tfrac{1}{N} \leq \varepsilon\,,$$

which is what we wanted to show for the definition of convergence to 0.

If your N isn't as big as the one above, your proof is wrong. If there is an n in your definition of N, your proof is wrong.

If your N is bigger than the one above, then most likely things are fine.

Comment on Activity 9.3. If there does not exist any $N \in \mathbb{N}$ such that '$\forall n > N\,,\ |a_n - L| < \varepsilon$' then that means that for any given $N \in \mathbb{N}$, there is some $n > N$ such that $|a_n - L| \geq \varepsilon$.

We will use this assertion infinitely many times, for different choices of N.

First (with $N = 1$) there is some integer, which we call n_1, such that $n_1 > 1$ and $|a_{n_1} - L| \geq \varepsilon$.

Now (with $N = n_1$) there is some integer n_2, such that $n_2 > n_1$ and $|a_{n_2} - L| \geq \varepsilon$.

Recursively, suppose for some $k \geq 2$ we have integers $n_1 < n_2 < \cdots < n_k$. Then (with $N = n_k$) there is some integer n_{k+1} such that $n_{k+1} > n_k$ and $|a_{n_k} - L| \geq \varepsilon$.

The set $\{n_1, n_2, \dots\}$ is infinite. This is because there is an (obvious!) bijection between this set and $\mathbb{N}$, namely $n_k \leftrightarrow k$ for each $k \in \mathbb{N}$, and we already proved that $\mathbb{N}$ is infinite. To check this bijection is well-defined (i.e. it really is a bijection) we need to observe that if $k < k'$ are in $\mathbb{N}$, then they are in correspondence with two *different* members of $\{n_1, n_2, \dots\}$, namely n_k and $n_{k'}$, which by construction satisfy $n_k < n_{k'}$.

Comment on Activity 9.4. See Activity 9.1(vi).

Comment on Activity 9.5. We have $a_n = \sum_{k=1}^{n} \frac{1}{k^k}$. We want to prove by induction that $a_n \leq \frac{3}{2} - \frac{1}{2^n}$.

The base case is $a_1 \leq \frac{3}{2} - \frac{1}{2^1}$, which we check by calculation is true (with equality).

Suppose as an induction hypothesis that for some given $s \in \mathbb{N}$ we have $a_s \leq \frac{3}{2} - \frac{1}{2^s}$.

Then we have

$$a_{s+1} = a_s + \tfrac{1}{(s+1)^{s+1}} \leq \tfrac{3}{2} - \tfrac{1}{2^s} + \tfrac{1}{(s+1)^{s+1}} \leq \tfrac{3}{2} - \tfrac{1}{2^s} + \tfrac{1}{2^{s+1}} = \tfrac{3}{2} - \tfrac{1}{2^{s+1}}\,,$$

which is what we wanted for the induction step. By induction, we conclude the desired inequality holds for all n. □

Comment on Activity 9.7. Suppose $\lim_{n\to\infty} a_n = A$ and $\lim_{n\to\infty} b_n = B$.

Given $\varepsilon > 0$, let N_a be such that for all $n > N_a$ we have $|a_n - A| < \frac{\varepsilon}{2}$, and let N_b be such that for all $n > N_b$ we have $|b_n - B| < \frac{\varepsilon}{2}$. Both N_a and $N - b$ exist by the definition of convergence. We choose $N = \max(N_a, N_b)$.

Suppose $n > N$. Then we have

$$\big|(a_n + b_n) - (A + B)\big| = \big|(a_n - A) + (b_n - B)\big| \le |a_n - A| + |b_n - B| < \tfrac{\varepsilon}{2} + \tfrac{\varepsilon}{2} = \varepsilon\,,$$

which is what we wanted to prove. □

Comment on Activity 9.8. Suppose $(a_n)_{n\in\mathbb{N}}$ is a sequence of nonnegative reals converging to 0. We want to show $\big(\sqrt{a_n}\big)_{n\in\mathbb{N}}$ converges to 0.

If you're revising, look at the exercise solutions. If you are looking for solutions to next week's homework, they are not here.

Comment on Activity 9.9. This is a little bit tricky because you have to consider all possible subsequences, and you don't know what these might look like. However, the point is that if $(a_{n_k})_{k\in\mathbb{N}}$ converges to some $p \in \mathbb{R}$, then for any $\varepsilon > 0$, from some point on all the terms of the subsequence are within ε of p. This is infinitely many terms. So those infinitely many terms have to also be present in the original sequence:

If $(a_n)_{n\in\mathbb{N}}$ has a subsequence converging to $p \in \mathbb{R}$, then for every $\varepsilon > 0$ there exist infinitely many terms of $(a_n)_{n\in\mathbb{N}}$ which are in $(p - \varepsilon, p + \varepsilon)$.

And now you just need to figure out how to choose ε, given p which is not 1 or −1, such that $(p - \varepsilon, p + \varepsilon)$ doesn't contain infinitely many terms of the given sequence. One choice that will work is $\varepsilon = \big||p| - 1\big|$.

Comment on Activity 9.10. For $(a_n)_{n\in\mathbb{N}}$, one choice that works is $(n)_{n\in\mathbb{N}}$. We've already seen that this sequence isn't bounded, and almost exactly the same proof shows no subsequence is bounded either, so it can't have a convergent subsequence.

For $(b_n)_{n\in\mathbb{N}}$, we can take b_n equal to either n (if n is odd) or zero (if n is even). This clearly isn't bounded, but the subsequence of even-numbered terms converges to 0.

Comment on Activity 9.11. If x is rational, then $x - \frac{1}{n}$ is rational for each $n \in \mathbb{N}$ and (if $n > 1/\varepsilon$) bigger than $x - \varepsilon$.

If $x - \varepsilon$ is rational, then similarly $x - \varepsilon + \frac{1}{n}$ is rational for each $n \in \mathbb{N}$ and if $n > 1/\varepsilon$ smaller than x.

So suppose x and $x - \varepsilon$ are both irrational: then both of them have a unique decimal representation (i.e. neither finishes with an infinite string of 9s). Since $x - \varepsilon < x$, there must be a first decimal place where the expansions differ. Let y be the number we get by terminating the decimal expansion of x at that place. Then y is by construction smaller than x, and larger than $x - \varepsilon$, and it is rational.

Now $y + \frac{1}{n}$ is rational and smaller than x for all $n > \frac{1}{x-y}$.

In each case, we found the desired infinitely many rational numbers between x and $x - \varepsilon$.

Now suppose that $(a_n)_{n\in\mathbb{N}}$ is a sequence whose terms contain all the rational numbers. Given any real number x and any $\varepsilon > 0$, we just proved that there are infinitely many terms of the sequence in $(x - \varepsilon, x)$.

In particular, we can construct a subsequence $(a_{n_k})_{k\in\mathbb{N}}$ as follows. Let n_1 be any index such that $x - 1 < a_{n_1} < x$ (using the above observation with $\varepsilon = 1$, such an index exists).

Now for each $k \ge 2$ in turn, given n_{k-1}, look at all the terms of $(a_n)_{n\in\mathbb{N}}$ which are in $\big(x - \frac{1}{k}, x\big)$. There are infinitely many, and only finitely many have an index less than or equal to n_{k-1}. So we can choose $n_k > n_{k-1}$ such that $x - \frac{1}{k} < a_{n_k} < x$.

The sequence $(a_{n_k})_{k\in\mathbb{N}}$ is sandwiched by $\big(x - \frac{1}{k}\big)_{k\in\mathbb{N}}$ and $(x)_{k\in\mathbb{N}}$, so by the Sandwich Theorem we have $\lim_{k\to\infty} a_{n_k} = x$. □

Comment on Activity 9.12. If at each stage in the construction the 'if it exists' is true, then we obtain a subsequence $(a_{n_k})_{k\in\mathbb{N}}$. By construction a_{n_1} is the biggest term in the entire sequence; in particular it is at least as big as all the following terms, so whatever $n_2 > n_1$ we choose we will have $a_{n_1} \geq a_{n_2}$. Similarly, for each $k \geq 2$, when we choose a_{n_k} it is at least as big as all of the following terms, and in particular whatever n_3 we choose we get $a_{n_k} \geq a_{n_{k+1}}$. So this is a monotone decreasing subsequence.

What is left is the possibility that at some stage k in the construction the 'if it exists' is false. That is, $(a_{n_{k-1}+1}, a_{n_{k-1}+2}, a_{n_{k-1}+3}, \dots)$ has no maximum element. Letting $K = n_{k-1} + 1$, that is precisely saying that $(a_K, a_{K+1}, \dots)$ has no biggest term.

Comment on Activity 9.13. The point here which you need to see is the following. If for some $k \geq 1$ we have followed the construction up to stage k—that is, we have constructed n_k—then we know that b_{n_k} is not a biggest element in the sequence; there is certainly, somewhere in the sequence, a bigger element. *But* we need to be sure that there is a bigger element *which comes after* b_{n_k}. This is the reason for choosing the *smallest index* every time: we know b_{n_k} is (by construction) bigger than all the terms from $b_{n_{k-1}}$ to b_{n_k-1}, and so (by an induction argument) it is the biggest term in $\{b_1, b_2, \dots, b_{n_k}\}$. So whatever the bigger term is that we know exists, it *has* to come after b_{n_k}.

This shows that the 'if it exists' will always be true—there will always be such a term—and then by construction we get a strictly increasing subsequence.

Comment on Activity 9.14. The proof of Theorem 9.49 is now the following. By Activity 9.12, either $(a_n)_{n\in\mathbb{N}}$ has a monotone decreasing subsequence, or it has a subsequence which has no biggest term. But then by Activity 9.13, *that* subsequence has a subsequence which is strictly increasing—and this is a subsequence of a subsequence of $(a_n)_{n\in\mathbb{N}}$, so by definition it is a subsequence of $(a_n)_{n\in\mathbb{N}}$. Either way, we found a monotone subsequence. □

Now to prove the Bolzano-Weierstrass theorem, suppose $(a_n)_{n\in\mathbb{N}}$ is a bounded sequence. Then any subsequence is also bounded, and by Theorem 9.49 there is a monotone subsequence $(a_{n_k})_{k\in\mathbb{N}}$. Now $(a_{n_k})_{k\in\mathbb{N}}$ is a bounded monotone sequence, so by Theorem 9.26 it is convergent. □

9.10 Solutions to exercises

Solution to Exercise 9.1.

The first thing to do here is to figure out what the limit is. A thought process is "for large n, the numerator is about $3n$ and the denominator is about n, so the fraction is about 3". Hence we expect 3 to be the limit. Let's now prove it.

Given $\varepsilon > 0$, we set N to be some natural number such that ... (leave this blank for the moment, and come back and fill it in later).

Now, for $n > N$, we have

$$\left|\frac{3n-1}{n+2} - 3\right| = \left|\frac{3n-1-3n-6}{n+2}\right| = \frac{7}{n+2} < \frac{7}{N}.$$

We now want to finish off by deducing that $7/N < \varepsilon$. So what do we want from N? Evidently, it suffices to take $N > 7/\varepsilon$. So now we go back and fill in: "N to be some natural number such that $N > 7\varepsilon$." Then we can indeed conclude that, for $n > N$, $|\frac{3n-1}{n+2} - 3| < \frac{7}{N} < \varepsilon$. So the sequence tends to 3, as claimed.

Solution to Exercise 9.2.

(a) How are we going to *use* the fact that the sequence $(a_n)_{n\in\mathbb{N}}$ converges to L? One idea you might have is to say that, for large enough N, the elements of the sequence have to be "close to L", so that they cannot be equal to M. How close should close be: closer than the distance $|L - M|$ between L and M.

So set $\varepsilon = |M - L|$. By the definition of a limit, there is some $N \in \mathbb{N}$ such that, for $n > N$, $|a_n - L| < |M - L|$, and that certainly implies that $a_n \neq M$.

That means that, if n has the property that $a_n = M$, then $n \leq N$. In other words, N is an upper bound for the set $\{n \in \mathbb{N} : a_n = M\}$, as required.

(b) We can use part (a): that's the point. Suppose the sequence does tend to a limit, and call the limit L. If $L \neq 1$, then $\{n \in \mathbb{N} \mid (-1)^n = 1\}$, which is the set of even numbers, is bounded above. That is false, which leaves only the possibility that $L = 1$. But then the set $\{n \in \mathbb{N} \mid (-1)^n = -1\}$, which is the set of odd numbers, is bounded above, which again is false. We conclude that the sequence does not converge to any limit, i.e., it is divergent.

Solution to Exercise 9.3.

To show that the sequence $(a_n)_{n\in\mathbb{N}}$ does **not** tend to the limit L, we need to show that there exists $\varepsilon > 0$ such that, for all $N \in \mathbb{N}$, there is some $n > N$ with $|a_n - L| \geq \varepsilon$.

We can take $\varepsilon = 1/2$ here. Now, whatever $N \in \mathbb{N}$ is proposed, take $n > \max(2, N)$. We see that $a_n < 1/2$, and so $|a_n - 1| > 1/2$. Thus indeed a_n does not converge to 1.

Solution to Exercise 9.4.

(a) Take, for instance, the sequence $(a_n)_{n\in\mathbb{N}}$ where $a_n = 1$ for n odd, and $a_n = 0$, for n even. Given any $\varepsilon > 0$, take $N = 1$: then $|a_n - L| = 0 < \varepsilon$ for all odd $n > 1$.

(b) Take the same sequence (why not?), and take $\varepsilon = 2$ and $N = 1$. Then indeed $|a_n - L| < 2$ for all $n > 1$.

[A sequence satisfies (a) if $L = 1$ is a *limit point* of the sequence. A sequence satisfies (b) (whatever L is) if and only if the sequence is *bounded.*]

Solution to Exercise 9.5.

You might want to generate a few terms of the sequence (a_n) in order to get a feel for what is going on. Whether or not this helps, you need to have the idea that the terms of the sequence (a_n) get smaller, while staying positive, and so that perhaps the sequence is decreasing and bounded below. In fact, you might (correctly) suspect that the sequence converges to 0, but you're not asked to prove that.

Indeed, it is clear that since the first term a_1 is positive, and each subsequent term is a positive multiple of the previous term, all terms are positive. (By now, you should be confident that you can write a formal induction argument if you really needed, but as far as I'm concerned this will suffice here.)

Also, since $2n + 1 \leq 3n$ for all $n \geq 2$, it follows that $a_n \leq a_{n-1}$ for all $n \geq 2$, in other words that (a_n) is a decreasing sequence, bounded below by 0. Therefore the sequence is convergent.

Solution to Exercise 9.6.

There are various ways to tackle this exercise. But they have one thing in common: the first thing to do is to understand how the sequence $(c_n)_{n\in\mathbb{N}}$ behaves for large n. Since the sequence $(a_n)_{n\in\mathbb{N}}$ is bounded, say with $|a_n| \leq M$ for every $n \in \mathbb{N}$, then also $|a_n^3| \leq M^3$ and $a_n^2 \leq M^2$. So the numerator "behaves like" $5n$, while the denominator "behaves like' n, in the sense that the other terms are "of smaller order" for large n. So we expect the limit to be equal to 5.

Here are three ways to show this.

(a) Write $c_n - 5 = \frac{a_n^3 - 5a_n^2}{a_n^2 + n}$, so

$$|c_n - 5| \leq \frac{|a_n^3 - 5a_n^2|}{n} \leq \frac{M^3 + 5M^2}{n}.$$

Now, given $\varepsilon > 0$, we can choose $N > (M^3 + 5M^2)/\varepsilon$, so that, for $n > N$, we have

$$|c_n - 5| \leq \frac{M^3 + 5M^2}{n} \leq \frac{M^3 + 5M^2}{N} < \varepsilon.$$

(b) Use the Algebra of Limits. Write

$$c_n = \frac{5 + a_n^3/n}{1 + a_n^2/n}.$$

Now show that a_n^3/n and a_n^2/n both tend to zero as $n \to \infty$. One way to do this is to use the Sandwich Theorem: $-M^3/n \le a_n^3/n \le M^3/n$, and by the Algebra of Limits the two sandwiching sequences tend to zero as $n \to \infty$, so a_n^3/n also does; similarly for a_n^2/n. Then we have that $\lim_{n\to\infty} c_n = \frac{5+\lim_{n\to\infty} a_n^3/n}{1+\lim_{n\to\infty} a_n^2/n} = 5$.

(c) Use the Sandwich Theorem directly Note that

$$\frac{-M^3 + 5n}{n} \le c_n \le \frac{M^3 + 5n}{n}.$$

Now argue that both the sequences on the outside tend to 5, and hence so does $(c_n)_{n\in\mathbb{N}}$.

Solution to Exercise 9.7. Since this was an exam question, I'll give the mark scheme (for this solution—there are other possibilities which would be marked differently and that could also get full marks) too.

(a) [2pts] A sequence $(a_n)_{n\ge1}$ is convergent if there is $L \in \mathbb{R}$ so that for every $\varepsilon > 0$ there is $N \in \mathbb{N}$ such that for all $n > N$ we have $|a_n - L| < \varepsilon$.

[3pts] Suppose that $(a_n)_{n\in\mathbb{N}}$ is convergent with limit L. Take any $\varepsilon > 0$. By the definition of convergence, there is some $N \in \mathbb{N}$ such that, for all $n > N$, $|a_n - L| < \varepsilon$. Now, for any $n > N$, we also have $n+1 > N$ and so $|a_{n+1} - L| < \varepsilon$. Therefore, $(a_{n+1})_{n\ge1}$ is convergent and $\lim\limits_{n\to\infty} a_n = \lim\limits_{n\to\infty} a_{n+1} = L$.

(b) [5pts: 1 for using induction and noting that the base case is valid, 2 each for the lower and upper bound in the induction step]
We proceed by induction on n. For $n = 1$, we have $2 < b = b_1 < 3$. Suppose that for $n = k$, we have $2 < b_k < 3$. Then, for $n = k + 1$, we obtain

$$b_{k+1} - 2 = b_k^2 - 4b_k + 4 = (b_k - 2)^2 > 0,$$

as $b_k > 2$. Hence, $b_{k+1} > 2$. Similarly,

$$3 - b_{k+1} = 3 - (b_k^2 - 4b_k + 6) = -b_k^2 + 4b_k - 3 = (3 - b_k)(b_k - 1) > 0,$$

as $3 > b_k > 2$. Hence, $b_{k+1} < 3$.

(c) [4pts: 2 for the plan and 2 for the details]
For all natural numbers n, we have

$$b_{n+1} - b_n = b_n^2 - 4b_n + 6 - b_n = b_n^2 - 5b_n + 6 = (b_n - 2)(b_n - 3).$$

From part (b), we have $b_n - 2 > 0$ and $b_n - 3 < 0$, hence $b_{n+1} - b_n < 0$ and $(b_n)_{n\ge1}$ is a decreasing sequence.

(d) [7pts: see breakdown in square brackets]
Parts (b) and (c) show that (b_n) is a bounded, monotone sequence. By Theorem 9.26, its limit $\lim\limits_{n\to\infty} b_n = B$ exists. [2] By part (a), $\lim\limits_{n\to\infty} b_{n+1} = B$ as well. [1] Hence

$$B = \lim_{n\to\infty} b_{n+1} = \lim_{n\to\infty} b_n^2 - 4b_n + 6 = B^2 - 4B + 6, \quad [2]$$

where we applied the results about the algebra of limits. The above quadratic equation has solutions $B = 2$ and $B = 3$. [1]

However, since $(b_n)_{n\ge1}$ is a decreasing sequence, we have $b_n \le b_{n-1} \le \cdots \le b_1 = b < 3$ for all natural numbers n. So $B = \lim\limits_{n\to\infty} b_n \le b < 3$. Hence $B = 2$. [1]

(e) [4pts: 1 for each of max/sup/inf/min] $\max S = \sup S = b_1 = b$, $\inf S = B = 2$, and $\min S$ does not exist because $2 < b_n$ for all $n \in \mathbb{N}$ and, therefore, $\inf S = 2 \notin S$.

Notes: A mark of 10/25 is equivalent to a bare pass; a mark of 17/25 is a First. As an exam setter, I am asked to ensure that there are at least 10 relatively easy marks available: here I would claim that (a) and (e) are certainly in this category, and at least some of the marks in (b). On the other hand, some parts of each question are supposed to be hard, and here I would nominate (d). In an ideal world, most marks would fall between 10 and (say) 20: in practice, the range on any one question is always wider than this.

There is an alternative approach to the question, pointed out to me by a class teacher based on some student answers. Set $c_n = b_n - 2$, and show that $c_{n+1} = c_n^2$. Then show by induction that $c_n = (c_1)^{2^{n-1}}$ for every $n \in \mathbb{N}$. Therefore $b_n = 2 + (b_1 - 2)^{2^{n-1}}$ for each n. From this exact formula, one may read off all the required results. Neat!

10

Analysis: Continuity

A function $f:\mathbb{R}\to\mathbb{R}$ is a rule of correspondence that assigns to each real number a unique real number. The functions we are most familiar with are actually unusually well-behaved, and most functions are impossible to describe fully, let alone to work with. Many bizarre functions make their appearance in analysis, and in order to avoid falling into pitfalls with simplistic thinking based on our experience with "nice" functions, we need our definitions and the hypotheses (assumptions) of theorems to be stated carefully and clearly.

Within the huge collection of functions, there is an important subset: the continuous functions. Continuous functions play a prominent role in analysis since they include all the most familiar and useful functions, and because they share many useful properties.

In this section we give the formal definition of a continuous function and prove two of the most important properties of continuous functions: the Extreme Value theorem and the Intermediate Value theorem.

10.1 Definition of continuity

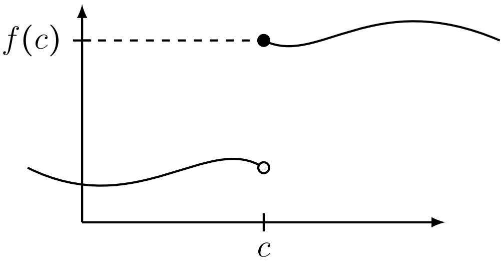


Figure 10.1: A function with a break at c. If x lies to the left of c, then $f(x)$ is not close to $f(c)$, no matter how close x comes to c.

In everyday speech, a 'continuous' process is one that proceeds without gaps of interruptions or sudden changes. What does it mean for a function $f:\mathbb{R}\to\mathbb{R}$ to be continuous? The common informal definition of this concept states that a function f is continuous if one can sketch its graph without lifting the pencil. In other words, the graph of f has no breaks in it. If a break does occur in the graph, then this break will occur at some point. Thus (based on this visual view of continuity), we first give the formal definition of the continuity of a function *at a point*. Next, if a function is continuous at *each* point, then it will be called continuous.

If a function has a break at a point, say c, then even if points x are close to c, the points $f(x)$ might not get close to $f(c)$, as illustrated in Figure 10.1.

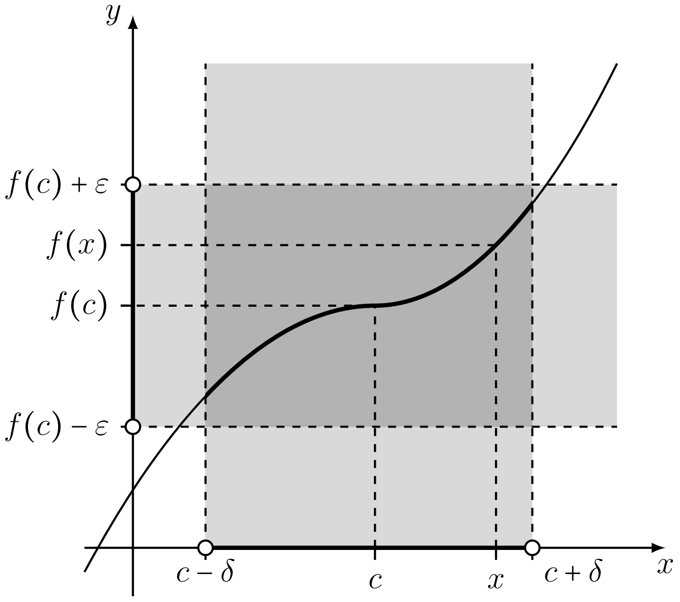


Figure 10.2: The definition of continuity of a function at point c. If the function is continuous at c, then given any $\varepsilon > 0$ (which determines a strip around the line $y = f(c)$ of width 2ε), there exists a $\delta > 0$ (which determines an interval of width 2δ around the point c) such that whenever x lies in this interval (so that x satisfies $c-\delta < x < c+\delta$, that is, $|x-c| < \delta$), then $f(x)$ satisfies $f(c)-\varepsilon < f(x) < f(c)+\varepsilon$, that is, $|f(x)-f(c)| < \varepsilon$.

This motivates the following definition of continuity, which guarantees that if a function is continuous at a point c, then we can make $f(x)$ as close as we like to $f(c)$, by choosing x sufficiently close to c. This is illustrated in Figure 10.2.

Definition 10.1.

1. Let I be an interval in $\mathbb{R}$ and let $c \in I$. A function $f : I \to \mathbb{R}$ is *continuous at* c if for every $\varepsilon > 0$, there exists a $\delta > 0$ such that for all $x \in I$ satisfying $|x-c| < \delta$, $|f(x)-f(c)| < \varepsilon$.
2. If f is not continuous at c, we say that f is *discontinuous at* c.
3. A function $f : I \to \mathbb{R}$ is *continuous on* I (or just *continuous* if I is clear from the context) if for every $c \in I$, f is continuous at c.
4. If f is not continuous on I, we say that f is *discontinuous on* I (or just *discontinuous* if I is clear from the context).

These definitions are (even) a bit more complicated than the definition of convergence of a sequence you met in the last chapter. You'll see that you need to work with 'continuous at a point' in much the same way as 'convergence to a limit'; the proof that some function is 'continuous at a point c' is rather like the proof that a sequence is convergent to a limit.

The statement that a function is continuous on a whole interval I is, written out with quantifiers:

$$\forall c \in I\,,\ \forall \varepsilon > 0\,,\ \exists \delta > 0\,,\ \forall x \in I \text{ such that } |x-c| < \delta \text{ we have } |f(x)-f(c)| < \varepsilon\,.$$

This is the most complicated statement you've seen so far. It is important to keep in mind what it is supposed to mean intuitively: name a point c, and a 'how close' ε, and then if x is 'close enough (δ)' to c, we're guaranteed that $f(x)$ is close to $f(c)$. This will help you remember what order the quantifiers above come in. It matters. You can (as you can guess from the sentence above) swap the first two 'for all' quantifiers without changing anything, but it is very important that *first* you name c and ε, *then* you decide on how small δ has to be, and only *after that* comes a second point x. In particular, the formula you write for δ *cannot* depend on x (it can, and usually will, depend on c and ε).

Let's see an example. As with convergence, I'll write it out in the formal style in order that this issue of 'what does δ depend on?' is easy to keep clear.

Example 10.2. Show that the function $f:\mathbb{R}\to\mathbb{R}$ given by $f(x)=x$ for all $x\in\mathbb{R}$ is continuous.

Proof. Given $c\in\mathbb{R}$ and $\varepsilon>0$, we choose $\delta=\varepsilon$.

Now given $x\in\mathbb{R}$ such that $|x-c|<\delta$, we want to show $|f(x)-f(c)|<\varepsilon$. We have

$$|f(x)-f(c)|=|x-c|<\delta=\varepsilon\,.$$

This is what we need for the definition of 'f is continuous at c', and since we proved it for an arbitrary $c\in\mathbb{R}$, we conclude that f is continuous at c for all $c\in\mathbb{R}$, i.e. f is continuous on $\mathbb{R}$. □

As usual, we do not know what we should choose δ to be when we write the line 'we choose $\delta=\ldots$', we leave it blank at first and fill it in later once we see what works.

Example 10.3. Show that the function $f:\mathbb{R}\to\mathbb{R}$ given by $f(x)=2x+1$ for all $x\in\mathbb{R}$ is continuous.

Proof. Given $c\in\mathbb{R}$ and $\varepsilon>0$, we choose $\delta=\frac{1}{2}\varepsilon$.

Now given $x\in\mathbb{R}$ such that $|x-c|<\delta$, we have:

$$|f(x)-f(c)|=|(2x+1)-(2c+1)|=2|x-c|<2\delta=\varepsilon\,.$$

Again, this is what we need for the definition of 'f is continuous at c', and since we proved it for an arbitrary $c\in\mathbb{R}$, we conclude that f is continuous on $\mathbb{R}$. □

Example 10.4. Show that the function $f:\mathbb{R}\to\mathbb{R}$ given by $f(x)=1$ for all $x\in\mathbb{R}$ is continuous.

Proof. Let $c\in\mathbb{R}=(-\infty,\infty)$. We have to prove that f is continuous at c. Let $\varepsilon>0$ be given. In this case, any positive choice of δ will work; for instance, let $\delta=1$. Then if $x\in\mathbb{R}$ and $|x-c|<\delta=1$, we have:

$$|f(x)-f(c)|=|1-1|=|0|=0<\varepsilon.$$

So f is continuous at c. Since the choice of $c\in\mathbb{R}$ was arbitrary, it follows that f is continuous on $\mathbb{R}$. □

Example 10.5. Show that the function $f:\mathbb{R}\to\mathbb{R}$ given by

$$f(x)=\begin{cases}0 & \text{if } x=0,\\ 1 & \text{if } x\in\mathbb{R}\setminus\{0\},\end{cases}$$

is discontinuous at 0 and continuous at all $c\in\mathbb{R}\setminus\{0\}$.

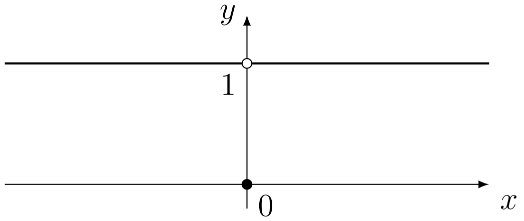


Figure 10.3: A function continuous everywhere except at 0.

Proof. Suppose that f is continuous at 0. Then for any given $\varepsilon>0$ there exists a $\delta>0$ such that whenever $|x-0|<\delta$, $|f(x)-f(0)|<\varepsilon$.

We just need to find one example of $\varepsilon>0$ for which the above statement fails (one counterexample to the 'for all'). One example that will work is $\varepsilon=\frac{1}{2}$.

To show $\varepsilon=\frac{1}{2}$ is a counterexample, we need to show there does not exist $\delta>0$ such that whenever $|x-0|<\delta$, $|f(x)-f(0)|<\frac{1}{2}$.

So let $\delta>0$ be given; we need to show 'whenever $|x-0|<\delta$, $|f(x)-f(0)|<\frac{1}{2}$' is false. In other words, we need to find one counterexample x, i.e. x with $|x|<\delta$ such that $f(x)$ is not within $\frac{1}{2}$ of $f(0)$. We can take $x=\frac{\delta}{2}$. To see that this choice of x is a counterexample, we need to observe that indeed $|x|<\delta$, and furthermore

$$\big|f(x)-f(0)\big|=|1-0|=1$$

which is not smaller than $\frac{1}{2}$.

So f is not continuous at 0.

Next we show that for all $c\in\mathbb{R}\setminus\{0\}$, f is continuous at c. Let $\varepsilon>0$ be given. Take $\delta=\frac{|c|}{2}>0$. Then if $x\in\mathbb{R}$ and $|x-c|<\delta$, we have

$$|c|-|x|\le\big||c|-|x|\big|\le|c-x|=|x-c|<\delta=\frac{|c|}{2}$$

and so

$$|x|>\frac{|c|}{2}>0.$$

Thus $x\neq0$ and so $f(x)=1$. Hence if $x\in\mathbb{R}$ and $|x-c|<\delta$, we obtain

$$|f(x)-f(c)|=|1-1|=|0|=0<\varepsilon.$$

Consequently f is continuous at c. □

In the above, note that the proof of continuity follows the same pattern as the previous examples. It's easy to get the proof of *discontinuity* at 0 wrong. If you are not sure what to do, write out the statement of 'f is continuous at 0' clearly, with all the quantifiers, and then negate it (i.e. follow the rules from Chapter 3), and check that the negation is a true statement. This is what we did above. If you are happy with this logic, then you can afford to shorten it:

'To prove f is not continuous at 0, pick $\varepsilon=\frac{1}{2}$. Given $\delta>0$, pick $x=\frac{\delta}{2}$. Then $|x|<\delta$, but $|f(x)-f(0)|=1>\varepsilon$.'

Example 10.6. Show that the function $f:(0,\infty)\to\mathbb{R}$ given by $f(x)=\frac{1}{x}$ for all $x\in\mathbb{R}$ is continuous.

Proof. Let $c\in(0,\infty)$. Given $\varepsilon>0$, let $\delta=\min\left\{\frac{c}{2},\frac{\varepsilon c^2}{2}\right\}$ (which is positive). Then if $x\in(0,\infty)$ and $|x-c|<\delta$, we have

$$c-x\leq|c-x|<\delta\leq\frac{c}{2},\text{ and so }x>\frac{c}{2}>0.$$

Consequently, if $x\in(0,\infty)$ and $|x-c|<\delta$,

$$\left|\frac{1}{x}-\frac{1}{c}\right|=\frac{|c-x|}{x\,c}=|x-c|\cdot\frac{1}{x}\cdot\frac{1}{c}<\delta\cdot\frac{2}{c}\cdot\frac{1}{c}=\frac{2\delta}{c^2}\leq\varepsilon.$$

So f is continuous at c. Since the choice of $c\in(0,\infty)$ was arbitrary, it follows that f is continuous on $(0,\infty)$. □

It's very easy in this last proof to make a mistake, *especially* if you write it informally 'let $\delta>0$ be chosen later' and only at the last line put in a value for δ. Much as in Warning 9.14, it is very tempting to write 'let $\delta=\varepsilon xc$', since that would make the algebra work: we have

$$|f(x)-f(c)|=\tfrac{|x-c|}{xc}<\tfrac{\delta}{xc}\,.$$

But this 'choice' of δ doesn't make sense: it depends on x, and (at the point where we choose it in the formal proof above) there *is no* x around. What we need is to give some real number for δ which guarantees that $\frac{\delta}{xc}$ will be at most ε *whatever* x gets chosen such that $|x-c|<\delta$. That would be difficult if x were very tiny (because then $\frac{1}{x}$ is huge) and this is why we choose δ small enough that we can write $x\geq\frac{c}{2}$, to rule out it being very close to 0.

10.2 Continuous functions preserve convergent sequences

We now give an alternative characterisation of continuity. You should have recognised that the proof that f is continuous at some given point c resembles rather closely the proof that a sequence converges to a given limit. The reason is that something rather similar is going on: and it turns out to be useful to recognise this fact formally.

Theorem 10.7. *Let I be an interval in $\mathbb{R}$ and let $c\in I$. Suppose that $f:I\to\mathbb{R}$ is a function. Then f is continuous at c if and only if*

$$\boxed{\begin{gathered}\textit{for every convergent sequence } (x_n)_{n\in\mathbb{N}} \textit{ contained in } I \textit{ with limit } c,\\ (f(x_n))_{n\in\mathbb{N}} \textit{ is convergent and } \lim_{n\to\infty}f(x_n)=f(c).\end{gathered}}\tag{10.1}$$

Proof. **"Only if" ($\Longrightarrow$) direction:** Assume that f is continuous at $c\in I$ and let $(x_n)_{n\in\mathbb{N}}$ be a convergent sequence contained in I with limit c. We have to show that $(f(x_n))_{n\in\mathbb{N}}$ converges to $f(c)$.

Let $\varepsilon>0$ be given.

Since f is continuous at $c\in I$, for the given $\varepsilon>0$, there exists $\delta>0$ such that for all $x\in I$ satisfying $|x-c|<\delta$ we have $\big|f(x)-f(c)\big|<\varepsilon$. Now since $(x_n)_{n\in\mathbb{N}}$ is convergent with limit c, by the definition of convergence there exists $N\in\mathbb{N}$ such that for all $n>N$ we have $|x_n-c|<\delta$. This is the N we will use to verify the definition of $\lim\limits_{n\to\infty}f(x_n)=f(c)$.

Suppose $n>N$. Then by choice of N we have $|x_n-c|<\delta$. Since $x_n\in I$ (because $(x_n)_{n\in\mathbb{N}}$ is assumed to be contained in I), by choice of δ that means we have $\big|f(x_n)-f(c)\big|<\varepsilon$, which is what we wanted to show.

"If" ($\Longleftarrow$) direction: Suppose that (10.1) holds. We have to show that f is continuous at c. We prove this by contradiction. Assume that f is not continuous at c, that is,

$$\neg\left[\forall\varepsilon > 0\ \exists\delta > 0 \text{ such that } \forall x \in I \text{ such that } |x-c| < \delta, |f(x)-f(c)| < \varepsilon,\right]$$

or equivalently,

$$\exists\varepsilon > 0 \text{ such that } \forall\delta > 0\ \exists x \in I \text{ such that } |x-c| < \delta \text{ but } |f(x)-f(c)| \geq \varepsilon\,.$$

So let $\varepsilon > 0$ be our counterexample to continuity of f at c, i.e. ε is such that

$$\forall\delta > 0\ \exists x \in I \text{ such that } |x-c| < \delta \text{ but } |f(x)-f(c)| \geq \varepsilon \tag{10.2}$$

is a true statement.

For each $n \in \mathbb{N}$, we want to choose a number x_n. We do this as follows. First, choose $\delta = \frac{1}{n}$. Since this is a positive number, by (10.2) there exists $x \in I$ such that $|x-c| < \delta = \frac{1}{n}$ and $|f(x)-f(c)| \geq \varepsilon$. We let x_n be any such x. That is, we choose x_n such that $|x_n - c| < \frac{1}{n}$ and $|f(x_n)-f(c)| \geq \varepsilon$.

This gives us a sequence $(x_n)_{n\in\mathbb{N}}$.

Claim 1: The sequence $(x_n)_{n\in\mathbb{N}}$ is contained in I and is convergent with limit c.

Indeed, we have for all $n \in \mathbb{N}$, $x_n \in I$. Furthermore, given any $\zeta > 0$, we can find $N \in \mathbb{N}$ such that $\frac{1}{\zeta} < N$ (Archimedean property), that is, $\frac{1}{N} < \zeta$. Hence for $n > N$, we have $|x_n - c| < \frac{1}{N} < \zeta$. So $(x_n)_{n\in\mathbb{N}}$ is convergent with limit c.

Claim 2: The sequence $(f(x_n))_{n\in\mathbb{N}}$ does not converge to $f(c)$.

Recall that $\lim\limits_{n\to\infty} f(x_n) = f(c)$ means (by definition):

$$\forall\zeta > 0\,,\ \exists N \in \mathbb{N}\,,\ \forall n \in \mathbb{N} \text{ with } n > N \text{ we have } \big|f(x_n) - f(c)\big| < \zeta\,.$$

We now show $\zeta = \frac{\varepsilon}{2}$ is a counterexample to this statement. That is, for any $N \in \mathbb{N}$,

$$\forall n \in \mathbb{N} \text{ with } n > N \text{ we have } \big|f(x_n) - f(c)\big| < \zeta$$

is false. It's enough to find one counterexample n. We choose $n = N+1$, which is an integer bigger than N.

Recall that we constructed x_n (for this particular n) such that $\big|f(x_n)-f(c)\big| \geq \varepsilon$. Since $\varepsilon > \zeta$, in particular $\big|f(x_n)-f(c)\big| < \zeta$ is false, which proves Claim 2.

Claims 1 and 2 show that (10.1) does not hold, a contradiction. Hence f is continuous at c. □

It's worth noticing that our choice $\delta = \frac{1}{n}$ is just one of many choices that work. What's going on in the 'if' part of the proof is that we want to show that *if* f is not continuous at c, *then* there is a sequence of points $(x_n)_{n\in\mathbb{N}}$ which witnesses it—that is, the points x_n get arbitrarily close to x_n but the function values don't get close to c. We could have written $\delta = 2^{-n}$, or $\delta = \frac{1}{\log(1+n)}$, equally well—we just need that if n is large then x_n is guaranteed to be close to c.

Activity 10.1. *Consider the function $f : [0,\infty] \to \mathbb{R}$ defined by*

$$f(x) = \begin{cases} 0 & \text{if } x = 0 \\ \sin\frac{1}{x} & \text{if } x \neq 0 \end{cases}\,.$$

Show that the sequence $\left(\frac{1}{\pi n}\right)_{n\in\mathbb{N}}$ converges to 0 *and that $\lim\limits_{n\to\infty} f\left(\frac{1}{\pi n}\right) = f(0)$. Is f continuous at* 0*?*

The point of Theorem 10.7 is that it lets us 'translate' the Algebra of Limits to show that doing algebraic operations with continuous functions gives us continuous functions; this is Theorem 10.9 below. As with the Algebra of Limits, it is painful to prove from the definition that a given function is continuous, and we would like tools that tell us that many of the functions we want to study are indeed continuous.

Before stating it, we introduce some convenient notation.

Definition 10.8. Let I be an interval in $\mathbb{R}$. Given functions $f : I \to \mathbb{R}$ and $g : I \to \mathbb{R}$, we define the following:

1. If $\alpha \in \mathbb{R}$, then we define the function $\alpha f : I \to \mathbb{R}$ by $(\alpha f)(x) = \alpha \cdot f(x)$, $x \in I$.
2. We define the *absolute value of* f to be the function $|f| : I \to \mathbb{R}$ given by $|f|(x) = |f(x)|$, $x \in I$.
3. The *sum of* f *and* g is the function $f + g : I \to \mathbb{R}$ defined by $(f+g)(x) = f(x) + g(x)$, $x \in I$.
4. The *product*[1] *of* f *and* g is the function $fg : I \to \mathbb{R}$ defined by $(fg)(x) = f(x)g(x)$, $x \in I$.
5. If $k \in \mathbb{N}$, then we define the k^{th} *power of* f, to be the function $f^k : I \to \mathbb{R}$ given by $f^k(x) = (f(x))^k$, $x \in I$.
6. If for all $x \in I$, $g(x) \neq 0$, then we define the function $\frac{1}{g} : I \to \mathbb{R}$ by $\left(\frac{1}{g}\right)(x) = \frac{1}{g(x)}$, $x \in I$.

Theorem 10.9 (Algebra of Continuous Functions)**.** *Let I be an interval in $\mathbb{R}$ and let $c \in I$. Suppose that $f : I \to \mathbb{R}$ and $g : I \to \mathbb{R}$ are continuous at c. Then:*

(a) For all $\alpha \in \mathbb{R}$, αf is continuous at c.

(b) $|f|$ is continuous at c.

(c) $f + g$ is continuous at c.

(d) fg is continuous at c.

(e) For all $k \in \mathbb{N}$, f^k is continuous at c.

(f) If for all $x \in I$, $g(x) \neq 0$, then $\frac{1}{g}$ is continuous at c.

Proof. Suppose that $(x_n)_{n\in\mathbb{N}}$ is a convergent sequence contained in I, with limit c. Since f and g are continuous at c, from Theorem 10.7, it follows that $(f(x_n))_{n\in\mathbb{N}}$ and $(g(x_n))_{n\in\mathbb{N}}$ are convergent with limits $f(c)$ and $g(c)$, respectively. Each one of the statements now follows easily from Theorem 9.31 and a second application of Theorem 10.7. For example, consider statement (d) (the other cases may be proved as exercises).

By Theorem 9.31, $(f(x_n)g(x_n))_{n\in\mathbb{N}}$ is convergent with limit $f(c)g(c)$, that is, $((fg)(x_n))_{n\in\mathbb{N}}$ is convergent with limit $(fg)(c)$. Since $(x_n)_{n\in\mathbb{N}}$ is arbitrary, this proves (10.1) for fg.

Thus by Theorem 10.7, fg is continuous at c. □

Example 10.10. Every polynomial function (that is, every function $p : \mathbb{R} \to \mathbb{R}$ defined by $p(x) = a_0 + a_1 x + \cdots + a_k x^k$, where $k \in \mathbb{N}$ and $a_0, \ldots, a_k \in \mathbb{R}$) is continuous.

[1] Remember back when we defined function composition I mentioned some books write fg for composition and this can confuse with product. Well, please try to not be confused by fg now being used for the product: it is *not* composition!

Proof. Since $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x$ for $x \in \mathbb{R}$ is continuous (see Example 10.2), it follows that for all $k \in \mathbb{N}$, the function $x \to x^k$ is continuous by Theorem 10.9(e). Thus given any scalars $a_0, a_1, \dots, a_k$ in $\mathbb{R}$, it follows that the functions $a_0 \cdot 1, a_1 \cdot x, \dots, a_k \cdot x^k$ are continuous by Theorem 10.9(a). Summing these up, using Theorem 10.9(c) k times, we see

$$p(x) = a_0 + a_1 x + \dots + a_k x^k, \quad x \in \mathbb{R}$$

is continuous. □

10.3 Restrictions and compositions of functions

Definition 10.11. If $f : I \to \mathbb{R}$ is a function on an interval I, and J is an interval contained in I (that is, $J \subseteq I$), then the *restriction of f to J*, is the function $f\big|_J : J \to \mathbb{R}$ defined by

$$f\big|_J(x) = f(x), \quad x \in \mathbb{R}.$$

The following theorem implies (completely as expected) that the restriction of a continuous function is continuous.

Theorem 10.12. *Let I and J be intervals such that $J \subseteq I$ and let $c \in J$. If f is continuous at c, then $f\big|_J$ is continuous at c.*

This is an exercise.

The converse of the above theorem is not true unless J is an open interval (this is part of the same exercise).

Recall from Section 5.2.3 that normally we only define the composition $g \circ f$ of two functions f and g if the codomain of f is equal to the domain of g. In Analysis, it is convenient to 'cheat' a bit: we will still talk about $g \circ f$ when the codomain of f is $\mathbb{R}$ and the domain of g is only some interval $I \subseteq \mathbb{R}$. However, be careful: for this to make sense, we need to be sure that the *range* of f is contained in I.

That is, we say: if $f : I \to \mathbb{R}$ and $g : J \to \mathbb{R}$ are functions such that for all $x \in I$, $f(x) \in J$, then we write $g \circ f : I \to \mathbb{R}$ for the function defined by

$$(g \circ f)(x) = g\big(f(x)\big).$$

The following theorem implies that the composition of continuous functions is continuous.

Theorem 10.13. *If $f : I \to \mathbb{R}$ is continuous at $c \in I$ and $g : J \to \mathbb{R}$ is continuous at $f(c)$ (with $f(x) \in J$ for all $x \in I$), then $g \circ f$ is continuous at c.*

Proof. Take $\varepsilon > 0$. Then, as g is continuous at $f(c)$, there is some $\eta > 0$ such that $y \in J$ and $|y - f(c)| < \eta$ imply that $|g(y) - g(f(c))| < \varepsilon$. As also f is continuous at c, there exists $\delta > 0$ such that $x \in I$ and $|x - c| < \delta$ imply $|f(x) - f(c)| < \eta$.

Now we assemble what we know. Suppose that $x \in I$ and $|x - c| < \delta$. Then $f(x) \in J$ and $|f(x) - f(c)| < \eta$, from which we deduce that $|g(f(x)) - g(f(c))| < \varepsilon$, i.e., $|(g \circ f)(x) - (g \circ f)(c)| < \varepsilon$. We conclude that $g \circ f$ is continuous at c. □

Example 10.14. Show that the function $f : (1, \infty) \to \mathbb{R}$ defined by

$$f(x) = \sqrt{\frac{x^2 - 1}{x^2 + 1}}, \quad x > 1,$$

is continuous on $(1, \infty)$.

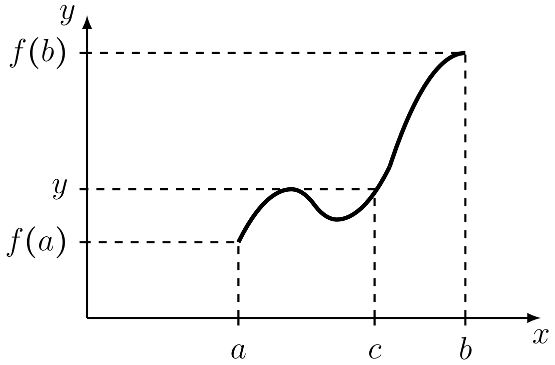
Proof. Let $g:(0,\infty)\to\mathbb{R}$ be defined by $g(x)=\sqrt{x}$. In an exercise you will prove that g is continuous. Let $h:\mathbb{R}\to(0,\infty)$ be defined by

$$h(x)=\frac{x^2-1}{x^2+1},\quad x\in\mathbb{R}.$$

We have already seen that all polynomial functions are continuous. Therefore, $p_1,p_2:\mathbb{R}\to\mathbb{R}$ defined by $p_1(x)=x^2-1$ and $p_2(x)=x^2+1$ are continuous. Since $p_2(x)\neq 0$ for all $x\in\mathbb{R}$, it follows by Theorem 10.9((f)) that $\frac{1}{p_2}$ is continuous. Then by Theorem 10.9((d)), $p_1\cdot\frac{1}{p_2}=h$ is continuous. Note that the restriction of h to $(1,\infty)$, $h|_{(1,\infty)}$ assumes only positive values: if $x\in(1,\infty)$ then $x>1$, therefore $x^2-1>0$, and since $x^2+1>0$ anyway, $h(x)>0$. This shows that the composition $g\circ h|_{(1,\infty)}=f$ is properly defined. By Theorem 10.12, $h|_{(1,\infty)}$ is continuous. Finally, by Theorem 10.13, $g\circ h|_{(1,\infty)}=f$ is continuous at each $c>1$, and therefore, continuous. □

10.4 Intermediate Value theorem

We now prove one of the most fundamental (and obvious!) theorems on continuous functions: a continuous function cannot "hop over" intermediate values. For instance, if the top of a mountain is 1976 meters above sea level and the foot of the mountain is 341 meters above sea level, then given any number between 341 and 1976, say 1001, there must exist a point on the mountain that is exactly 1001 meters above sea level.



The Intermediate Value theorem was first proved by Bernhard Bolzano in 1817.

Theorem 10.15. (Intermediate Value theorem). *If $f:[a,b]\to\mathbb{R}$ is continuous and y is such that $f(a)\le y\le f(b)$ or $f(b)\le y\le f(a)$, then there exists $c\in[a,b]$ such that $f(c)=y$.*

The theorem statement says 'if $f(a)\le y\le f(b)$ or $f(b)\le y\le f(a)$'. This is two separate (almost—unless $f(a)=f(b)$) cases. It's easy to prove the theorem if either $f(a)=y$ or $f(b)=y$, because we just take $c=a$ or $c=b$ respectively. So let's suppose that y is not equal to $f(a)$ or $f(b)$, but rather strictly in between them. And let's look at the first case, $f(a)<f(b)$, which is the picture above.

As we can see from the above picture, it might be the case that $f(x)=y$ occurs at several points; in the figure, it occurs twice (once at c, and once earlier at what looks like a local maximum of f). We would like to avoid confusing the different possibilities, so we pick out some special c; maybe the easiest is to pick the biggest. That is, we want to prove there exists $c\in[a,b]$ such that $f(c)=y$, *and* $f(x)>c$ for all $c<x\le b$. Intuitively, the c we want should just be the biggest element of $\{x:f(x)\le y\}$; what we need to do is prove that that exists and works.

The 'idea'—the reason that continuity comes in to the proof—is the following. We know f is continuous at c. That is, if x is close to c then $f(x)$ is close to $f(c)$.

If $f(c)$ is smaller than y, then so is $f(x)$ for all x close to c. In particular, if we look at x just a little bit bigger than c, then $f(x)$ will be smaller than y—but then x should be in S, so c isn't an upper bound for S, a contradiction.

If $f(c)$ is bigger than y, then so is $f(x)$ for all x close to c. In particular, if we look at any x just a little bit smaller than c, then $f(x)$ is bigger than y—but then c isn't a *least* upper bound for S, again a contradiction.

We saw an argument like this before, in the proof of Example 8.9. This is really the same argument as there, just written out in general.

Let's now put in the formal details.

Proof. If $y = f(a)$ then $c = a$ satisfies the statement of the theorem. Similarly if $y = f(b)$ then $c = b$ satisfies the statement of the theorem. So suppose y is not equal to $f(a)$ or $f(b)$.
Case 1: Suppose that $f(a) < y < f(b)$.

Let $S = \{x \in [a,b] \mid f(x) \le y\}$. We want to prove that

1. $\sup S$ exists, and

2. if we set $c = \sup S$, then $c \in [a,b]$ and $f(c) = y$.

Since $f(a) \le y$, it follows that $a \in S$, so $S \ne \emptyset$. And S is clearly bounded above by b. Therefore, by the least upper bound property of the reals, $\sup S$ exists.

Write $c = \sup S$. Since $a \in S$, by definition $a \le c$. Since b is an upper bound of S, $c \le b$. Therefore, $c \in [a,b]$, and it remains to prove that $f(c) = y$.

Suppose for a contradiction that $f(c) \ne y$, and let

$$\varepsilon = \frac{|f(c) - y|}{2},$$

which is positive. Since $c \in [a,b]$, so f is continuous at c. That means that there exists $\delta > 0$ such that

$$\big|f(x) - f(c)\big| < \frac{|f(c) - y|}{2} \quad \text{for all} \quad x \in [a,b] \text{ such that } |x - c| < \delta\,. \tag{10.3}$$

Fix $\delta > 0$ such that (10.3) holds.

If $f(c) < y$: In this case, we have $c < b$ since $f(b) > y$. Now observe that either $c + \frac{\delta}{2} \le b$, or $|b - c| < \delta$ (or both). In particular, there is an $x > c$ such that $x \in [a,b]$ and $|x - c| < \delta$; fix any such x. Now by (10.3), we have

$$f(x) < f(c) + \frac{|f(c) - y|}{2} < y$$

and so by definition of S, we have $x \in S$, and we already know $x > c$. But c is assumed to be an upper bound of S, which is a contradiction.

If $f(c) > y$: In this case, we have $c > a$ since $f(a) < y$. As before, observe that either $c - \frac{\delta}{2} \ge a$, or $|a - c| < \delta$ (or both) and so there is a $z < c$ such that $z \in [a,b]$ and $|z - c| < \delta$; fix any such z. Now given any $x \in [z,c]$, we have $x \in [a,b]$ and $|x - c| < \delta$, so by (10.3) we have

$$f(x) > f(c) - \frac{|f(c) - y|}{2} > y\,,$$

and in particular x is not in S. That is, no element of $[z,c]$ is in S, and (because c is an upper bound of S) no element of (c,∞) is in S. Putting these together, no element of $[z,\infty)$ is in S, so z is an upper bound of S. But we know $z < c$, which contradicts our assumption that c is a least upper bound of S.

Assuming $f(c) \ne y$, we considered both possibilities, $f(c) < y$ and $f(c) > y$, and in either case got to a contradiction. So the only possibility is that $f(c) = y$, which is what we wanted.

Case 2: Suppose that $f(a) > y > f(b)$.

It would be easy to modify the above proof—just swap signs—to handle this case too. But it is neater (and less work!) to *reduce* this case to Case 1. By Theorem 10.9, since f is continuous, so is $(-f)$. Since $f(a) > y > f(b)$, so $(-f)(a) < -y < (-f)(b)$.

So by applying Case 1 to $-f$, there is some $c \in [a,b]$ such that $(-f)(c) = -y$, and this tells us $f(c) = y$, which is what we wanted. □

Example 10.16. Show that every polynomial of odd degree with real coefficients has at least one real root.

The *idea* here is simple. Suppose that our odd-degree polynomial is $p(x) = a_0 + a_1x + \cdots + a_kx^k$, where k is odd. We know a_k is not zero (that's what it means to say the degree is k). Dividing the whole polynomial by a_k doesn't change the roots, so let's assume $p(x) = a_0 + a_1x + \cdots + a_{k-1}x^{k-1} + x^k$.

When $|x|$ is very big, x^k will be much bigger than all the other terms; the graph of $p(x)$ and of x^k will look pretty similar. So when $|x|$ is very big and x is negative, we should find $p(x)$ is also negative. So there is some a such that $p(a) < 0$. Similarly, if $|x|$ is big and $x > 0$, then $p(x)$ will also be positive. So there is some b such that $p(b) > 0$. And then applying the Intermediate Value theorem on $[a, b]$, with $y = 0$, says that there is some $c \in [a, b]$ such that $p(c) = 0$, which is what we want.

Proof. Suppose that p is a polynomial with degree k, where k is an odd natural number. Then the coefficient of x^k in $p(x)$ is not zero. Since $p(x)/s$ has the same roots as $p(x)$ for any non-zero s, we can assume that the coefficient of x^k in $p(x)$ is 1. That is, we have

$$p(x) = a_0 + a_1x + \cdots + a_{k-1}x^{k-1} + x^k\,.$$

We want to first justify that there is some b such that $p(b) > 0$ (the algebra is a bit simpler than for a). We will actually choose b to be a positive integer. Observe that

$$\lim_{n\to\infty} \frac{p(n)}{n^k} = \lim_{n\to\infty} \tfrac{a_0}{n^k} + \tfrac{a_1}{n^{k-1}} + \cdots + \tfrac{a_{k-1}}{n} + 1 = 1$$

where the first equality is just writing out $p(n)$ and simplifying, and the second equality is by the Algebra of Limits.

Using the definition of $\lim_{n\to\infty} \frac{p(n)}{n^k} = 1$, with $\varepsilon = \frac{1}{2}$, there exists some N such that for all $n > N$ we have

$$\left|\frac{p(n)}{n^k} - 1\right| < \tfrac{1}{2} \qquad \text{and so} \qquad \frac{p(n)}{n^k} > \tfrac{1}{2}\,.$$

In particular, we can let $b = N + 1$ and obtain $p(b) > \frac{1}{2}b^k > 0$, which is what we wanted.

We do something similar for a (which will be a negative integer). We have

$$\lim_{n\to\infty} \frac{p(-n)}{(-n)^k} = \lim_{n\to\infty} \tfrac{a_0}{(-n)^k} + \tfrac{a_1}{(-n)^{k-1}} + \cdots + \tfrac{a_{k-1}}{-n} + 1 = 1$$

and again using the definition of the limit, with $\varepsilon = \frac{1}{2}$, there is N such that for all $n > N$ we have

$$\left|\frac{p(-n)}{(-n)^k} - 1\right| < \tfrac{1}{2} \qquad \text{and so} \qquad \frac{p(-n)}{(-n)^k} > \tfrac{1}{2}\,.$$

In particular, we can let $a = -N - 1$, and this gives $p(a) < \frac{1}{2}(-N - 1)^k = -\frac{1}{2}(N + 1)^k < 0$, which is what we wanted.

Now we apply the Intermediate Value theorem to $p(x)$, on the interval $[a, b]$, with $y = 0$. The function p is continuous by Example 10.10, and $f(a) < 0 = y < f(b)$, so the conditions of the Intermediate Value theorem are satisfied. We conclude there is some $c \in [a, b]$ such that $p(c) = 0$, which is what we wanted. □

It's worth noticing that a bit more is true. If we want to know where a polynomial (or any continuous function!) has roots, it's enough to find a point where the polynomial takes a value smaller than 0 and another close by where it takes a value bigger than 0. Then there has to be a root in between.

Example 10.17. The polynomial $p(x) = x^3 - x^{2014} + \frac{1}{399}$ has a real root in $[-1, 1]$.

Proof. $p(1) = \frac{1}{399} > 0$ and $p(-1) = -2 + \frac{1}{399} < 0$ and so by the Intermediate Value theorem $\exists c \in [-1, 1]$ such that $p(c) = 0$. □

Remark 10.18. You've no doubt already noticed doing MA100 that computers can be rather useful for solving 'methods' problems. Wouldn't it be nice if they could also help us prove things? Well, sadly we still do not know how to make a computer do all of the inventive clever stuff you need in order to prove interesting statements. But you can get the computer to do the algebra for you. And, courtesy of this observation about roots of functions, you can also get a computer to prove for you that a polynomial that shows up in your proof has a root smaller than 1 (which, we're imagining, will be useful to you..!). Or to show that a 50 by 50 matrix is *positive definite*, i.e. all its eigenvalues are positive (why should you care? well, because it is a useful thing to know about a matrix). In short, you can get a computer to do a lot of numerical work for you, give you an answer which is some funny decimal, and *prove* that this decimal is correct up to ten (or a hundred, if you want) places. Quite a lot of modern proofs in mathematics have parts which are numerical work done by a computer, but which the computer can prove is correct.

Why should you care about being able to prove a computer's numerical work is correct? Here's an example: evaluate $e^{\pi\sqrt{163}}$. With a calculator, you can check it is equal to the integer $640\,323^3 + 744$. Try again, with a computer, to check it's true to five or so decimal places, and you should be convinced.

In fact, this number is not an integer; it's off by about 10^{-11} from an integer. This number is about 10^{17}, so the percentage away from an integer is about $10^{-26}\%$. It's rather amazing that such a simple expression can be so incredibly close to an integer without actually being an integer.

But it would be rather embarrassing if you thought it was an integer and assumed that in a proof!

Example 10.19. Show that at any given time, there exists a pair of diametrically opposite points on the equator which have the same temperature.

Proof. Let $T(\Theta)$ denote the surface temperature at the point at longitude Θ. See Figure 10.4. (Note that $\Theta(0) = \Theta(2\pi)$.) Assuming that T is a continuous function of Θ, it follows that the function $f : [0, \pi] \to \mathbb{R}$ defined by $f(\Theta) = T(\Theta) - T(\Theta + \pi)$ is continuous as well. If $f(0) = 0$, then it follows that the temperatures at 0 and 180° longitude are the same. If $f(0) \neq 0$, then since $f(0)$ and $f(\pi) = -f(0)$ have opposite signs, by the Intermediate Value theorem, it follows that f must vanish at some point, and so the claim follows. □

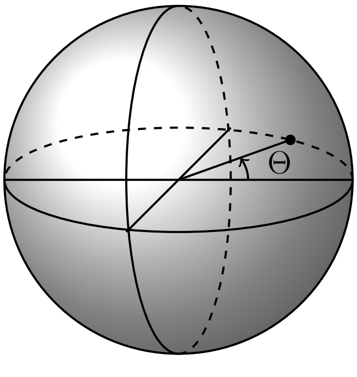


Figure 10.4: The point on the equator with longitude Θ.

10.5 Extreme Value theorem

We've seen that functions in general can do all kinds of unpleasant things, jumping around all over the place and so on. Continuous functions don't behave this badly, but we've still seen continuous functions which go off to infinity, such as $f : (0,1) \to \mathbb{R}$ defined by $f(x) = \frac{1}{x}$; this gets very big as x gets close to 0.

There are also continuous functions which do some rather strange things, such as the continuous function $g : \mathbb{R} \to \mathbb{R}$ defined by

$$g(x) = \begin{cases} 0 & \text{if } x = 0 \\ x \sin \frac{1}{x} & \text{if } x \neq 0 \end{cases} ,$$

which has infinitely many local maxima and minima, even if you only look at the interval $[-1,1]$ (see Figure 10.5).

Another 'funny function' is $h : (0,\infty) \to \mathbb{R}$ defined by

$$h(x) = (1-x) \sin \tfrac{1}{x} ,$$

which also has infinitely many local maxima (as x gets closer to 0), where the function values get closer and closer to 1, yet no global maximum exists. This function is also continuous—but notice that it is not defined at 0, and in fact if we try to change the function to one defined on $[0,\infty)$ (i.e. we give the function a value at 0) then it will not be continuous at 0.

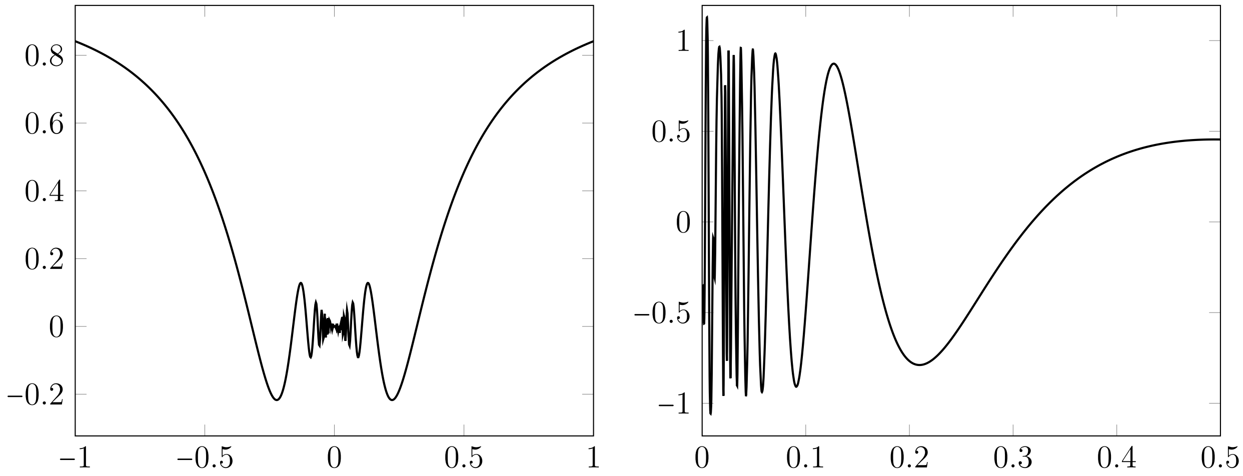


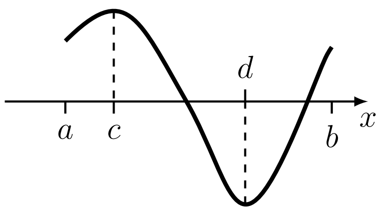
Figure 10.5: The functions $g(x)$ and $h(x)$.

Activity 10.2. *Prove that $g(x)$ as defined above is continuous on $\mathbb{R}$ (you should assume the sine function is continuous).*

Prove that there is no continuous function $h^* : [0,\infty) \to \mathbb{R}$ such that $h^*(x) = h(x)$ for all $x \in (0,\infty)$.

You might well imagine that there are continuous functions on closed intervals which have some similar nasty behaviour: maybe they go off to infinity somewhere in the middle of the interval, or they have infinitely many local maxima which (like $h(x)$ above) keep getting bigger and bigger so that even if the function stays bounded, there is no global maximum?

In fact, surprisingly, this is not the case. Any continuous function f on any closed interval is bounded, and it has at least one global maximum and minimum (the extreme values).



In this figure the extreme value are both attained once each, at c and d. For a function like $x \to \cos x$, on the interval $[0, 1000]$, there are many global maxima (and minima!)—0, 2π, 4π and so on are all global maxima. There can even be infinitely many global maxima. A trivial example is a constant function on I: every point is a global maximum.

Activity 10.3. *Find a function $f : [0,1] \to \mathbb{R}$ which is continuous, not constant, and has infinitely many global maxima.*

Theorem 10.20 (Extreme Value theorem)**.** *Let $[a,b]$ be any closed and bounded interval and let $f : [a,b] \to \mathbb{R}$ be a continuous function. Then there exists $c \in [a,b]$ such that*

$$f(c) = \sup\{f(x) \mid x \in [a,b]\}, \tag{10.4}$$

and there exists $d \in [a,b]$ such that

$$f(d) = \inf\{f(x) \mid x \in [a,b]\}. \tag{10.5}$$

Since $c, d \in [a,b]$ in the above theorem, the supremum and infimum in (10.4) and (10.5) are in fact the maximum and minimum, respectively. This proof is a beautiful application of the Bolzano–Weierstrass theorem—actually two beautiful applications.

We'll only prove the 'maximum' half of the theorem; the 'minimum' half is an exercise.

The idea is the following. Suppose for a contradiction that $\sup\{f(x) \mid x \in [a,b]\}$ does not exist. How can that happen? This is a non-empty set of real numbers; if it has an upper bound then the least upper bound principle says it has a supremum. So the only possibility is that this set doesn't have an upper bound. Well, that would mean that there are points $x_1, x_2, \dots$ in $[a,b]$ where the function values $f(x_1), f(x_2), \dots$ are growing bigger and bigger: the sequence of function values isn't bounded above. But this looks suspiciously like a contradiction. We know that if $\lim_{n\to\infty} x_n = c$, then $\lim_{x\to\infty} f(x_n) = f(c)$ by Theorem 10.7. But this can't be: the sequence of function values is unbounded, so it cannot be convergent.

But this isn't quite a contradiction: we don't know that $(x_n)_{n\in\mathbb{N}}$ is a convergent sequence—what if that sequence bounces around in $[a,b]$ without tending to a limit? The answer is: apply the Bolzano-Weierstrass theorem to find a convergent subsequence $(x_{n_k})_{k\in\mathbb{N}}$, and repeat the above argument with this convergent subsequence—this time it works.

That argument shows that $M = \sup\{f(x) \mid x \in [a,b]\}$ exists. But why is there actually a value $c \in [a,b]$ such that $f(c) = M$? Well, M is supposed to be a *least* upper bound of $\{f(x) \mid x \in [a,b]\}$. That means that for every $\varepsilon > 0$,

$$M - \varepsilon \text{ isn't an upper bound, i.e. there is some } x \in [a,b] \text{ such that } M \geq f(x) > M - \varepsilon. \tag{10.6}$$

Note that we can write that $M \geq f(x)$ since M is an upper bound for $\{f(x) \mid x \in [a,b]\}$. We want to use this to construct a sequence $(x_n)_{n\in\mathbb{N}}$ such that the function values converge to M, i.e. $\lim_{n\to\infty} f(x_n) = M$. We'll use the same trick we saw before: use (10.6) for a sequence of ε values which tends to zero. The obvious 'sequence tending to zero' is $\left(\frac{1}{n}\right)_{n\in\mathbb{N}}$, so let's use that. By (10.6), for each $n \in \mathbb{N}$ there is $x_n \in [a,b]$ such that $M \geq f(x) > M - \frac{1}{n}$. The Sandwich Theorem tells us $\lim_{n\to\infty} f(x_n) = M$. If $\lim_{n\to\infty} x_n = c$ exists, then by Theorem 10.7 we have $M = f(c)$, which is what we want.

Again, there is no reason why $\lim\limits_{n\to\infty} x_n$ should exist: if f has several global maxima, then perhaps $(x_n)_{n\in\mathbb{N}}$ bounces around between them without converging. But, again, the Bolzano-Weierstrass theorem rescues us.

Proof. We prove the first half of the theorem, leaving the second half as an exercise.

Let $S = \{f(x) \mid x \in [a,b]\}$. We first want to prove $M = \sup S$ exists, then we want to show that there is some $c \in [a,b]$ such that $f(c) = M$.

To show that sup S exists, we use the least upper bound property of $\mathbb{R}$. We just need to show that S is not empty and that it has an upper bound.

S is not empty because $f(a) \in S$.

Now suppose for a contradiction that S has no upper bound. Then in particular, for each $n \in \mathbb{N}$, the integer n is not an upper bound for S. That means there is an element of S which is bigger than n, i.e. a function value of f which is bigger than n. There is some $x_n \in [a,b]$ such that $f(x_n) > n$.

This gives us a sequence $(x_n)_{n\in\mathbb{N}}$ which is bounded: it is in $[a,b]$. By the Bolzano-Weierstrass theorem, there is a convergent subsequence $\left(x_{n_k}\right)_{k\in\mathbb{N}}$, and by Theorem 9.13 the limit s of this subsequence is in $[a,b]$.

Since $1 \le n_1 < n_2 < \dots$ by the definition of a subsequence, we have $n_k \ge k$. Thus $f(x_{n_k}) > n_k \ge k$ is true for each $k \in \mathbb{N}$, and so $\left(f(x_{n_k})\right)_{k\in\mathbb{N}}$ is not a bounded sequence. By Theorem 9.22 it is therefore not a convergent sequence. But this is a contradiction to Theorem 10.7, which says that $\lim\limits_{k\to\infty} f(x_{n_k}) = f(s)$, since $\lim\limits_{k\to\infty} x_{n_k} = s \in [a,b]$ and f is continuous on $[a,b]$ (and so in particular at s). This contradiction shows that our assumption—that S has no upper bound—is false.

Thus S has an upper bound, and we already observed that it is non-empty. So the least upper bound property of the reals says that sup S exists.

Now we show that $M = \sup S$ is $M = f(c)$ for some $c \in [a,b]$.

For each $n \in \mathbb{N}$, we let x_n be a point in $[a,b]$ such that $f(x_n) > M - \frac{1}{n}$. This exists since M is a *least* upper bound of S, and so in particular $M - \frac{1}{n}$ is not an upper bound of S.

Now the Sandwich Theorem says that, since $M - \frac{1}{n} < f(x_n) \le M$ holds for each $n \in \mathbb{N}$, so $\lim\limits_{n\to\infty} f(x_n) = M$.

By the Bolzano-Weierstrass theorem, $(x_n)_{n\in\mathbb{N}}$ has a convergent subsequence $(x_{n_k})_{k\in\mathbb{N}}$. Let $c = \lim\limits_{k\to\infty} x_{n_k}$; by Theorem 9.13 we have $c \in [a,b]$.

The sequence $\left(f(x_{n_k})\right)_{k\in\mathbb{N}}$ is a subsequence of $\left(f(x_n)\right)_{n\in\mathbb{N}}$ (which we just saw is convergent with limit M), so by Theorem 9.45 it is convergent with limit M.

Now by Theorem 10.7, since $c \in [a,b]$ and so f is continuous at c, we have $f(c) = M$. This finishes the proof of the first half of the theorem.

The proof that there exists $d \in [a,b]$ such that $f(d) = \inf S$ is left as an exercise. □

Something we should immediately notice at this point is the following. We have just proved a theorem which isn't obviously true, and the proof is not really all that easy. But all the work is being done by the theorems we proved already! We are proving things about continuous functions using convergent sequences, yet we never actually needed to use the definitions of either concept. Nor are we producing any 'pages of equations' as you might have expected from your school maths. This is good, because working with the definitions is painful and writing pages of equations is boring and easy to mess up.

This is your first taste of how modern mathematics looks. We want to build up a beautiful palace of a theorem, but we generally will not go all the way down to the bricks-and-mortar of working with all the basic definitions. Rather, we want to play architect: we outline how the proof should go, and call upon theorems we (or, usually, others!) already proved to serve as the walls and roof.

10.6 Sample exercises

Exercise 10.1. *Prove, using the definition of continuity, that the function $f:[0,\infty)\to\mathbb{R}$ given by $f(x)=\sqrt{x}$ is continuous at 4.*

Hint: First show that $|x-4|\geq 2|\sqrt{x}-2|$ for every $x\in[0,\infty)$.

Prove that the function $f:\mathbb{R}\to\mathbb{R}$ given by

$$f(x)=\begin{cases} x & \text{if } x \text{ is irrational,}\\ 0 & \text{if } x \text{ is rational,}\end{cases}$$

is continuous at 0.

Exercise 10.2. *Prove that if $f:\mathbb{R}\to\mathbb{R}$ is continuous and $f(x)=0$ whenever x is rational, then $f(x)=0$ for all $x\in\mathbb{R}$.*

Hint: Given any real number c, there exists a sequence of rational numbers $(q_n)_{n\in\mathbb{N}}$ that converges to c.

Exercise 10.3. *(a) Let $J=(a,b)$ be an open interval contained in another interval I. Let $f:I\to\mathbb{R}$ be a function. Let $c\in J$ and assume that $f\big|_J$ is continuous at c. Prove that f is continuous at c.*

(b) Give an example of intervals J and I with $J\subseteq I$, $c\in J$ and a function $f:I\to\mathbb{R}$ such that $f\big|_J$ is continuous at c, but f is not continuous at c.

(This shows that it is necessary to assume that J is an open *interval in (a)).)*

Exercise 10.4. *Show that the statement of Theorem 10.20 does not hold if $[a,b]$ is replaced by $[a,b)$.*

Exercise 10.5. *A function $f:\mathbb{R}\to\mathbb{R}$ is a* periodic function *if there exists $T>0$ such that for all $x\in\mathbb{R}$, $f(x+T)=f(x)$. If $f:\mathbb{R}\to\mathbb{R}$ is continuous and periodic, then prove that f is bounded, that is, the set $S=\{f(x)\mid x\in\mathbb{R}\}$ is bounded.*

Give an example of a periodic function g such that g is not bounded.

Exercise 10.6. ***Exam Question, 2009 Q5.***

(a) Let I be an interval in $\mathbb{R}$ and let $c\in I$.

What does it mean to say that a function $f:I\to\mathbb{R}$ is continuous at c ? What does it mean to say that a function $f:I\to\mathbb{R}$ is continuous on I?

(b) Suppose that $f:\mathbb{R}\to\mathbb{R}$, $g:\mathbb{R}\to\mathbb{R}$ and $h:\mathbb{R}\to\mathbb{R}$ are functions such that

(1) f and g are continuous on $\mathbb{R}$,

(2) $f(0)=g(0)$, and

(3) for every $x\in\mathbb{R}$, $f(x)\leq h(x)\leq g(x)$.

Show that h is continuous at 0.

(c) State the Intermediate Value Theorem.

Suppose that the function $f:[0,2]\to\mathbb{R}$ is continuous on the interval $[0,2]$ and $f(0)=f(2)\geq f(1)$. Prove that there exist numbers $a,b\in[0,2]$ such that $|a-b|=1$ and $f(a)=f(b)$.

Hint: Consider the function $g:[0,1]\to\mathbb{R}$ given by $g(x)=f(x+1)-f(x)$.

10.7 Comments on selected activities

Comment on Activity 10.1. We have

$$\lim_{n\to\infty} \tfrac{1}{\pi n} = \tfrac{1}{\pi} \lim_{n\to\infty} \tfrac{1}{n} = 0$$

using the Algebra of Limits and the known fact that $\lim_{n\to\infty} 1/n = 0$.

Since $f\left(\frac{1}{\pi n}\right) = sin(\pi n) = 0$, we have

$$\lim_{n\to\infty} f\left(\tfrac{1}{\pi n}\right) = f(0)\,.$$

However, this function f is *not* continuous at 0. To see this, observe that the sequence

$$\left(\tfrac{1}{2\pi n+\pi/2}\right)_{n\in\mathbb{N}}$$

is also convergent with limit zero, but

$$f\left(\tfrac{1}{2\pi n+\pi/2}\right) = 1$$

for all $n \in \mathbb{N}$. Since $1 \neq f(0)$, we see that (10.1) does not hold. So by Theorem 10.7, f is not continuous at 0.

Comment on Activity 10.2. We'll need to cheat a bit to prove that g is continous on $\mathbb{R}$. We don't know that the sine function is continuous, and proving it is rather hard given that we do not really know what the function is at all! We sort-of know that it comes from Euler's identity, but we don't really know how to work with infinite series. So let's just assume it is a continuous function (which is true).

Now for any $c \neq 0$, we can find an interval $[a, b]$ which contains c but not 0. And on that interval, $g(x)$ is a composition of two continuous functions, so it is continuous.

Proving continuity at 0 is easier, assuming we are happy to say we know $|sinx| \leq 1$ is true for all $x \in \mathbb{R}$. For any $\varepsilon > 0$, choose $\delta = \varepsilon$. Then for any $|x - 0| < \delta$ we have

$$\left|g(x) - g(0)\right| = \left|x \sin \tfrac{1}{x}\right| = |x| \cdot \left|\sin \tfrac{1}{x}\right| \leq |x| < \delta = \varepsilon\,,$$

which is what we wanted. □

If a continuous h^* existed, then necessarily we would have, for any $(x_n)_{n\in\mathbb{N}}$ which is convergent with limit 0 and all of whose terms are positive, the statement

$$h^*(0) = \lim_{n\to\infty} h^*(x_n) = \lim_{n\to\infty} h(x_n)$$

by Theorem 10.7. In particular, there cannot be two choices of $(x_n)_{n\in\mathbb{N}}$ where the limits of function values are different. But the two sequences in the solution above to Activity 10.1 do give different limits, namely 0 and 1 respectively (though proving the second sequence gives function values converging to 1 needs a little bit more work).

Comment on Activity 10.3. We can 'cheat' by for example letting

$$f(x) = \begin{cases} 1 & \text{if } x \leq \frac{1}{2} \\ \frac{3}{2} - x & \text{if } x > \frac{1}{2} \end{cases}\,.$$

But this only has infinitely many global maxima because it's constant on part of $[0, 1]$. Can we find a function which isn't constant on any part of $[0, 1]$ that does the job?

We can—try modifying one of the examples you saw before the Extreme Value theorem.

10.8 Solutions to exercises

Solution to Exercise 10.1.

First, we show the inequality given in the hint. We have that, for every non-negative x, $|x-4| = |(\sqrt{x}-2)(\sqrt{x}+2)| = |\sqrt{x}-2|\,|\sqrt{x}+2| \geq 2|\sqrt{x}-2|$.

Now we show that the square root function is continuous at 2. Take any $\varepsilon > 0$, and set $\delta = \varepsilon$. Then, if $x \in [0,\infty)$ with $|x-4| < \delta$, we have $|\sqrt{x}-\sqrt{4}| = |\sqrt{x}-2| \leq \frac{1}{2}|x-4| < \frac{1}{2}\delta < \varepsilon$, as required.

Solution to Exercise 10.2.

Let c be any real number (rational or irrational), and – following the hint – take some sequence (q_n) of rational numbers with $q_n \to c$. As f is continuous at c, we have $f(q_n) \to f(c)$, by Theorem 10.7. As each $f(q_n)$ is equal to 0, so is $f(c)$. Thus $f(c) = 0$ for all real c.

Solution to Exercise 10.3.

(a) If we choose $t = \frac{1}{2}\min(c-a, b-c)$, we see that inside our open interval (a,b), there is an open interval $(c-t, c+t)$ with c in the middle. That means that every point within distance t of c is in (a,b).

Now, let's prove that f is continuous at c. Given $\varepsilon > 0$, we know that there is some $\delta > 0$ such that, for every $x \in J$ with $|x-c| < \delta$, we have $|f(x)-f(c)| < \varepsilon$. We need the same conclusion without the "$\in J$", and that would be no problem at all if $\delta \leq t$, since then all points x within distance δ of c would be in $J = (a,b)$. The key point is that we are allowed to take a smaller δ, as long as we keep it positive. So here the natural thing to do is to set $\delta' = \min(\delta, t) > 0$. Now every x such that $|x-c| < \delta'$ satisfies both that $x \in J$ and tha $|x-c| < \delta$, and therefore $|f(x)-f(c)| < \varepsilon$.

(b) We can follow the hint and take $f(x) = \lfloor x \rfloor$. This takes the value 1 for $x \in [1,2)$, and so f is certainly continuous on $J = [1,2)$. However, f is not continuous on $(0,2)$, as (for instance) $f(1-1/2n) = 0$, for all $n \in \mathbb{N}$, so $f(1-1/2n)$ does not tend to $1 = f(1)$, even though $1-1/2n \to 1$.

Solution to Exercise 10.4.

We need to find an example of a continuous function $f : [a,b) \to \mathbb{R}$ such that there is no $c \in [a,b)$ with $f(c) = \sup\{f(x) : x \in [a,b)\}$. In other words, we want a function that does not have a maximum on $[a,b)$. If you think about it, you will see that any strictly increasing function will do, for instance $f(x) = x$ on $[1,2)$: here $\sup\{f(x) \mid x \in [1,2)\} = \sup[1,2) = 2$, but there is no $c \in [1,2)$ with $f(x) = x = 2$. It is even possible to come up with a function $f : [1,2) \to \mathbb{R}$ that is not bounded above (and hence the supremum does not exist) – one easy example is $f(x) = 1/(2-x)$.

Solution to Exercise 10.5.

The Extreme Value Theorem tells us that the restriction of f to $[0,T]$ is bounded: there is some M such that $|f(x)| \leq M$ for all $x \in [0.T]$.

Now note that, for any $x \in \mathbb{R}$, there are k and t such that $x = kT + t$, and $0 \leq t < T$. (We can take $k = \lfloor x/T \rfloor$.) As f is periodic with period T, we have $f(x) = f(t)$, so $|f(x)| \leq M$. The conclusion is that $|f(x)| \leq M$ for all $x \in \mathbb{R}$, and so f is bounded.

For an example of a periodic function which isn't bounded, of course we will need to look at discontinuous functions. One example is to consider the function g defined by setting, for each $0 < x \leq 1$ and each integer n,

$$g(n+x) = \tfrac{1}{x}\,.$$

This is well-defined, because there is exactly one way to write any given real number y in the form $y = n + x$ where n is integer and $0 < x \leq 1$. It is obviously periodic with period 1. But it is not bounded, because for each natural number m we have

$$g\left(\tfrac{1}{m}\right) = m\,.$$

Solution to Exercise 10.6.
(a) A function $f : I \to \mathbb{R}$ is continuous at c if for every $\varepsilon > 0$ there exists $\delta > 0$ such that for every $x \in I$, $|x - c| < \delta$, we have $|f(x) - f(c)| < \varepsilon$. [3pts]

A function $f : I \to \mathbb{R}$ is continuous on I if it is continuous at every point $c \in I$. [2pts]

(b) From (2) and (3), we have $f(0) = g(0) = h(0)$. [1pt]

We must show that for every $\varepsilon > 0$ there exists $\delta > 0$ such that for every x such that $|x - 0| < \delta$, we have $|h(x) - h(0)| < \varepsilon$. By (1), we know that

(i) for every $\varepsilon > 0$ there exists $\delta_f > 0$ such that for every x such that $|x - 0| < \delta_f$, we have $|f(x) - f(0)| < \varepsilon$, and

(ii) for every $\varepsilon > 0$ there exists $\delta_g > 0$ such that for every x such that $|x - 0| < \delta_g$, we have $|g(x) - g(0)| < \varepsilon$.

So, for given $\varepsilon > 0$, let $\delta = \min\{\delta_f, \delta_g\}$. For every $|x - 0| < \delta$, we have $|x - 0| < \delta_f$ and $|x - 0| < \delta_g$, hence $|f(x) - f(0)| < \varepsilon$ and $|g(x) - g(0)| < \varepsilon$.

So,

$$h(0) - h(x) = f(0) - h(x) \leq f(0) - f(x) \leq |f(x) - f(0)| < \varepsilon$$

and

$$h(x) - h(0) = h(x) - g(0) \leq g(x) - g(0) \leq |g(x) - g(0)| < \varepsilon.$$

[7pts for the bulk of the proof: 4 for the structure and idea, and 3 for the details]

(c) Intermediate Value Theorem: If $f : [a, b] \to \mathbb{R}$ is continuous and y is such that either $f(a) \leq y \leq f(b)$ or $f(b) \leq y \leq f(a)$, then there exists $c \in [a, b]$ such that $f(c) = y$. [3pts]

The function $j : \mathbb{R} \to \mathbb{R}$ given by $j(x) = x + 1$ is continuous by the Algebra of Limits. Since f is continuous on $[0, 2] \supseteq [1, 2]$, the composition h, $h(x) = f(x + 1) = f(j(x))$, is continuous on $[0, 1]$. Therefore the function $g(x) = f(x + 1) - f(x) = h(x) - f(x)$ is continuous on $[0, 1]$. [3pts, including 1 just for saying that g is continuous]

We see that $g(1) = f(2) - f(1) \geq 0$ and $g(0) = f(1) - f(2) \leq 0$. By the Intermediate Value Theorem, there exists $c \in [0, 1]$ such that $g(c) = f(c + 1) - f(c) = 0$. Take $a = c$, $b = c + 1$ and observe that $0 \leq c = a < b = c + 1 \leq 2$, $|a - b| = 1$ and $f(a) = f(b)$. [6pts: 3 for the idea and 3 for the detail]