MA102
Mathematical Proof and Analysis

and

MA103
Introduction to Abstract Mathematics

Michaelmas Term, weeks 1–5

Lecture Notes

These lecture notes were compiled by Peter Allen in 2021. However much of the content comes from Martin Anthony, Graham Brightwell, Jan van den Heuvel and Michele Harvey.

Contents

1 Introduction **5**
- 1.1 What is this course about? . . . 5
  - 1.1.1 How to get the most out of this course (and all the other maths courses) 8
  - 1.1.2 Topics covered (MA102, first half of MA103) . . . 10
- 1.2 Moodle . . . 10
- 1.3 Reading . . . 10
- 1.4 Activities and sample exercises . . . 11

2 Mathematical statements, proof, and logic **12**
- 2.1 Introduction . . . 12
- 2.2 Mathematical statements and proof . . . 12
  - 2.2.1 Examples of Mathematical Statements . . . 13
  - 2.2.2 Introduction to proving statements . . . 14
- 2.3 Some basic logic . . . 18
  - 2.3.1 Negation . . . 18
  - 2.3.2 Conjunction and disjunction . . . 20
  - 2.3.3 If-then statements . . . 21
  - 2.3.4 If and only if statements; logical equivalence . . . 22
- 2.4 Implications and associated statements . . . 23
  - 2.4.1 Converse statements . . . 23
  - 2.4.2 Contrapositive statements . . . 24
  - 2.4.3 Converse of the contrapositive . . . 24
- 2.5 What is a proof? . . . 25
- 2.6 How to prove it . . . 26
- 2.7 What is not a proof? . . . 28
- 2.8 Sample exercises . . . 30
- 2.9 Comments on selected activities . . . 30
- 2.10 Solutions to exercises . . . 31

3 Sets and quantifiers **32**
- 3.1 Sets . . . 32
  - 3.1.1 Basics . . . 32
  - 3.1.2 A note on notation . . . 33
  - 3.1.3 Set equality . . . 34
  - 3.1.4 Subsets . . . 34

3.1.5 Unions and intersections . . . 35
3.1.6 Arbitrary unions and intersections . . . 35
3.1.7 Universal sets and complements . . . 36
3.1.8 Sets and logic . . . 36
3.1.9 Cartesian products . . . 37
3.1.10 Power sets . . . 37
3.2 Quantifiers . . . 38
3.2.1 Quantifiers and arbitrary unions and intersections; empty sets . . . 39
3.3 Proof by contradiction . . . 41
3.4 Some terminology . . . 42
3.5 General advice . . . 43
3.5.1 Introduction . . . 43
3.5.2 Definition chasing and cases . . . 44
3.5.3 How to write mathematics . . . 46
3.5.4 How to do mathematics . . . 47
3.5.5 How to become better in mathematics . . . 48
3.6 Non-examinable: set theory—take 2 . . . 49
3.7 Sample exercises . . . 50
3.8 Comments on selected activities . . . 50
3.9 Solutions to exercises . . . 51

4 Structures, natural numbers and proof by induction 52
4.1 Introduction . . . 52
4.2 Mathematical structures . . . 52
4.2.1 Greatest and least elements . . . 54
4.3 The principle of induction . . . 55
4.3.1 Proof by induction . . . 55
4.3.2 An example . . . 56
4.3.3 Induction: why be careful? . . . 57
4.3.4 Variants . . . 58
4.4 Summation formulae . . . 60
4.5 Recursively defined sequences . . . 61
4.6 Sample exercises . . . 62
4.7 Comments on selected activities . . . 63
4.8 Solutions to exercises . . . 64

5 Functions and counting 67
5.1 Introduction . . . 67
5.2 Functions . . . 67
5.2.1 Basic definitions . . . 67
5.2.2 Composition of functions . . . 69
5.3 Bijections, surjections and injections . . . 70
5.4 Inverse functions . . . 72
5.4.1 Definition, and existence . . . 72
5.4.2 Examples . . . 72
5.5 Functions on sets . . . 73
5.6 Counting as a bijection . . . 74
5.7 The pigeonhole principle . . . 75
5.7.1 The principle . . . 75
5.7.2 What will be on the exam? . . . 77

5.7.3 Some applications of the Pigeonhole Principle . . . 79
5.8 A generalised form of PP . . . 81
5.9 Infinite sets . . . 81
5.10 Sample exercises . . . 81
5.11 Comments on selected activities . . . 82
5.12 Solutions to exercises . . . 82

6 Equivalence relations and the rational numbers 85
6.1 Introduction . . . 85
6.2 Equivalence relations . . . 85
6.2.1 Relations in general . . . 85
6.2.2 The special properties of equivalence relations . . . 86
6.3 Equivalence classes . . . 87
6.3.1 What's the point? . . . 89
6.4 Rational numbers . . . 90
6.4.1 An important equivalence relation . . . 90
6.4.2 Rational numbers as equivalence classes . . . 91
6.4.3 Doing arithmetic . . . 91
6.4.4 Non-examinable: Fields . . . 93
6.5 Sample exercises . . . 94
6.6 Solutions to exercises . . . 94

7 Real and complex numbers 96
7.1 Introduction . . . 96
7.2 Rational numbers and real numbers . . . 96
7.2.1 Real numbers: a 'sketchy' introduction . . . 97
7.2.2 Rationality and repeating patterns . . . 98
7.2.3 Irrational numbers . . . 100
7.2.4 'Density' of the rational numbers . . . 101
7.3 Complex numbers . . . 101
7.3.1 Introduction . . . 101
7.3.2 Complex numbers: a formal approach . . . 102
7.3.3 Complex numbers: a more usual approach . . . 102
7.3.4 Roots of polynomials . . . 104
7.3.5 The complex plane . . . 105
7.3.6 Polar form of z . . . 106
7.3.7 Exponential form of z . . . 107
7.4 Sample exercises . . . 109
7.5 Comments on selected activities . . . 109
7.6 Solutions to exercises . . . 110

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 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 which you spend three years training 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:

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

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. 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 future career for you!) 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.

1.1.1 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 normal years, I would expect you to ask lots of questions in lectures and in examples sessions. This year, we can't do that, but I do expect you to save up your questions for the Q & A sessions. However, when I ask a question in the lecture, and there is a break in the video, the intention is that you take time at this point seriously thinking about how to answer the question — this will help you understand the material better and get more out of the course. These questions *are* considered to be part of the course content, and it's quite possible that I will ask them again on the exam.

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 'Satisfactory' 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) relevant to that 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.

1.1.2 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 first five 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. The lecturer for the Analysis section of the course is Prof. Amol Sasane, and he will issue lecture notes covering the topic later in term.

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.

1.2 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.

1.3 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.

For the first half of the course (the part covered by these notes), the following two books are recommended, and most chapters of the notes will start with a reference to the corresponding chapters in these two books.

- Biggs, Norman L., *Discrete Mathematics*, Second edition. (Oxford University Press, 2002). [ISBN 0198507178].
- Eccles, P.J., *An Introduction to Mathematical Reasoning: numbers, sets and functions*. (Cambridge University Press, 1997). [ISBN 0521597188].

There is one topic that neither of these covers, which is the topic of Complex Numbers. However, this is a topic that is well-covered in a number of other textbooks — look around.

1.4 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. Even if some things look funny the first time you see them, expect that as you see them repeatedly through the course, you will get used to them.

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.

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.

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 'Boris Johnson' is not a sentence: it makes no assertion about what Boris Johnson did or did not do. 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 $\forall$ — 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.

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.

[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!

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'll get to that next term; for now, don't worry about it.

(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

$$n(n + 1) = 2k(2k + 1) = 2\left(k(2k + 1)\right).$$

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

$$n(n + 1) = (2k + 1)(2k + 2) = 2\left((2k + 1)(k + 1)\right),$$

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 true. 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.

This is true. 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: *if* n^2 is even *then* n is even.

Why would that establish what we want (namely that 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 natural numbers n, 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. If I write down one of the statements above, you'll be able to see immediately whether it is a simple true-or-false statement (a proposition) or whether there is some *free variable* in it and its truth could depend on the value of the free variable (a predicate). However later, when we are dealing with more complicated statements and have to explain something difficult, it will be useful for me to be able to say 'consider the proposition ...' and 'we have the predicate ...' and expect that these words have made your life easier — you know already that what is coming should be respectively a true-or-false statement, and have a free variable (or two) in it. Quite a lot of mathematical vocabulary and notation is there 'to help the reader'. It will always look unnecessary when it's introduced, because that will always be in a simple situation where what is intended is obvious. We will never test you on it (there will not be an exam question asking which of the following statements are predicates), but knowing it will help you understand and write mathematics better.

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:

- 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:

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

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'

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*.)

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

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

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.

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 $(P \implies Q) \wedge (Q \implies P)$.

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 '$P \iff Q$'

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

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'.

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

The *contrapositive* of an implication $P \implies Q$ is the statement $\neg Q \implies \neg P$. The contrapositive is logically equivalent to the implication, as Table 2.7 shows. (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.

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 6—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 $2 \times 2 = 2 + 2 = 4$ (which we'll see how to do next term). 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.
Let p and q be real numbers.

For all real a, b we have $ab \leq \frac{a^2+b^2}{2}$.
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 apear 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 $x \in \mathbb{R}$, 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 $x \in \mathbb{R}$.

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

where to get to the last line we used the identity $(\sin x)^2 + (\cos x)^2 = 1$, which holds for all $x \in \mathbb{R}$ 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. (That simply says that (2.1) holds, because $0 = 0$ 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 $x \in \mathbb{R}$. We have

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

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.

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?'.

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

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

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 $x = \mathsf{banana}$ 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

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

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 ($\implies$). 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.

Warning 3.1. 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 3.2. 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.

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 $E \setminus A$ and is

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

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. Now, a minor nastiness here is that $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$ is not the same thing as $\mathbb{R} \times \mathbb{R}^2$. For example $(1, 2, 2)$ is an element of the first set, whereas $(1, (2, 2))$ is an element of the second set. We will not need to worry about this, because we won't ever work with both sets at the same time. However, *we do not* say these two sets are equal, even though they look kind of similar and have kind of similar properties. One is a set of triples, the other is a set of pairs. We defined set equality, and according to that definition these two sets are different. We did not define *kind of similar* and we will not do so.

What you should remember here is: if you have two objects, and you want to write that they are equal, then check it according to the definition. If you can, great. If not, then they are not in fact equal, and your class teacher (or exam marker) will be very unhappy that you wrote nonsense. Generally, this happens when you write = because you feel you need to write some symbol and this is the one you are happiest with. Don't do that, figure out what in fact you want to say (in English, or indeed in whatever your favourite natural language is) and write it (in English, because otherwise I probably won't understand, sorry).

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 3.3. 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.

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 first thing to try if you are supposed to prove a universal statement. 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 3.4. 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 $P \implies Q$. One way to do this is by contradiction. What this means is that you suppose P is true but Q is false (in other words, that the statement $P \implies Q$ is false) and you show that, somehow, this leads to a conclusion that you know, definitely, to be false.

Here's an example.

Example 3.5. 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, it is not even, 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 a number X is not prime, that means 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 $2, 3, 5, \ldots, M$. 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. □

[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.

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 $\{p_1, \ldots, p_t\}$. Consider the integer $N = \big(p_1 \times p_2 \times \cdots \times p_t\big) + 1$. Now N is bigger than any of $p_1, \ldots, p_t$, so (by our assumption that $p_1, \ldots, p_t$ are all the prime numbers) it cannot be prime. And by construction N is not divisible by any of $p_1, \ldots, p_t$ (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

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

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 magic 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 Definition chasing and cases

There is a 'how to prove it' strategy that comes together with 'understand the statement'. Namely, try replacing words (or symbols) with a defined meaning with the definition written out. Often this can suggest a way to proceed.

Example 3.6. Prove that $\{x \in \mathbb{R} \mid x^2 + 4 \geq 8\} \cap \mathbb{N} = \{y \in \mathbb{Z} \mid y \geq 2\}$.

The first thing to notice with this statement is that the $=$ is a *set equality*. That has a definition, so we might get somewhere by writing it in. Since this is the aim — this is what we want to prove — we're going to be changing our aim, i.e. working backwards, to start with. Let's first give the proof, then explain it a little bit.

Proof.

$$\{x \in \mathbb{R} \mid x^2 + 4 \geq 8\} \cap \mathbb{N} = \{y \in \mathbb{Z} \mid y \geq 2\}$$

$$\forall z\,, \Big(z \in \{x \in \mathbb{R} \mid x^2 + 4 \geq 8\} \cap \mathbb{N}\Big) \iff \Big(z \in \{y \in \mathbb{Z} \mid y \geq 2\}\Big)$$

$$\forall z\,, \Big(z^2 + 4 \geq 8 \text{ and } z \text{ is a positive integer}\Big) \iff \Big(z \geq 2 \text{ is an integer}\Big)$$

Fix z. $\Big(z^2 + 4 \geq 8 \text{ and } z \text{ is a positive integer}\Big) \iff \Big(z \geq 2 \text{ is an integer}\Big)$

If z is not an integer, or z is not positive, then obviously both sides of $\Big(z^2 + 4 \geq 8 \text{ and } z \text{ is a positive integer}\Big) \iff \Big(z \geq 2 \text{ is an integer}\Big)$ are false, so the $\iff$ evaluates to True.

If $z = 1$, then we can check both sides of the $\iff$ are false, so the $\iff$ evaluates to True.

If $z \geq 2$ is an integer, then the right hand side of the $\iff$ is obviously true. For the left hand side, we need to check that since $z \geq 2$ we have $z^2 \geq 4$, and so $z^2 + 4 \geq 8$. That means that in this case both sides of the $\iff$ are true, so the $\iff$ evaluates to True.

Since any z is either not an integer, or is not positive, or it is 1, or it is an integer at least 2, we considered all the possibilities for z, and in each case we checked that $\Big(z^2 + 4 \geq 8 \text{ and } z \in \mathbb{N}\Big) \iff \Big(z \geq 2 \text{ is an integer}\Big)$ is true. So we can conclude

$$\forall z\,, \Big(z^2 + 4 \geq 8 \text{ and } z \in \mathbb{N}\Big) \iff \Big(z \geq 2 \text{ is an integer}\Big)$$

By definition (of $\wedge$ and of the sets written out below), that is the same thing as

$$\forall z\,, \Big(z \in \{x \in \mathbb{R} \mid x^2 + 4 \geq 8\} \cap \mathbb{N}\Big) \iff \Big(z \in \{y \in \mathbb{Z} \mid y \geq 2\}\Big),$$

and by definition, *that* is the same thing as

$$\{x \in \mathbb{R} \mid x^2 + 4 \geq 8\} \cap \mathbb{N} = \{y \in \mathbb{Z} \mid y \geq 2\}$$

so we are done. □

Again, the black lines are a complete proof. But we didn't know how to get started without thinking a bit first about what it is we actually wanted to prove. The first red line is just repeating what we want to prove. The second red line is writing out the definition of set equality *in this particular example*. That's what I mean by 'know and use' the definition — it's never going to help much to simply copy the definition from your notes; what you need to do is to write the definition as it applies to the thing you're working with.

The third red line is, again, simply copying out the definitions as they apply in this example. On the right, we're simply filling in what it means for z to be in the set $\{y \in \mathbb{Z} \mid y \geq 2\}$. On the left, we're filling in what it means for z to be in the conjunction of the two sets: namely (by definition) it is a real number such that $z^2 + 4 \geq 8$, and also it is a positive integer. Since all positive integers are real, I didn't bother to write the 'is a real number' bit. So far, our 'current aim' has been getting longer each line, which looks like negative progress — but it is also getting more concrete; we replaced abstract notation with things that you are familiar with. Generally that means it will be easier to handle.

At this point, we can see a standard strategy to try. We're supposed to prove a 'for all' statement, so let's pick a particular z and try to prove it for that particular z. This gives us the first black line of our proof, and (for the first time) the current aim actually gets shorter. What we now have to prove is something simple. Saying that z is an integer at least 2 is supposed to be the same thing as saying that z is a positive integer such that $z^2 + 4 \geq 8$.

There are a few ways to proceed at this point, but the one I chose is to illustrate another standard technique, 'proof by cases'. At this moment, we said nothing about what z is. The $\iff$ statement we are trying to prove could be true for any of several different reasons, depending on what z is. We simply list a bunch of reasons, called *dividing into cases*, and then check that every z is covered by one of these reasons.

Once we checked that our cases are *exhaustive* — that is, any possible z falls into at least one of them — then what we have proved is that for any z we have $\big(z^2 + 4 \geq 8 \text{ and } z \text{ is a positive integer}\big) \iff \big(z \geq 2 \text{ is an integer}\big)$. So we can write that down as the next black line; and then we finish the proof off by recopying the red lines from earlier in the reverse order, and checking that they really make sense written out forwards.

It's important that you are happy with this proof. If not, you should talk to me or your class teacher for a better explanation.

You may well feel that we've done a lot of unnecessary formalism to prove something 'obvious', if you're already happy with what the set notation means. This is a trap — it's important to be able to figure out how to write a formal proof from the definitions now, even though you know how to write an intuitive and convincing explanation of why these two sets are the same without bothering. This is because later (very soon) you'll be dealing with statements which are not so obvious, and you will not be able to rely on your intuition; then you need to be able to get started with a formal proof.

In particular, you may well feel that the definition chasing we did — replacing the set equality with its definition, and replacing the set membership and conjunction with their definitions — was just some formal nonsense that you did not need in order to see why the statement is true. However, later in the course, the statements you can attack by definition chasing will not be obvious, but it will still sometimes be the case that the only thing you need to do to get a solution is to replace notation or terms with their definitions till you get to something obvious.

Finally, we saw a 'proof by cases' of a 'for all' statement. There will be lots more of these to come. You haven't seen anything like this before because simple algebra statements, when they're true, are true for exactly one reason — the calculation you do to prove them. More complicated statements generally have multiple possible reasons for being true, as we saw here.

If you're not happy with the logic, think of it the following way. Whatever z is, we need to provide a reason why the predicate we're looking at (the $\iff$ statement) is True for that particular z. If there were only say 5 possible values of z, we could just do that by writing out each of the five corresponding statements and checking them. Since there are infinitely many possible values of z, we can't do that.

But we can tell a Checker how they should go about checking any particular z they want. You can imagine a dialogue with the Checker. The line 'fix z' means, we tell the Checker to decide on a particular z that they should check; maybe it's 5, or 0, or π, or banana. Then the 'if z is not an integer' line means: we tell the Checker to first ask themselves whether their favourite z is an integer; if it's not, we explain to them why the $\iff$ is true (your favourite z is not an integer, so both the left and right side of the $\iff$ come out to False, so the $\iff$ comes out True). Then the next line tells the Checker what to do if $z = 1$, and so on. Finally we make sure our cases are exhaustive — that means we are now confident that whatever z the Checker asks us for help with checking, we have written down a reason for the Checker why the $\iff$ comes out True.

In particular, 'fix z' does not mean that z is somehow 'all the possibilities at once'.

How should you know to think about proving something by cases? This is simple to say (but not always easy to do). If you can't find one argument that works for every z, then find an argument that works for some z, write it down, figure out which zs exactly it works for, and then think about how to handle the other zs. Keep going until you find you've dealt with every possible z.

3.5.3 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 "$x^2 = 1 \implies x = 1$ 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.

3.5.4 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.

3.5.5 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

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

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 $\left\{s \in S : P(s) \text{ is true}\right\}$ 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

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

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 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*

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

3.8 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.

3.9 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 ×, and the relation <.

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

(4) The real numbers $\mathbb{R}$ (intuitively: points on the number line) which again come with the operations + and ×, 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 it's not clear what < should be, so we leave it out.

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 Lent Term in MA103.

(6) The 'clock numbers' $\mathbb{Z}_{24}$, which are the integers $\{0, 1, 2, \ldots, 23\}$ 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 will write down a rather short list of assumptions, called *axioms*. And then we will *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. We'll develop it in MA103, in Lent Term, as a warm-up to 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. We will prove this from the axioms for the natural numbers in Lent Term. The main 'idea' of the proof is to use induction; it's worth thinking now about how you might do it.

Activity 4.1. *Use the Principle of Induction to prove the Well-Ordering Principle (and keep your proof safe for the next three months).*

Your proof for this activity will probably assume some properties of the natural numbers, such as (perhaps) that 1 is the least natural number. Once you get to Lent Term, you should pull out your proof again and look at what assumptions you made. Which of the assumptions can you justify from the Peano axioms *without* using the Well-Ordering Principle?

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*. However, the proof will come next term; for now, 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 fine point of view, and in Lent Term, when we come to an axiomatic approach to the natural numbers, one of our axioms will be (more or less) the statement that this particular 'and so on' is going to be accepted. We will actually be even more specific there, and so the Principle of Induction as stated above will need a (very short!) proof.

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 $1, 1, 2, 6, ...$ 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. $1^1 + 1 = 2$ 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 4.2. *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. 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 4.3. *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 'asssuming $P(1)$ 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 a proof by induction.

If you complete your '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.

Activity 4.4. *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 $k \geq 3$. We want to prove that 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

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

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

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

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.

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).

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:*

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

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 4.2. 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 4.3. 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 4.4. 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. This function was actually an important function (at least in the UK): it's the (in 2018) income tax you pay on income £x.

Activity 5.1. *Find a single formula which gives the function $g(x)$ above.*

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. Another example function is Drink, with domain $\{\text{Beer}, \text{Milk}\}$ and codomain $\{\text{Yes}, \text{No}, \text{Maybe}\}$ which is defined by $\text{Drink}(\text{Milk}) = \text{Maybe}$ and $\text{Drink}(\text{Beer}) = \text{Yes}$.

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 $\{1, \ldots, 1\,000\,000\}$ to $\{1, \ldots, 6\}$. (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. The Drink function describes your lecturer's preferences—it might not be very interesting, but at least it's easy to describe.

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

$$f(1) = 1 \text{ and } f(n) = 2 + 3f(n-1), \text{ for } n \geq 2\,.$$

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.

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 Composition of functions

Suppose that X, Y, Z are sets and that $f : X \to Y$ and $g : Y \to Z$. Then the *composition* $g \circ f$, also denoted by gf, 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. For example, given the function RightTime : {Morning, Evening} → {Beer, Milk} defined by RightTime(Morning) = Milk and RightTime(Evening) = Beer, it makes sense to talk about Drink ∘ RightTime. I think that in the morning it's the right time for milk, and in the evening it's the right time for beer. So if we put Morning into the composition Drink ∘ RightTime, then we can see that I will Maybe have a drink in the morning. It doesn't make sense to consider RightTime ∘ Drink, because whatever input from {Beer, Milk} we put into Drink the output is something not in the domain of RightTime; that function doesn't know what to do with an input Maybe.

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. A further point to be careful about is that the notation fg can cause confusion. 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. It should always be clear from the context whether gf should be interpreted as a composition. If I need to talk about the product of the functions f and g I will denote this by $f(x)g(x)$. The notation $g \circ f$ leads to less confusion, but it is not used in all textbooks.

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 $\forall y \in Y, \exists x \in X, \mathsf{s.t.}\ f(x) = y$.

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.** To do this, we 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.** We need to prove that, for each $y \in (-1, 1)$, 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. Let me explain why this proof is not hard.

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 $f(x) = f(y) \implies x = y$ is true for all $x, y \in \mathbb{R}$. 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.

What you should notice is that although there are a lot of steps here (and this only got to 'f is injective') all the steps are basic strategies: mostly definition chasing, plus a couple of times we did some high-school algebra to solve equations. Because there are a lot of steps, you have *no chance* of looking at the problem and seeing how the proof will go; it's easy to get scared.

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 $(g \circ f)(x) = x$ for all $x \in X$ and $(f \circ g)(y) = y$ for all $y \in Y$. 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}.

Theorem 5.8. *$f : X \to Y$ has an inverse function if and only if f is a bijection. When f is bijective, there is a unique inverse function.*

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: $f : X \to Y$ has an inverse $\Leftarrow$ f is bijective.

Suppose f is a bijection. For each $y \in Y$ there is exactly one $x \in X$ with $f(x) = y$. Define $g : Y \to X$ by $g(y) = x$. Then this is an inverse of f. Check this!

Next, we show: $f : X \to Y$ has an inverse $\Rightarrow$ f is bijective.

Suppose f has an inverse function g. We know that for any $y \in Y$, $f(g(y)) = (f \circ g)(y) = y$, so there is some $x \in X$ (namely $x = g(y)$) such that $f(x) = y$. So f is surjective.

Now 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 when f is bijective, the inverse is unique.

Suppose that g and h are inverses of f. Then both have domain Y and codomain X, and we just need to check that $g(y) = h(y)$ for every $y \in Y$. Well, $h \circ f$ is the identity function on X and $f \circ g$ is the identity function on Y. So, for any $y \in Y$ 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.

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 $x \to \big(f(x)\big)^{-1} = 1/f(x)$.

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,

$$y = f(x) \iff y = 3x + 1 \iff x = (y - 1)/3,$$

so

$$f^{-1}(y) = \frac{1}{3}(y - 1).$$

Let $\mathbb{Z}$ denote 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.

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 5.12. 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 5.13. 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 5.14 (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 5.15 (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 5.16. *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 $g : A \setminus \{a\} \to B \setminus \{b\}$.*

Proof. Given A and B, and elements a and b, as in the lemma statement, 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 want to use f to help us construct g. We consider two cases.

Case 1: $f(x) \in B \setminus \{b\}$ for each $x \in A \setminus \{a\}$.

This case is easy. 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 $f(s) = b$.

This case is simply what we get when we say 'we are not in Case 1'. It's what is left over after dealing with the easy case.

Let's first check that there is only one s such that $f(s) = b$. Indeed, suppose that for some $x \in A$ we have $f(x) = b$. Then $f(x) = f(s)$, and since f is injective, we conclude $x = s$.

This time, if we tried to define g as in Case 1, we would find g is not well-defined. g is supposed to have codomain $B \setminus \{b\}$, but $f(s) = b$. But this is the only 'problem'; we can hope to define $g(s)$ in some other way. The trick is: 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 we know $f(x)$ is always in B and we don't use $f(s)$ which is the only way of getting b.

What is not quite so clear is that g is injective. Let's check. Suppose that $g(x) = g(y)$ for some x, y. We want to show $x = y$.
If neither x nor y is equal to s, then by definition we have $g(x) = f(x)$ and $g(y) = f(y)$, so $f(x) = f(y)$, so since f is injective we have $x = y$. We need to deal with the case that at least one of x and y is equal to s; suppose without loss of generality it is x. Then we have $g(y) = g(x) = f(a)$. If $y \neq x$ then $g(y) = f(y) = f(a)$, but then since f is injective we have $y = a$ — and this is impossible, since $y \in A \setminus \{a\}$. So in this case also $y = x$ and we are done.

In either case, we were able to construct an injective g as desired, and the two cases are exhaustive. □

This proof is not all that easy to understand — because it is quite abstract — so here is a concrete 'story' of the proof.

Suppose you have a set of hotel guests (A) who are booked into the set of single rooms (B) in a hotel. The function $f : A \to B$ says which guest is booked into each room: that it is injective is telling you that each room has at most one guest booked in (some rooms might be empty, but no room has two guests booked in to it).

Now one guest (called a) checks out, and there is a water leak in one room (room number b) so becomes unusable. What does the hotel manager do? Well, if none of the remaining guests (the set $A \setminus \{a\}$) is booked into the wet room, they don't have to do anything. That's case 1.

If on the other hand there is a guest s booked into the wet room, then the manager can solve the problem by changing s's room to the one a has vacated. That's case 2.

We'll see this Lemma is what we need to prove Theorem 5.15 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 5.15.

Proof of Theorem 5.15. 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 5.16, 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 5.14.

Proof of Theorem 5.14. 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.

Suppose there is an injection $f : A \to B$. Consider the composite function $h^{-1} \circ f \circ g : \mathbb{N}_n \to \mathbb{N}_m$. If we can prove that this is an injection, then from Theorem 5.15 it follows that $n \leq m$.

So, let us prove injectivity. Suppose $a, b \in \mathbb{N}_n$ with $a \neq b$. Since g is a bijection $g(a), g(b) \in A$ with $g(a) \neq g(b)$. Since f is an injection, there are $f(g(a)), f(g(b)) \in B$ with $f(g(a)) \neq f(g(b))$. Since h^{-1} is a bijection, $h^{-1}(f(g(a)))$ and $h^{-1}(f(g(b)))$ belong to $\mathbb{N}_m$, and $h^{-1}(f(g(a))) \neq h^{-1}(f(g(b)))$. This last inequality is what we need. □

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 5.17. *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 such that we can write $|S| = m$ and $|S| = n$, 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 $|S| = m$ and $|S| = n$, then there are by definition bijections $f : \mathbb{N}_m \to S$ and $g : \mathbb{N}_n \to S$, and so $f^{-1} \circ g$ is a bijection from $\mathbb{N}_n \to \mathbb{N}_m$. And now Theorem 5.17 says $n = m$.

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 5.14) is to notice that it's enough to prove Theorem 5.15. This isn't 'necessary' — you can write a proof of Theorem 5.14 without deducing it from Theorem 5.15 — 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 5.15? 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 $1 \leq m$ 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 $m \geq 2$.

Now, at this point Lemma 5.16 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 5.16 is in order to prove Theorem 5.15. It is certainly not the case that some historical mathematician proved Lemma 5.16 and then noticed that they could use it to prove Theorem 5.15. What we can see at this point is that our induction hypothesis $P(k)$ will tell us $k \leq m-1$ (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 $m \geq 2$ 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 5.16. One could (and in previous years we did) not bother to write a separate Lemma, but simply prove the statement in quotes above at this point. But 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 5.18. *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 5.19. *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 5.20. *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 soon: 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 5.21. *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 5.22. *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 $A \cap B = \varnothing$. 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 $(X \setminus Y) \cup (Y \setminus X)$ and $X \cap Y$ are disjoint. Therefore,

$$|X \cup Y| = |(X \setminus Y) \cup (Y \setminus X)| + |X \cap Y|.$$

Now, $(X \setminus Y)$ and $(Y \setminus X)$ are disjoint, so

$$|(X \setminus Y) \cup (Y \setminus X)| = |(X \setminus Y)| + |(Y \setminus X)|$$

and therefore

$$|X \cup Y| = |(X \setminus Y)| + |(Y \setminus X)| + |X \cap Y|.$$

Now, the sets $X \setminus Y$ and $X \cap Y$ are disjoint and their union is X, so

$$|X| = |(X \setminus Y) \cup (X \cap Y)| = |X \setminus Y| + |X \cap Y|.$$

A similar argument shows that

$$|Y| = |(Y \setminus X) \cup (X \cap Y)| = |Y \setminus X| + |X \cap Y|.$$

These mean that

$$|X \setminus Y| = |X| - |X \cap Y| \text{ and } |Y \setminus X| = |Y| - |X \cap Y|.$$

So we have

$$\begin{aligned} |X \cup Y| &= |(X \setminus Y)| + |(Y \setminus X)| + |X \cap Y| \\ &= (|X| - |X \cap Y|) + (|Y| - |X \cap Y|) + |X \cap Y| \\ &= |X| + |Y| - |X \cap Y|. \end{aligned}$$

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. As an important example, we show how to *formally construct* the rational numbers using the integers and a carefully chosen equivalence relation.

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 $x, y \in X$, $x\,R\,y \iff y\,R\,x$).
- [**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 Equivalence classes

Given an equivalence relation, it is natural to group together objects that are related to each other. The resulting groupings are known as *equivalence classes*. In this section, we formally define equivalence classes and discuss some of their properties.

Definition 6.7. Suppose R is an equivalence relation on a set X and, for $x \in X$, let $[x]_R$ be the set of all $y \in X$ such that $y\,R\,x$. So,

$$[x]_R = \{y \in X \mid y\,R\,x\}.$$

Often, we will want to talk about the set of all equivalence classes of R. This set is written X/R, and referred to as the *quotient set of X by R*. So we have

$$X/R = \left\{[x]_R : x \in X\right\}.$$

Notice that each $[x]_R$ is a *subset* of X. If R is clear from the context—which it usually will be; in general we will only be talking about one equivalence relation at any given time—we may just write $[x]$ for $[x]_R$.

Example 6.8. Consider again R on $\mathbb{N}$ given by $m\,R\,n \iff m+n$ is even. Any even number is related to any other even number; and any odd number to any odd number. So there are two equivalence classes:

$$[1] = [3] = [5] = \cdots = \text{set of odd positive integers},$$

$$[2] = [4] = [6] = \cdots = \text{set of even positive integers},$$

and we have $\mathbb{N}/R = \big\{[1],[2]\big\}$.

You should keep in mind that even though we use the word 'equivalence class', what an equivalence class *is*, is simply a set: and you know how to handle sets. The name 'equivalence class' is just to remind you that this particular set is a special set and (as we'll shortly see) they have some extra nice properties. Similarly, we might say that 3 is a *representative* of the equivalence class set of odd positive integers (in the above example). That means exactly the same as saying that 3 is a member of the set set of odd positive integers; we use the word 'representative' instead of 'member' to remind ourselves that we are dealing with a special set.

Example 6.9. Given a function $f : X \to Y$, define a relation R on X by $x\,R\,z \iff f(x) = f(z)$. Then R is an equivalence relation. If f is a surjection, the equivalence classes are the sets

$$\{x \in X : f(x) = y\} = f^{-1}\big(\{y\}\big),$$

for $y \in Y$. Note that the place where we use that f is a surjection is that it implies each $f^{-1}\big(\{y\}\big)$ is non-empty. If f is not a surjection, then the equivalence classes are the sets $f^{-1}\big(\{y\}\big)$ for all $y \in Y$ such that there is an $x \in X$ with $y = f(x)$, in other words for each $y \in f(X)$.

Activity 6.1. *Check this!*

The equivalence classes have a number of important properties. These are given in the following result.

Theorem 6.10. *Suppose R is an equivalence relation on a set X. Then*

(i) For $x, y \in X$, $[x] = [y] \iff x\,R\,y$

(ii) For $x, y \in X$, if x and y are not related by R, then $[x] \cap [y] = \varnothing$.

Proof. (i) This is an if and only if statement, so we have two things to prove: namely that $[x] = [y] \implies x\,R\,y$ and that $x\,R\,y \implies [x] = [y]$.

Suppose, then, that $[x] = [y]$. The relation R is reflexive, so we have $x\,R\,x$. This means that $x \in [x]$. But if $[x] = [y]$, then we must have $x \in [y]$. But that means (by definition of $[y]$) that $x\,R\,y$.

Conversely, suppose that $x\,R\,y$. We now want to show that $[x] = [y]$. So let $z \in [x]$. (We will show that $z \in [y]$.) Then $z\,R\,x$. But, because $x\,R\,y$ and R is transitive, it follows that $z\,R\,y$ and hence $z \in [y]$. This shows $[x] \subseteq [y]$. We now need to show that $[y] \subseteq [x]$. Suppose $w \in [y]$. Then $w\,R\,y$ and, since $x\,R\,y$, we also have, since R is symmetric, $y\,R\,x$. So $w\,R\,y$ and $y\,R\,x$. By transitivity of R, $w\,R\,x$ and hence $w \in [x]$. This shows that $[y] \subseteq [x]$. Because $[x] \subseteq [y]$ and $[y] \subseteq [x]$, $[x] = [y]$, as required.

(ii) Suppose x and y are not related. We prove by contradiction that $[x] \cap [y] = \varnothing$. So suppose $[x] \cap [y] \neq \varnothing$. Let z be any member of the intersection $[x] \cap [y]$. (The fact that we're assuming the intersection is non-empty means there is such a z.) Then $z \in [x]$, so $z\,R\,x$ and $z \in [y]$, so $z\,R\,y$. Because R is symmetric, $x\,R\,z$. So: $x\,R\,z$ and $z\,R\,y$ and, therefore, by transitivity, $x\,R\,y$. But this contradicts the fact that x, y are not related by R. So $[x] \cap [y] = \varnothing$. □

Theorem 6.10 shows that either two equivalence classes are equal, or they are *disjoint*. Furthermore, because an equivalence relation is reflexive, any $x \in X$ is in some equivalence class (since it certainly belongs to $[x]$ because $x\,R\,x$). So what we see is that the equivalence classes form a *partition* of X: their union is the whole of X, and no two equivalence classes overlap.

Example 6.11. Consider again the equivalence relation R on $\mathbb{N}$ given by

$$m\,R\,n \iff m + n \text{ is even.}$$

We have seen that there are precisely two equivalence classes: the set of odd positive integers and the set of even positive integers. Note that, as the theory predicted, these form a partition of all of $\mathbb{N}$ (since every natural number is even or odd, but not both).

6.3.1 What's the point?

You're used to saying that two numbers are *equal* (or indeed two sets, or two functions...). Equality of integers (for example) is an equivalence relation, as you can easily check. It's not a very interesting equivalence relation, because its equivalence classes are all sets of size one.

In general, an equivalence relation is what we want to have when we get to the situation 'these two things are kind of the same, but they're not actually equal'. Let's give a familiar example.

If I give you a function $f : \mathbb{R} \to \mathbb{R}$ which has an integral $\int f(x)\,\mathrm{d}x$, what do I mean by that? Well, I might say (for a specific example) $\int 3x^2\,\mathrm{d}x = x^3$. But I could also write $\int 3x^2\,\mathrm{d}x = x^3 + 10$. As you know from school, an indefinite integral is only defined up to a constant; you probably were told to write $\int 3x^2\,\mathrm{d}x = x^3 + C$ where C is a constant. As you know, if you want to work out some definite integral, like $\int_{x=-4}^{7} 3x^2\,\mathrm{d}x$, the constant C cancels and it doesn't really matter what you chose.

We'd like to say '*the* indefinite integral of $f(x)$ is *the* function $F(x)$ such that $\frac{\mathrm{d}}{\mathrm{d}x}F(x) = f(x)$'. But that is *not well-defined*. There are lots of possible choices for $F(x)$. They are functions which differ by a constant, so we can't say '*the*' function; 'the' implies there is exactly one, which is not true.

In school, you dealt with this by always writing $+C$. That's fine (i.e. it works), but it gets annoying, especially if you have several integrals to do and you therefore need to write down several different letters for the different constants of integration. Most of the time (not all..!) it doesn't really matter what the constant is. You'd like to say these different functions are 'kind of the same'.

Define an equivalence relation S on functions $f : \mathbb{R} \to \mathbb{R}$ by fSg if and only if $\exists C \in \mathbb{R} : \forall x \in \mathbb{R}\, f(x) - g(x) = C$. In English, we say fSg if the functions f and g differ by a constant.

Activity 6.2. *Check that S is an equivalence relation.*

What are the equivalence classes of S? Well, they are sets of functions. If f is any particular function, then $[f]_S$ is
the set of all functions $g : \mathbb{R} \to \mathbb{R}$ such that $g(x) = f(x) + C$ for some constant C.

We can say that $\int 3x^2\,\mathrm{d}x$ is $[x^3]_S$. That is, if we pick any function f in $[x^3]_S$ (remember, this is a set of functions) then we have $\frac{\mathrm{d}}{\mathrm{d}x}f(x) = 3x^2$. And if we pick any function that's not in $[x^3]_S$, then its derivative (if it is has one!) will *not* be $3x^2$.

The advantage of this is that we can work with several indefinite integrals without having to write several different letters for constants of integration, but while still being reminded by the notation $[f]_S$ that when it matters we should put them in. We formalised the idea that $x^3 + 5$ and $x^3 + 10$ are 'kind of the same' as far as being indefinite integrals is concerned: what it means is they're both representatives of $[x^3]_S$.

In this case, we don't really gain a lot by introducing this equivalence relation. It is also pretty easy to write $+C$ whenever we want to write an indefinite integral. What we are doing when we write $+C$ every time, is simply writing out explicitly the *definition* of the equivalence relation S on every line. Whatever equivalence relation you are asked to work with, you *can* always write out the definition on every line instead of talking about equivalence classes.

However, if the equivalence relation we want to work with is complicated, it very quickly gets painful to write out the definition every time, and the mass of written-out-definition makes it hard to see what's important. Let's see an (important!) example.

6.4 Rational numbers

You're used to working with rational numbers — that is, the fractions, the set $\mathbb{Q}$, the numbers we can write as $\frac{p}{q}$ where p and q are integers (and q is not zero). You know how to add and multiply fractions, and so on. But why does all that makes sense? We can certainly think of the natural numbers as representing a physical concept — these are the numbers you use to count things (plus zero), the natural numbers $\mathbb{N}$. It makes sense to say that $2+3=3+2$, because either way, if we're counting apples we've counted to five apples. You're probably used enough by now to debt to feel that the concept of -1 is a natural enough thing (even if you are maybe not so happy with a negative bank balance), so you are presumably happy with the integers $\mathbb{Z}$. But what about fractions? What does it mean to multiply them?

Think about this for a moment—you might say you can make sense of $\frac{-1}{5}$ in terms of reality: it means I owe you a fifth of an apple; if there are five people who each owe you a fifth of an apple, then you are owed one apple, and this all sounds good. But what does it mean to multiply by $\frac{-1}{5}$? Why is $\frac{-1}{5}\cdot\frac{-1}{5}$ equal to $\frac{1}{25}$? You can probably come up with some sentence involving apples, but I'm not sure it will be very convincing—try it!

Another thing you can think about: 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?

6.4.1 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 pause for a moment to prove that Q is indeed an equivalence relation.

Q **is Reflexive:** $(m,n)Q(m,n)$ because $mn=nm$.

Q **is Symmetric:** $(m,n)Q(p,q) \implies mq=np \implies pn=qm \implies (p,q)Q(m,n)$.

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 $(m,n)Q(s,t)$.

6.4.2 Rational numbers as equivalence classes

We usually write the equivalence class $[(m,n)]_Q$ as $\frac{m}{n}$. For example, we then have the (familiar) fact that $\frac{2}{5} = \frac{4}{10}$ which follows from the fact that $[(2,5)]_Q = [(4,10)]_Q$ (i.e. these two sets are equal). Why are they equal? You could prove it from the definition of set equality, but it's easier to use the theory we developed. We know $(2,5)Q(4,10)$, because $2 \times 10 = 4 \times 5$. And now Theorem 6.10 tells us $[(2,5)]_Q = [(4,10)]_Q$.

We can now say what the *set of fractions*, written $\mathbb{Q}$, is. It is the set of all the equivalence classes of the relation Q. So $\frac{2}{5}$ is a fraction. So is $\frac{2}{1}$. So is $\frac{4}{10}$, and (as we just saw) in fact $\frac{2}{5}$ is the same thing as $\frac{4}{10}$.

What we have done here is to find a way of making sense of fractions, and being able to say when two fractions are the same, without ever having to define 'division'. We are only relying on the properties of $\mathbb{Z}$—adding and multiplying integers—that you are already happy with.

Logically, this is the 'right thing to do'.

To see why, think about how you might try to define 'division' without using fractions. You *can* do that if you try hard enough (for example, you might write out exactly what you mean by decimal long division) but you will end up with a complicated definition that's hard to work with (why is it true that $\frac{2}{14}$ and $\frac{3}{21}$ have the same decimal expansion..?). Whereas if we define fractions, we can rather easily define division: we'll just say that dividing by n means multiplying by $\frac{1}{n}$. (We *didn't* say what multiplying fractions means yet — we'll get to that!) and this turns out to be much easier to work with.

What about simply saying 'obviously fractions exist and we can just work with them'? The problem with this is: what if there is something we're missing? It's a bit hard to explain what exactly the problem might be here: you are so used to fractions that you probably cannot imagine what could possibly be a problem. But it *is* a bit funny that $\frac{-1}{5} \cdot \frac{-1}{5} = \frac{1}{25}$; it's hard to explain what that should mean in 'real world' terms. The last time we saw something a bit funny was in Section 3.6, and there, we *did* run into problems with a way of defining sets that at first looks perfectly reasonable.

What we are doing here—we're currently part-way through—is to *construct* the fractions from the integers. So far, we defined an equivalence relation, and we created a set $\mathbb{Q}$ which is the set of equivalence classes. But a set on its own isn't very interesting: we want to do things with it.

6.4.3 Doing arithmetic

How do we 'do arithmetic' with rational numbers. Well, you've been doing this for years, but how would we define addition and multiplication of rational numbers in an abstract setting?

I'm going to deliberately make the definition in a very formal (and maybe slightly scary) way, then explain why it's exactly what you're used to.

Definition 6.12 (Addition and multiplication of rational numbers)**.** Suppose q and r are rational numbers. That is, they are equivalence classes of the equivalence relation Q; they are sets whose pairs are members of the form (x,y) where x is an integer and y is a non-negative integer.

To find out what $q \oplus r$ is, pick a representative (a,b) of q and a representative (c,d) of r. We define $q \oplus r = \big[(ad+bc, bd)\big]_Q$.

Similarly, we define $q \otimes r = \big[(ac, bd)\big]_Q$.

At this point, you *should* be concerned. Why is this well-defined? That is, why don't we run into the same problem as with 'define t to be the number of cards in a deck', that depending on which deck you pick, you get a different answer.

This is a perfectly reasonable concern. Suppose I try to calculate $\frac{1}{3} \oplus \frac{1}{4}$. I could pick $(1,3)$ as a representative of $\frac{1}{3}$, and $(2,8)$ as a representative of $\frac{1}{4}$. Then I get $\frac{1}{3} \oplus \frac{1}{4} = \big[(14,24)\big]_Q$ (i.e. the fraction $\frac{14}{24}$). I could equally well pick $(-3,-9)$ as a representative of $\frac{1}{3}$ and $(5,20)$ as a representative of $\frac{1}{4}$, in which case I get $\frac{1}{3} \oplus \frac{1}{4} = \big[(-105,-180)\big]_Q$ (the fraction $\frac{-105}{-180}$. The numbers we get for these different choices are certainly different, but some magic has happened: we can see $14 \times (-180) = 24 \times (-105)$, so $\frac{14}{24} = \frac{-105}{-180}$. We did actually get the same answer both times.

What we have just done is checked that the definition of $\oplus$ is well-defined at least in this one very special case. But that is not good enough. We need to *prove* that this will always work. That is, we need to prove the following.

Theorem 6.13. *Suppose $a, b, c, d, a', b', c', d'$ are any integers with b, b', d, d' not equal to zero. If we have*

$$(a,b)\,Q\,(a',b') \quad \textit{and} \quad (c,d)\,Q\,(c',d')$$

then

$$\big(ad+bc, bd\big)\,Q\,\big(a'd'+b'c', b'd'\big) \quad \textit{and} \quad \big(ac, bd\big)\,Q\,\big(a'c', b'd'\big).$$

Just to be clear if $(a,b)Q(a',b')$, that is saying that they are in the same equivalence class (call it q) of Q. Similarly (c,d) and (c',d') are in the same equivalence class (call it r) of Q. The conclusion of the theorem is that if we want to know what $q \oplus r$ is, or $q \otimes r$, it *doesn't matter* which of the two representatives we pick for q or for r. We may well get different numbers out of the definition, but (as in the example with $\frac{1}{3} \oplus \frac{1}{4}$) we will always get representatives of *the same equivalence class* out.

This theorem will be an exercise—so there is no proof in these notes. But here is a warning. You *cannot* prove it by relying on anything about fractions. The whole point of Theorem 6.13 is to *show* that it makes sense to talk about adding and multiplying fractions using our definition. If you assume something about fractions to prove it, your argument is essentially 'It works because it works'; it's circular (i.e. it is nonsense). Your proof of Theorem 6.13 needs to use the definition of Q, and it needs to use stuff you know about the *integers* (like that multiplication is commutative, that we can cancel non-zero factors from both sides of an equation, and so on).

Once we are happy that $\oplus$ and $\otimes$ are well-defined, we can stop being so careful. In the rest of the course, we'll just write $\frac{1}{3} + \frac{1}{4}$ rather than $\frac{1}{3} \oplus \frac{1}{4}$, and we will not worry any more about whether we have $\frac{1}{3}$ or $\frac{2}{6}$ as a representative of the fraction. We don't have to worry—we *proved* it is OK! Having done that, we don't really need to keep remembering that $\frac{1}{3}$ is really a set and not a number. We can just remember that $\frac{1}{3} = \frac{2}{6} = \ldots$ and we can just add fractions as we're used to doing.

We will do one more thing: we will *identify* the integer $n \in \mathbb{Z}$ with the fraction $\frac{n}{1} \in \mathbb{Q}$. Officially these are not the same thing (one is a number, the other is a set), but (as you can check from the definitions) you will get the same answers to calculations whichever you use.

That means we will write $\mathbb{Z} \subseteq \mathbb{Q}$, and from now on we will stop thinking of the members of $\mathbb{Q}$ as being sets, we'll just think of them as numbers (as you're used to).

Finally, we are in a position to define 'division'. If $\frac{a}{b} \in \mathbb{Q}$ is not 0 (i.e. we don't have $a = 0$) then we say that 'dividing by $\frac{a}{b}$' means multiplying by the fraction $\frac{b}{a}$.

By the way, the rational numbers are described as such because they are (or, more formally, can be represented by) *ratios* of integers.

6.4.4 Non-examinable: Fields

We should, at this point, really go off and check that addition and multiplication of fractions behave 'the way they should do'; that multiplication is commutative, and so on. What we would like to check, really, is that $\mathbb{Q}$ is a *field*. What does that mean?

Definition 6.14 (Field axioms)**.** $\mathbb{F}$ is a field, with operations + and ×, if we have:

($\mathbb{F}$1) Closure under addition and multiplication: for each $a, b \in \mathbb{F}$ both $a + b$ and $a \times b$ are in $\mathbb{F}$.

($\mathbb{F}$2) Commutative addition and multiplication: for each $a, b \in \mathbb{F}$ we have $a + b = b + a$ and $a \times b = b \times a$.

($\mathbb{F}$3) Associative addition and multiplication: for each $a, b, c \in \mathbb{F}$ we have $(a + b) + c = a + (b + c)$ and $(a \times b) \times c = a \times (b \times c)$.

($\mathbb{F}$4) The distributive law: for each $a, b, c \in \mathbb{F}$ we have $(a + b) \times c = a \times c + b \times c$.

($\mathbb{F}$5) Additive and multiplicative identity: there are two different elements 0 and 1, such that for each $a \in \mathbb{F}$ we have $a + 0 = a$ and $a \times 1 = a$.

($\mathbb{F}$6) Additive and multiplicative inverses: for each $a \in \mathbb{F}$ there is an element $-a$ such that $a + (-a) = 0$, and if $a \neq 0$ there is an element a^{-1} such that $a \times a^{-1} = 1$.

If you want to, you can do this check for $\mathbb{Q}$ without too much trouble: it's long, but not hard. You'll need to use the definition of $\mathbb{Q}$ together with its operations $\oplus$ and $\otimes$, and you'll need to know things like that multiplication of integers is commutative, and the distributive law for the integers.

You should notice that the axioms for a field are all things you knew long ago are true for the rational numbers, or for the real numbers[1]. They are all part of the 'doing algebra as normal' that you learned in school. You'll probably notice, too, that there are some properties that the rational numbers have which *aren't* listed. For example the rational numbers have an order and you know how to do algebra with the < sign, too. We could have written down some more axioms saying that there is an order and saying how 'algebra as normal' works with an order (things like: if $a < b$ then $a + c < b + c$). That would give us an *ordered field*. You will see later in the course that some fields are not ordered—for example there is no way to put a sensible order on $\mathbb{C}$; no matter what you try, some piece of 'algebra as normal with <' won't work.

This is your first (brief, and non-examinable!) introduction to the axiomatic approach to mathematics, which we will see a good deal more of next term. What is the point?

Well, look to your MA100 notes on linear algebra (if you got that far—if not, it will start in the next week or two) and look at a few statements. Matrix addition is commutative; both addition and multiplication are associative. There isn't really an explicit proof given for these statements, but you can probably see how to check at least the statements for addition. You'll notice that all the things you do in your proof are using the field axioms. What that means is: *those statements are true not just for matrices of real numbers, but for any field.* In fact, that's true for most of the liner algebra in MA100.

That turns out to be incredibly useful. There are many different fields in mathematics, and some of them have practical applications too. For one example, the way that this document was transmitted from my computer to yours makes use of linear algebra over the field $\mathbb{Z}_2$. Linear algebra over $\mathbb{Z}_2$ is the basis of *coding theory*, which is (part of) what makes Internet communication work reliably.

[1]These axioms are standard, though in some texts you might see an explicit statement that + and × are functions from $\mathbb{F}^2$ to $\mathbb{F}$ and the axiom of closure missing. This doesn't make any important difference.

But you do not have to learn a whole new MA100 course to understand coding theory. All you need to know is what $\mathbb{Z}_2$ is (next term) and to quickly check which results in MA100 use only the field axioms. Then you can simply use what you learned in MA100 (and when you want to do linear algebra over $\mathbb{Z}_3$, you don't even need to check which results are allowed, since you already did that for $\mathbb{Z}_2$).

Not everything in MA100 does use only the field axioms. For example, you can't find a unit vector in the direction $\binom{1}{1}$, because the length of that vector is $\sqrt{2}$, which (we said earlier) isn't rational.

If we tried to do mathematics without the axiomatic approach to structures, we'd either spend forever re-proving (and trying to learn!) dozens of almost-identical theorems for all the different fields we want to do linear algebra over (and so on), or we would have to say something vague like 'matrix addition is commutative whenever we can do algebra as normal'. The first of these is a waste of time and energy, the second is dangerous: what *is* algebra as normal? Does it include taking square roots? Either you have to guess, or you have to check the proof for square-rooting every time you want to use a theorem (which is again a waste of time and energy).

With the axiomatic approach, we can simply say 'matrix addition is commutative over any field': easy to learn and precise, once you remember what a field is. Quite a lot of mathematics is like this: you need to learn some definition or concept, which at first looks like formality for the sake of it (you don't do algebra by thinking explicitly about the field axioms!) but the payoff is that in the long run it will make your life easier.

Don't be fooled into believing that checking the field axioms for $\mathbb{Q}$ from our definition (remember, $\mathbb{Q}$ is a set of equivalence classes with some funny formulae defining addition and multiplication) is somehow 'automatically' going to work. It's reasonable to think: we start with integers (where multiplication is commutative), we construct something with pairs of integers and define 'multiplication', of course the multiplication will be commutative.

That's not a valid argument. To see why, think about 2-by-2 matrices (with integer entries, say). We build the set of 2-by-2 integer matrices by starting with the integers (where multiplication is commutative) and define 'multiplication' of matrices, but the multiplication is *not* commutative.

6.5 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, and describe the corresponding equivalence classes.*

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. *Suppose that $f : X \to Y$ is a surjection. Define the relation R on X by $x\,R\,y \iff f(x) = f(y)$. Prove that R is an equivalence relation. What are the equivalence classes? Let C denote the set of equivalence classes $[x]$ for $x \in X$. Prove that if $[x] = [y]$ then $f(x) = f(y)$. This means that we can define a function $g : C \to Y$ by: $g([x]) = f(x)$. Prove that g is a bijection.*

Exercise 6.5. *Prove that the set $\{x \in \mathbb{Z} \mid x \text{ is a multiple of } 4\}$ has no lower bound.*

6.6 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. Given any $x \in \mathbb{Z}$, the equivalence class $[x]$ consists precisely of those integers y such that $y^2 = x^2$. So $[x] = \{x, -x\}$.

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.

For $x \in X$, $[x]$ is the set of all $y \in X$ with $f(y) = f(x)$, so, since f is a surjection, the equivalence classes are exactly the sets C_z for each $z \in Y$, where $C_z = \{x \in X \mid f(x) = z\}$ is the set of elements of X mapped onto z by f.

The fact that $[x] = [y]$ implies $f(x) = f(y)$ follows directly either from this description of equivalence classes, or from the fact that $[x] = [y]$ implies $x\,R\,y$, which implies $f(y) = f(x)$.

Let g be as defined. It is surjective because for each $z \in Y$, there is some $x \in X$ such that $f(x) = z$ (since f is surjective) and hence $g([x]) = f(x) = z$. Also, g is bijective because $g([x]) = g([y])$ implies $f(x) = f(y)$, which means $x\,R\,y$ and hence that $[x] = [y]$.

Solution to Exercise 6.5. We can prove this by contradiction. Suppose that the set $S = \{x \in \mathbb{Z} \mid x \text{ is a multiple of } 4\}$ has a lower bound, l. Then, for all $x \in S$, $x \geq l$. Now, one of $l-1, l-2, l-3, l-4$ must be a multiple of 4. So one of these numbers is in S. However, each is less than l, contradicting the fact that l is a lower bound on S.

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.

7.2.1 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

$$a_0 + \frac{a_1}{10} + \frac{a_2}{(10)^2} + \cdots + \frac{a_n}{(10)^n}.$$

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 $0.99999\dots$, all of whose digits after the decimal point are 9, is in fact the same as the number $1.0000000\dots$.

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 $0.1\overline{123}$.

7.2.2 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.

$$\begin{array}{r} 0.5714285\cdots \\ 7\,\overline{)\,4.0000000} \\ \underline{3.5} \\ .50 \\ \underline{.49} \\ 10 \\ \underline{7} \\ 30 \\ \underline{28} \\ 20 \\ \underline{14} \\ 60 \\ \underline{56} \\ 40 \\ \underline{35} \\ 50 \end{array}$$

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.

$$\begin{array}{r} 0.5714285\cdots \\ 7\,\overline{)\,4.0000000} \\ \underline{3.5} \\ .\mathbf{5}0 \\ \underline{.49} \\ 10 \\ \underline{7} \\ 30 \\ \underline{28} \\ 20 \\ \underline{14} \\ 60 \\ \underline{56} \\ 40 \\ \underline{35} \\ \mathbf{5}0 \end{array}$$

We can formalise this very easily:

Theorem 7.3. *If $\frac{p}{q} = a_0 \cdot a_1 a_2 a_3 \ldots$ 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.*

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 $\{1, 2, \ldots, q+1\}$ to $\{0, 1, \ldots, q-1\}$ by setting $f(i) = r_i$. Since the domain is larger than the codomain, by the Pigeonhole Principle there exist $i, j \in \{1, 2, \ldots, q+1\}$ 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 Lent 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.*

7.2.3 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 $a_0.a_1a_2\ldots a_n$ is within $1/(10)^n$ of the real number with infinite decimal expansion $a_0.a_1a_2\ldots$.

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.

7.2.4 '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. Recall that in the last chapter, we constructed the rational numbers from the integers, by explaining how to view rational numbers as equivalence classes of pairs of integers, and explaining how, in terms of these equivalence classes, to do addition and multiplication.

The formal construction of 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.

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 — and these other things are called '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 6.4.1). 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 $\mathrm{Re}(z)$, and the real number b is the imaginary part of z, denoted $\mathrm{Im}(z)$. Note that $\mathrm{Im}(z)$ 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.

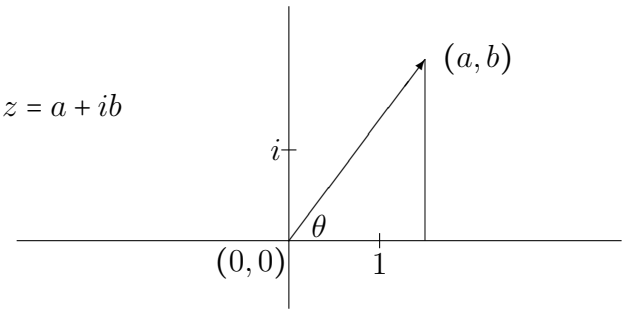
Theorem 7.13. *Two complex numbers are equal if and only if their real and imaginary parts are equal.*

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 $(a, b)^T$ 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.

$$e^{i\frac{2\pi}{3}} = \cos\tfrac{2\pi}{3} + i\sin\tfrac{2\pi}{3} = -\tfrac{1}{2} + i\tfrac{\sqrt{3}}{2}.$$
$$e^{2+i\sqrt{3}} = e^2e^{i\sqrt{3}} = e^2\cos\sqrt{3} + ie^2\sin\sqrt{3}.$$

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

$$w^6 = (1 - i\sqrt{3})^6 = (2e^{-i\frac{\pi}{3}})^6 = 2^6e^{-i2\pi} = 64$$
$$zw = (2\sqrt{2}e^{i\frac{\pi}{4}})(2e^{-i\frac{\pi}{3}}) = 4\sqrt{2}e^{-i\frac{\pi}{12}}$$

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 $z, w \in \mathbb{C}$,

$$e^{z+w} = e^ze^w \qquad \text{and} \qquad (e^z)^n = e^{nz} \quad \text{for } n \in \mathbb{Z}.$$

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 $z^6 = (re^{i\theta})^6 = r^6e^{i6\theta}$, $\quad -1 = e^{i\pi} = e^{i(\pi+2n\pi)}$

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

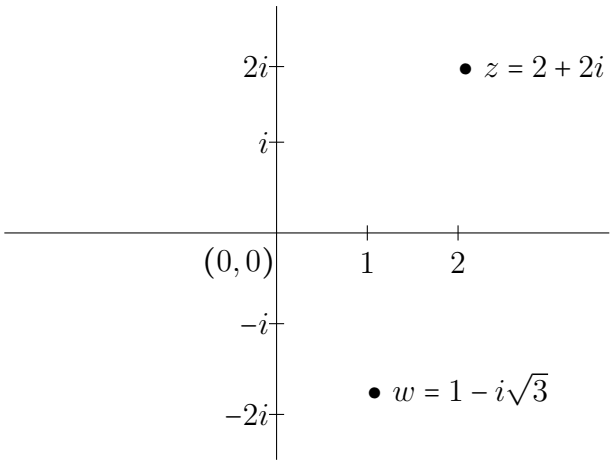
$$a^2 = nb^2$$

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,

$$(1 + \sqrt{3}i)^{30} = z^{30} = \left(2e^{\pi i/3}\right)^{30} = 2^{30}e^{30\pi i/3} = 2^{30}e^{10\pi i} = 2^{30}.$$