Table of notation

Term	Meaning	First Used
$\square$	The proof is complete	Page 4
$m \mid n$	m divides n	Page 4
$m \not\mid n$	m does not divide n	Page 4
$a \pmod n$	remainder on dividing a by n	Page 20
$a \equiv b \pmod n$	n divides $a - b$	Page 22
$\in$	is a member of	Page 6
$\notin$	is not a member of	Page 6
$\{ \dots \}$	the set of $\dots$	Page 6
$\{x \in A : x \text{ has property P}\}$	the set of $x \in A$ such that x has property P	Page 6
$\{x \in A \mid x \text{ has property P}\}$	the set of $x \in A$ such that x has property P	In lectures
$A \subseteq B$	A is a subset of B	Page 6
$A \supseteq B$	B is a subset of A	Page 17
$\emptyset$	the empty set	Page 7
$A \cup B$	A union $B = \{x : x \in A \text{ or } x \in B\}$	Page 48
$A \cap B$	A intersection $B = \{x : x \in A \text{ and } x \in B\}$	Page 18
$A \setminus B$	the complement of B in $A = \{x \in A : x \notin B\}$	Page 7
A^c	the complement of A	Page 54
id_A	the identity map from the set A to itself	Page 61
$\forall$	for all	Page 52
$\exists$	there exists	Page 52
$P \& Q, P \wedge Q$	P and Q	Page 14,49
$P \vee Q$	P or Q (or both)	Page 49
$\neg P$	not P	Page 51
$\Longrightarrow$	implies	Pages 14, 51
$\Longleftrightarrow$	is equivalent to	Page 14
$\overline{z}$	conjugate of z	Page 35
$\lvert z \rvert$	modulus of z	Page 36
$\Re(z)$	real part of z	Page 32
$\Im(z)$	imaginary part of z	Page 32

Lecture Notes for MA 132 Foundations

based on notes by D. Mond, revised in 2011 by J. Cremona

Contents

1 Introduction

Alongside the subject matter of this course is the overriding aim of introducing you to university mathematics.

Mathematics is, above all, the subject where one thing follows from another. It is the science of rigorous reasoning. In a first university course like this, in some ways it doesn't matter about what, or where we start; the point is to learn to get from A to B by rigorous reasoning.

So one of the things we will emphasise most of all, in all of the first year courses, is proving things.

Proof has received a bad press. It is said to be hard - and that's true: it's the hardest thing there is, to prove a new mathematical theorem, and that is what research mathematicians spend a lot of their time doing.

It is also thought to be rather pedantic - the mathematician is the person who, where everyone else can see a brown cow, says "I see a cow, at least one side of which is brown". There are reasons for this, of course. For one thing, mathematics, alone among all fields of knowledge, has the possibility of perfect rigour. Given this, why settle for less? There is another reason, too. In circumstances where we have no sensory experience and little intuition, proof may be our only access to knowledge. But before we get there, we have to become fluent in the techniques of proof. Most first year students go through an initial period in some subjects during which they have to learn to prove things which are already perfectly obvious to them, and under these circumstances proof can seem like pointless pedantry. But hopefully, at some time in your first year you will start to learn, and learn how to prove, things which are not at all obvious. This happens quicker in Algebra than in Analysis and Topology, because our only access to knowledge about Algebra is through reasoning, whereas with Analysis and Topology we already know an enormous amount through our visual and tactile experience, and it takes our power of reasoning longer to catch up.

Compare the following two theorems, the first topological, the second algebraic:

Theorem 1.1. The Jordan Curve Theorem *A simple continuous closed plane curve separates the plane into two regions.*

Here "continuous" means that you can draw it without taking the pen off the paper, "simple" means that it does not cross itself, and "closed" means that it ends back where it began. Make a drawing or two. It's "obviously true", no?

Theorem 1.2. *There are infinitely many prime numbers.*

A prime number is a natural number $(1, 2, 3, \ldots)$ which is greater than 1 and cannot be divided (exactly, without remainder) by any natural number except 1 and itself. The numbers $2, 3, 5, 7$ and 11 are prime, whereas $4 = 2 \times 2, 6 = 2 \times 3, 9 = 3 \times 3$ and $12 = 3 \times 4$ are not. Note that 1 is *not* a prime number, even though its only divisors are itself (and 1!): if 1 were counted as prime, it would complicate many statements.

I would say that Theorem 1.2 is less obvious than Theorem 1.1. But in fact Theorem 1.2 will be the first theorem we prove in the course, whereas you won't meet a proof of Theorem 1.1 until a lot later. Theorem 1.1 becomes a little less obvious when you try making precise what it means to "separate the plane into two regions", or what it is for a curve to "be continuous". And less obvious still, when you think about the fact that it is not necessarily true of a simple continuous closed curve on the surface of a torus.

In some fields you have to be more patient than others, and sometimes the word "obvious" just covers up the fact that you are not aware of the difficulties.

A second thing that is hard about proof is understanding other peoples' proofs. To the person who is writing the proof, what they are saying may have become clear, because they have found the right way to think about it. They have found the light switch, to use a metaphor of Andrew Wiles, and can see the furniture for what it is, while the rest of us are groping around in the dark and aren't even sure if this four-legged wooden object is the same four legged wooden object we bumped into half an hour ago. My job, as a lecturer, is to try to see things from your point of view as well as from my own, and to help you find your own light switches - which may be in different places from mine. But this will also become your job. You have to learn to write a clear account, taking into account where misunderstanding can occur, and what may require explanation even though you find it obvious.

In fact, the word "obvious" covers up more mistakes in mathematics than any other. *Try to use it only where what is obvious is not the truth of the statement in question, but its proof.*

Mathematics is certainly a subject in which one can make mistakes. To recognise a mistake, one must have a rigorous criterion for truth, and mathematics does. This possibility of getting it wrong (of "being wrong") is what puts many people off the subject, especially at school, with its high premium on getting good marks[1] . Mathematics has its unique form of stressfulness.

But it is also the basis for two very undeniably good things: the possibility of agreement, and the development of humility in the face of the facts, the recognition that one was mistaken, and can now move on. As Ian Stewart puts it,

> When two members of the Arts Faculty argue, they may find it impossible to reach a resolution. When two mathematicians argue — and they do, often in a highly emotional and aggressive way — suddenly one will stop, and say 'I'm sorry, you're quite right, now I see my mistake.' And they will go off and have lunch together, the best of friends.[2]

I hope that during your mathematical degree at Warwick you enjoy the intellectual and spiritual benefits of mathematics more than you suffer from its stressfulness.

Note on Exercises The exercises handed out each week are also interspersed through the text here, partly in order to prompt you to do them at the best moment, when a new concept or technique needs practice or a proof needs completing. There should be some easy ones and some more difficult ones. Don't be put off if you can't do them all.

1.1 Other reading

It's always a good idea to get more than one angle on a subject, so I encourage you to read other books, especially if you have difficulty with any of the topics dealt with here. For a very good introduction to a lot of first year algebra, and more besides, I recommend *Algebra and Geometry*, by Alan Beardon, (Cambridge University Press, 2005). Another, slightly older, introduction to university maths is *Foundations of Mathematics* by Ian Stewart and David Tall, (Oxford University Press, 1977). The rather elderly textbook *One-variable calculus with an introduction to linear algebra*, by Tom M. Apostol, (Blaisdell, 1967) has lots of superb

[1] which, for good or ill, we continue at Warwick. Other suggestions are welcome - seriously.

[2] in *Letters to a Young Mathematician*, Basic Books 2007

exercises. In particular it has an excellent section on induction, from where I have taken some exercises for the first sheet.

Apostol and Stewart and Tall are available in the university library. Near them on the shelves are many other books on related topics, many of them at a similar level. It's a good idea to develop your independence by browsing in the library and looking for alternative explanations, different takes on the subject, and further developments and exercises.

Richard Gregory's classic book on perception, *Eye and Brain*, shows a drawing of an experiment in which two kittens are placed in small baskets suspended from a beam which can pivot horizontally about its midpoint. One of the baskets, which hangs just above the floor, has holes for the kitten's legs. The other basket, hanging at the same height, has no holes. Both baskets are small enough that the kittens can look out and observe the room around them. The kitten whose legs poke out can move its basket, and, in the process, the beam and the other kitten, by walking on the floor. The apparatus is surrounded by objects of interest to kittens. Both look around intently. As the walking kitten moves in response to its curiosity, the beam rotates and the passenger kitten also has a chance to study its surroundings. After some time, the two kittens are taken out of the baskets and released. By means of simple tests, it is possible to determine how much each has learnt about its environment. They show that the kitten which was in control has earned very much more than the passenger.

2 Natural numbers, Proof by Induction and the Fundamental Theorem of Arithmetic

The first mathematical objects we will discuss are the natural numbers $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ and the integers $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, 3, , \ldots\}$. Some people say 0 is not a natural number. Of course, this is a matter of preference and nothing more. I assume you are familiar with the arithmetic operations $+, -, \times$ and $\div$ (also written /). One property of these operations that we will use repeatedly is

Division with remainder. If m, n are natural numbers with $n > 0$ then there exist natural numbers q, r such that

$$m = qn + r \quad with \quad 0 \leq r < n. \tag{1}$$

This is probably so ingrained in your experience that it is hard to answer the question "Why is this so?". But it's worth asking, and trying to answer. We'll come back to it.

Although in this sense any natural number (except 0) can divide another, we will only say that one number divides another if it does so exactly, without remainder. More precisely, n divides m if there exists a natural number q such that $m = qn$. Thus, 3 divides 24 and 5 doesn't. We sometimes use the notation $n \mid m$ to mean that n divides m, and $n \nmid m$ to indicate that n does not divide m.

Proposition 2.1. *Let a, b, c be natural numbers. If $a \mid b$ and $b \mid c$ then $a \mid c$.*

Proof. That $a \mid b$ and $b \mid c$ means that there are natural numbers q_1 and q_2 such that $b = q_1 a$ and $c = q_2 b$. It follows that $c = q_1 q_2 a$, and since $q_1 q_2 \in \mathbb{N}$ this gives $a \mid c$. □

The sign □ here means "end of proof". Old texts use QED.

Proposition 2.1 is often referred to as the "transitivity of divisibility".

Shortly we will prove Theorem 1.2, the infinity of the primes. However it turns out that we need the following preparatory step:

Lemma 2.2. *Every natural number greater than 1 is divisible by some prime number.*

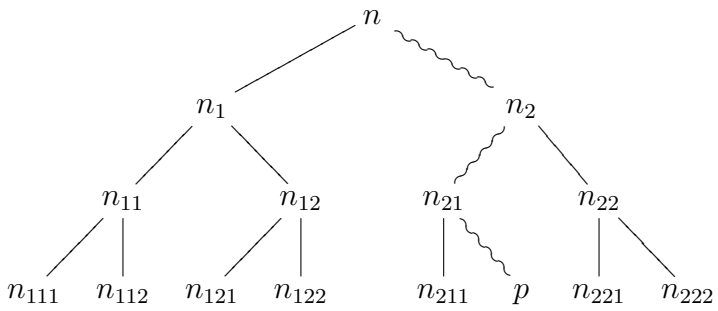
Proof. Let n be a natural number. If n is itself prime, then because $n \mid n$, the statement of the lemma holds. If n is not prime, then it is a product $n_1 \times n_2$, with n_1 and n_2 both smaller than n. If n_1 or n_2 is prime, then we've won and we stop. If not, each can be written as the product of two still smaller numbers;

$$n_1 = n_{11} n_{12}, \qquad n_2 = n_{21} n_{22}.$$

If any of $n_{11}, \ldots, n_{22}$ is prime, then by the transitivity of divisibility (Proposition 2.1) it divides n and we stop. Otherwise, the process goes on and on, with the factors getting smaller and smaller. So it has to stop at some point - after fewer than n steps, indeed. The only way it can stop is when one of the factors is prime, so this must happen at some point. Once again, by transitivity this prime divides n.

In the following diagram the process stops after two iterations, p is a prime, and the wavy line means "divides". As $p \mid n_{21}$, $n_{21} \mid n_2$ and $n_2 \mid n$, it follows by the transitivity of

divisibility, that $p \mid n$.



□

The proof just given is what one might call a discovery-type proof: its structure is very similar to the procedure by which one might actually set about finding a prime number dividing a given natural number n. But it's a bit messy, and needs some cumbersome notation — n_1 and n_2 for the first pair of factors of n, n_{11}, n_{12}, n_{21} and n_{22} for their factors, $n_{111}, \ldots, n_{222}$ for *their* factors, and so on. Is there a more elegant way of proving it? I leave this question for later.

Now we prove Theorem 1.2, the infinity of the primes. The idea on which the proof is based is very simple: if I take any collection of natural numbers, for example $3, 5, 6$ and 12, multiply them all together, and add 1, then the result is not divisible by any of the numbers I started with. That's because the remainder on division by any of them is 1: for example, if I divide $1081 = 3 \times 5 \times 6 \times 12 + 1$ by 5, I get

$$1081 = 5 \times (3 \times 6 \times 12) + 1 = 5 \times 216 + 1.$$

Proof of Theorem 1.2: Suppose that $p_1, \ldots, p_n$ is any list of prime numbers. We will show that there is another prime number not in the list. This implies that how ever many primes you might have found, there's always another. In other words, the number of primes is infinite (*in finite* means literally *unending*).

To prove the existence of another prime, consider the number $p_1 \times p_2 \times \cdots \times p_n + 1$. By the lemma, it is divisible by some prime number (possibly itself, if it happens to be prime). As it is not divisible by any of $p_1, \ldots, p_n$, because division by any of them leaves remainder 1, any prime that divides it comes from outside our list. Thus our list does not contain all the primes. □

This proof was apparently known to Euclid.

2.1 The Well-Ordering Principle

We now go on to something rather different. The following property of the natural numbers is fundamental:

The Well-Ordering Principle (WOP). Every non-empty subset of $\mathbb{N}$ has a least element.

Here we say that n is a least element of the set $S \subseteq \mathbb{N}$ if $n \in S$ and $n \leq m$ for any $m \in S$.

Does a similar statement hold with $\mathbb{Z}$ in place of $\mathbb{N}$? With $\mathbb{Q}$ in place of $\mathbb{N}$? With the non-negative rationals $\mathbb{Q}_{\geq 0}$ in place of $\mathbb{N}$?

Example 2.3. We use the Well-Ordering Principle to give a shorter and cleaner proof of Lemma 2.2. Denote by S the set of natural numbers greater than 1 which are *not* divisible by any prime. We have to show that S is empty, of course. If it is not empty, then by the Well-Ordering Principle it has a least element, say n_0. Now $n_0 > 1$ and either n_0 is prime, or it is not.

If n_0 is prime, then it certainly has a prime factor, namely itself. But this contradicts the fact that $n \in S$ while S only contains numbers with no prime factors.

So n_0 is not prime, and hence we can write it as a product, $n_0 = n_1 n_2$, with both n_1 and n_2 smaller than n_0 and bigger than 1. But then neither can be in S, (since n_0 was the smallest element of S) and so each is divisible by a prime. But any prime dividing either n_1 or n_2 will also divide n_0. Once again, n_0 is divisible by a prime, and we have a contradiction.

So in all cases, we derive an absurdity from the supposition that S has a least element n_0. Since $S \subset \mathbb{N}$, if not empty it must have a least element. Therefore the only possibility is that S is empty. □

Exercise 2.1. *The Well-Ordering Principle can be used to give an even shorter proof of Lemma 2.2. Can you find one? Hint: take, as S, the set of all factors of n which are > 1.*

The logical structure of the second proof of Lemma 2.2 is to imagine that the negation of what we want to prove is true, and then to derive a contradiction from this supposition. We are left with no alternative to the statement we want to prove. A proof with this logical structure is known as a proof by contradiction. It's something we use everyday: when faced with a choice between two alternative statements, we believe the one that is more believable. If one of the two alternatives we are presented with has unbelievable consequences, we reject it and believe the other.

A successful Proof by Contradiction in mathematics offers you the alternative of believing either the statement you set out to prove, or something whose falsity is indisputable. Typically, this falsehood will be of something like "the number n is and is not prime", which is false for obvious logical reasons. Or, later, when you've built up a body of solid mathematical knowledge, the falsehood might be something you know not to be true in view of that knowledge, like "27 is a prime number". We will use Proof by Contradiction many times.

The Well-Ordering Principle has the following obvious generalisation:

Fact. *Any subset T of the integers $\mathbb{Z}$ which is bounded below, has a least element.*

That T be *bounded below* means that there is some integer less than or equal to all the members of T. Such an integer is called a **lower bound** for T. For example, the set $\{-34, -33, \ldots\}$ is bounded below, by -34, or by -162 for that matter. The set $T := \{n \in \mathbb{Z} : n^2 < 79\}$ is also bounded below. For example, -10 is a lower bound, since if $n < -10$ then $n^2 > 100$, so that $n \notin T$, and it therefore follows that all of the members of T must be no less than -10.

Exercise 2.2. *What is the least element of $\{n \in \mathbb{N} : n^2 < 79\}$? What is the least element of $\{n \in \mathbb{N} : n^2 > 79\}$?*

The Well-Ordering Principle is at the root of the Principle of Induction (or mathematical induction), a method of proof you may well have met before. We state it first as a peculiarly bland fact about subsets of $\mathbb{N}$. Its import will become clear in a moment.

Principle of Induction (POI). Suppose that $T \subseteq \mathbb{N}$, and that

Property 1: $0 \in T$, and

Property 2: For every natural number $n \geq 1$, if $n-1 \in T$ then $n \in T$.

Then $T = \mathbb{N}$.

Proof. This follows easily from the Well-Ordering Principle. Consider the complement[3] $S = \mathbb{N} \setminus T$ of T in $\mathbb{N}$. If S is not empty then by the WOP it has a least element, call it n_0. As we are told (Property 1 of T) that $0 \in T$, certainly $0 \notin S$, so n_0 must be greater than 0, so $n_0 \geq 1$. By definition of n_0 as the smallest natural number not in T, $n_0 - 1$ must be in T. But then by Property 2 of T, $(n_0 - 1) + 1$ is in T also. That is, $n_0 \in T$. This contradiction ($n_0 \notin T$ and $n_0 \in T$) is plainly false, so we are forced to return to our starting assumption, that $\mathbb{N} \setminus T \neq \emptyset$, and reject it. It can't be true, as it has an unbelievable consequence. □

How does the Principle of Induction give rise to a method of proof?

Example 2.4. You may well know the formula

$$1 + 2 + \cdots + n = \frac{1}{2}n(n+1). \tag{2}$$

Here is a proof that it is true for all $n \in \mathbb{N}$, using the POI.

For each integer n, either the equality (2) holds, or it does not. Let T be the set of those n for which it is true:

$$T = \{n \in \mathbb{N} : \text{equality (2) holds}\}.$$

We want to show that T is all of $\mathbb{N}$. First of all, (2) holds[4] for $n = 0$, so T has Property 1.

Now we check that it has Property 2. If (2) is true for $n-1$, then using the truth of (2) for $n-1$, we get

$$1 + \cdots + n = 1 + \cdots + (n-1) + n \tag{3}$$

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

This is equal to

$$\frac{1}{2}\big((n-1)n + 2n\big) = \frac{1}{2}n(n+1).$$

So if (2) holds for $n-1$ then it holds for n. Thus, T has Property 2 as well, and therefore by the POI, T is all of $\mathbb{N}$. In other words, (2) holds for all $n \in \mathbb{N}$. □

The Principle of Induction is often stated like this: let $P(n)$ be a series of statements, one for each natural number n. (The equality (2) is an example.) If

Property 1': $P(0)$ holds, and

Property 2': Whenever $P(n)$ holds then $P(n+1)$ holds also,

[3] If A is a set and B a subset of A then the *complement of B in A*, written $A \setminus B$, is the set $\{x \in A : x \notin B\}$.

[4] When $n = 0$ the sum on the left is empty so has value 0. If you don't like this, start with $n = 1$.

then $P(n)$ holds for all $n \in \mathbb{N}$.

The previous version implies this version—just take, as T, the set of n for which $P(n)$ holds. This second version is how we usually use induction when proving something. If it is more understandable than the first version, this is probably because it is more obviously useful. The first version, though simpler, may be harder to understand because it is not at all clear what use it is or why we are interested in it.

Example 2.5. We use induction to prove that for all $n \geq 1$,

$$1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2.$$

First we check that it is true for $n = 1$ (the *initial step* of the induction). This is trivial - on the left hand side we have 1^3 and on the right 1^2.

Next we check that **if** it is true for n, **then** it is true for $n + 1$. This is the heart of the proof, and is usually known as the *induction step*. To prove that $P(n)$ implies $P(n+1)$, we assume $P(n)$ and show that $P(n+1)$ follows. Careful! Assuming $P(n)$ is not the the same as assuming that $P(n)$ is true for all n. What we are doing is showing that if, for some value n, $P(n)$ holds, then necessarily $P(n+1)$ holds also.

To proceed: we have to show that if

$$1^3 + \cdots + n^3 = (1 + \cdots + n)^2 \tag{5}$$

then

$$1^3 + \cdots + (n+1)^3 = (1 + \cdots + (n+1))^2. \tag{6}$$

In practice, we try to transform one side of (6) into the other, making use of (5) at some point along the way. It's not always clear which side to begin with. In this example, I think it's easiest like this:

$$(1+\cdots(n+1))^2 = \big((1+\cdots+n)+(n+1)\big)^2 = (1+\cdots+n)^2 + 2(1+\cdots+n)(n+1) + (n+1)^2.$$

By the equality proved in the previous example, $(1 + \cdots + n) = \frac{1}{2}n(n+1)$, so the middle term on the right is $n(n+1)^2$. So the whole right hand side is

$$(1 + \cdots + n)^2 + n(n+1)^2 + (n+1)^2 = (1 + \cdots + n)^2 + (n+1)^3.$$

Using the induction hypothesis (5), the first term here is equal to $1^3 + \cdots + n^3$. So we have shown that *if* (5) holds, *then* (6) holds. Together with the initial step, this completes the proof.

Exercise 2.3. Use induction to prove the following formulae:

1.
$$1^2 + 2^2 + \cdots + n^2 = \frac{1}{6}n(n+1)(2n+1) \tag{7}$$

2.
$$1 + 3 + 5 + 7 + \cdots + (2n+1) = (n+1)^2 \tag{8}$$

Exercise 2.4. (i) Prove for all $n \in \mathbb{N}$, $10^n - 1$ is divisible by 9.

(ii) There is a well-known rule that a natural number is divisible by 3 if and only if the sum of the digits in its decimal representation is divisible by 3. Part (i) of this exercise is the

first step in a proof of this fact. Can you complete the proof? Hint: the point is to compare the two numbers

$$k_0 + k_1 \times 10 + k_2 \times 10^2 + \cdots + k_n \times 10^n$$

and

$$k_0 + k_1 + \cdots + k_n.$$

(iii) Is a rule like the rule in (ii) true for divisibility by 9?

Exercise 2.5. (Taken from Apostol, Calculus, Volume 1)
(i) Note that

$$1 = 1$$
$$1 - 4 = -(1 + 2)$$
$$1 - 4 + 9 = 1 + 2 + 3$$
$$1 - 4 + 9 - 16 = -(1 + 2 + 3 + 4).$$

Guess the general law and prove it by induction.

(ii) Note that

$$\begin{array}{rrrcl} & & 1 - \frac{1}{2} & = & \frac{1}{2} \\ & (1 - \frac{1}{2}) & (1 - \frac{1}{3}) & = & \frac{1}{3} \\ (1 - \frac{1}{2}) & (1 - \frac{1}{3}) & (1 - \frac{1}{4}) & = & \frac{1}{4} \end{array}$$

Guess the general law and prove it by induction.

(iii) Guess a general law which simplifies the product

$$\big(1 - \frac{1}{4}\big)\big(1 - \frac{1}{9}\big)\big(1 - \frac{1}{16}\big)\cdots\big(1 - \frac{1}{n^2}\big)$$

and prove it by induction.

Induction works fine once you have the formula or statement you wish to prove, but relies on some other means of obtaining it in the first place. There's nothing wrong with intelligent guesswork, but sometimes a more scientific procedure is needed. Here is a method for finding formulae for the sum of the first n cubes, fourth powers, etc. It is cumulative, in the sense that to find a formula for the first n cubes, you need to know formulae for the first n first powers and the first n squares, and then to find the formula for the first n fourth powers you need to know the formulae for first, second and third powers, etc. etc.

The starting point for the formula for the first n cubes is that

$$(k-1)^4 = k^4 - 4k^3 + 6k^2 - 4k + 1,$$

from which it follows that

$$k^4 - (k-1)^4 = 4k^3 - 6k^2 + 4k - 1.$$

We write this out n times:

$$\begin{array}{lcllcllcllcl} n^4 & - & (n-1)^4 & = & 4n^3 & - & 6n^2 & + & 4n & - & 1 \\ (n-1)^4 & - & ((n-1)-1)^4 & = & 4(n-1)^3 & - & 6(n-1)^2 & + & 4(n-1) & - & 1 \\ \cdots & \cdot & \cdots & \cdot & \cdots & \cdots & \cdot & \cdots & \cdot & \cdots & \\ k^4 & - & (k-1)^4 & = & 4k^3 & - & 6k^2 & + & 4k & - & 1 \\ \cdots & \cdot & \cdots & \cdot & \cdots & \cdots & \cdot & \cdots & \cdot & \cdots & \\ 1^4 & - & 0^4 & = & 4(1)^3 & - & 6(1)^2 & + & 4 \cdot 1 & - & 1 \end{array} \tag{9}$$

Now add together all these equations to get one big equation: the sum of all the left hand sides is equal to the sum of all the right hand sides. On the left hand side there is a "telescopic cancellation": the first term on each line (except the first) cancels with the second term on the line before, and we are left with just n^4. On the right hand side, there is no cancellation. Instead, we are left with

$$4\sum_{k=1}^{n} k^3 - 6\sum_{k=1}^{n} k^2 + 4\sum_{k=1}^{n} k - n.$$

Equating right and left sides and rearranging, we get

$$\sum_{k=1}^{n} k^3 = \frac{1}{4}\big(n^4 + 6\sum_{k=1}^{n} k^2 - 4\sum_{k=1}^{n} k + n\big).$$

If we input the formulae for $\sum_{k=1}^{n} k$ and $\sum_{k=1}^{n} k^2$ that we already have, we arrive at a formula for $\sum_{k=1}^{n} k^3$.

Exercise 2.6. 1. Complete this process to find an explicit formula for $\sum_{k=1}^{n} k^3$.

2. Check your answer by induction.

3. Use a similar method to find a formula for $\sum_{k=1}^{n} k^4$.

4. Check it by induction.

At the start of this section I stated the rule for division with remainder and asked you to prove it.

Proposition 2.6. *If m and n are natural numbers with $n > 0$, there exist natural numbers q, and r, with $0 \leq r < n$, such that $m = qn + r$.*

Proof. Consider the set $\{r \in \mathbb{N} : r = m - qn \text{ for some } q \in \mathbb{N}\}$. Call this set R (for "Remainders"). By the Well-Ordering Principle, R has a least element, r_0, equal to $m - q_0 n$ for some $q_0 \in \mathbb{N}$. We want to show that $r_0 < n$, for then we will have $m = q_0 n + r_0$ with $0 \leq r_0 < n$, as required.

Suppose, to the contrary, that $r_0 \geq n$. Then $r_0 - n$ is still in $\mathbb{N}$, and, as it is equal to $m - (q_0 + 1)n$, is in R. This contradicts the definition of r_0 as the least element of R. We are forced to conclude that $r_0 < n$. □

2.2 The Fundamental Theorem of Arithmetic

Here is yet another slightly different Principle of Induction:

Principle of Induction II. Suppose that $T \subseteq \mathbb{N}$ and that

1. $0 \in T$, and
2. for every natural number n, **if** $0, 1, \ldots, n-1$ are all in T, **then** $n \in T$.

Then T is all of $\mathbb{N}$.

Proof. Almost the same as the proof of the previous POI. As before, if T is not all of $\mathbb{N}$, i.e. if $\mathbb{N} \setminus T \neq \emptyset$, let n_0 be the least member of $\mathbb{N} \setminus T$. Then $0, \ldots, n_0 - 1$ must all be in T; so by Property 2, $n_0 \in T$. □

We will use this shortly to prove some crucial facts about factorisation.

Remark 2.7. The Principle of Induction has many minor variants; for example, in place of Property 1, we might have the statement

Property 1' $3 \in T$

From this, and the same Property 2 as before, we deduce that T contains all the natural numbers greater than or equal to 3.

Theorem 2.8. (The "Fundamental Theorem of Arithmetic").

(i) Every natural number greater than 1 can be written as a product of prime numbers.

(ii) Such a factorisation is unique, except for the order of the terms.

I clarify the meaning of (ii): a factorisation of a natural number n consists of an expression $n = p_1 \ldots p_s$ where each p_i is a prime number. Note that $s = 1$ is allowed, when n is itself prime (a "product" of one prime). Uniqueness of the prime factorisation of n, up to the order of its terms, means that if $n = p_1 \ldots p_s$ and also $n = q_1 \ldots q_t$, then $s = t$ and the list $q_1, \ldots, q_s$ can be obtained from the list $p_1, \ldots, p_s$ by re-ordering.

Proof. *Existence of the factorisation:* We use induction, in fact POI II. The statement is trivially true for the first number we come to, 2, since 2 is prime. In fact (and this will be important in a moment), it is trivially true for *every* prime number.

Now we have to show that the set of natural numbers which can be written as a product of primes has property 2 of the POI. This is called "making the induction step". Suppose that every natural number between 2 and n has a factorisation as a product of primes. We have to show that from this it follows that $n+1$ does too. There are two possibilities: $n+1$ is prime, or it is not.

- If $n+1$ is prime, then it does have a factorisation as a product of primes (one prime!).
- If $n+1$ is not prime, then $n+1 = qr$ where q and r are both natural numbers greater than 1 and less than $n+1$. Hence $2 \leq q, r \leq n$. So q is a product of primes, and so is r, *by the induction hypothesis*; putting these two factorisations together, we get an expression for $n+1$ as a product of primes.

In either case, we have seen that **if** the numbers $2, \ldots, n$ can each be written as a product of primes, **then** so can $n+1$. Thus the set of natural numbers which can be written as a product of primes has property 2. As it has property 1 (but with the natural number 2 in place of the natural number 0), by POI II, it must be all of $\{n \in \mathbb{N} : n \geq 2\}$.

Notice that we have used POI II here; POI I would not do the job. Knowing that n has a factorisation as a product of primes does not enable us to express $n+1$ as a product of primes — we needed to use the fact that any two non-trivial factors of a non-prime $n+1$ could be written as a product of primes, and so we needed to know that any two natural numbers less than $n+1$ had this property.

Uniqueness of the factorisation Again we use POI II. Property 1 certainly holds: 2 has a unique prime factorisation; indeed, any product of two or more primes must be greater than 2. Now we show that Property 2 also holds. Suppose that each of the numbers $2, \ldots, n$ has a *unique* prime factorisation. We must show that so does $n+1$. Suppose

$$n+1 = p_1 \ldots p_s = q_1 \ldots q_t \tag{10}$$

where each of the p_i and q_j is prime. By reordering each side, we may assume that $p_1 \leq p_2 \leq \cdots \leq p_s$ and $q_1 \leq q_2 \leq \cdots q_t$. We consider two cases:

- $p_1 = q_1$, and
- $p_1 \neq q_1$

In the first case, dividing the equality $p_1 \cdots p_s = q_1 \cdots q_t$ by p_1, we deduce that $p_2 \cdots p_s = q_2 \ldots q_t$. As $p_1 > 1$, $p_2 \cdots p_t < n+1$ and so must have a unique prime factorisation, by our supposition. Therefore $s = t$ and, since we have written the primes in increasing order, $p_2 = q_2, \ldots, p_s = q_s$. Since also $p_1 = q_1$, the two factorisations of $n+1$ coincide, and $n+1$ has a unique prime factorisation.

In the second case, suppose $p_1 < q_1$. Then

$$\begin{aligned} p_1(p_2 \cdots p_s - q_2 \cdots q_t) &= p_1 p_2 \cdots p_s - p_1 q_2 \cdots q_t \\ &= q_1 \cdots q_t - p_1 q_2 \cdots q_t \\ &= (q_1 - p_1) q_2 \cdots q_t \end{aligned} \tag{11}$$

Let $r_1 \ldots r_u$ be a prime factorisation of $q_1 - p_1$; putting this together with the prime factorisation $q_2 \ldots q_t$ gives a prime factorisation of the right hand side of (11) and therefore of its left hand side, $p_1(p_2 \ldots p_s - q_2 \ldots q_t)$. As this number is less than $n+1$, its prime factorisation is unique (up to order), by our inductive assumption. It is clear (from the left side) that p_1 is one of its prime factors; hence p_1 must be *either* a prime factor of $q_1 - p_1$ (that is, one of the r_j) *or* equal to one of $q_2, \ldots, q_t$. But p_1 is not equal to any of the q_j, because $p_1 < q_1 \leq q_2 \leq \cdots \leq q_t$. So it must be one of the r_j, a prime factor of $q_1 - p_1$. But this means that p_1 divides q_1, which is absurd since q_1 is a prime and $1 < p_1 < q_1$. This absurdity leads us to conclude that p_1 *cannot be* less than q_1.

The same argument, with the roles of the p's and q's reversed, shows that it is also impossible to have $p_1 > q_1$. The proof is complete. □

The Fundamental Theorem of Arithmetic allows us to speak of "the prime factorisation of n" and "the prime factors of n" without ambiguity.

Corollary 2.9. *If the prime number p divides the product of natural numbers m and n, then $p \mid m$ or $p \mid n$.*

Proof. By putting together a prime factorisation of m and a prime factorisation of n, we get a prime factorisation of mn. The prime factors of mn are therefore the prime factors of

m together with the prime factors of n. As p is one of them, it must be among the prime factors of m or the prime factors of n. □

Lemma 2.10. *If ℓ, m and n are positive natural numbers and $m \mid n$, then the highest power of ℓ to divide m is less than or equal to the highest power of ℓ to divide n.*

Proof. If $\ell^k \mid m$ and $m \mid n$ then $\ell^k \mid n$, by transitivity of division. □

We will shortly use this result in the case where ℓ is prime.

Definition 2.11. *Let m and n be positive natural numbers. The **highest common factor** of m and n (denoted* $\mathrm{hcf}(m,n)$*) is the largest number to divide both m and n. (A common alternative name is the **Greatest Common Divisor**, written* $\gcd(m,n)$*.) The **lowest common multiple** of m and n (denoted* $\mathrm{lcm}(m,n)$*) is the least positive number divisible by both m and n.*

That there should exist a lowest common multiple follows immediately from the Well-Ordering Principle: it is the least element of the set S of positive numbers divisible by both m and n, which is non-empty since it contains mn. The existence of a highest common factor does not require the Well Ordering Principle, since the sets of divisors of m and n are **finite** (and both contain 1).

It is convenient to extend the definitions of hcf and lcm to all of $\mathbb{N}$ by setting $\mathrm{hcf}(n,0) = \mathrm{hcf}(0,n) = n$ and $\mathrm{lcm}(n,0) = \mathrm{lcm}(0,n) = 0$ for all $n \geq 0$. (In the next chapter we'll extend them again to allow negative m, n.)

There are easy[5] procedures for finding the hcf and lcm of two natural numbers, using their prime factorisations. First an example:

$$720 = 2^4 \times 3^2 \times 5 \qquad \text{and} \qquad 350 = 2 \times 5^2 \times 7$$

$$\mathrm{hcf}(720, 350) = 2 \times 5, \qquad \text{and} \qquad \mathrm{lcm}(720, 350) = 2^4 \times 3^2 \times 5^2 \times 7.$$

In preparation for an explanation and a universal formula, we rewrite this as

$$\begin{array}{lcccccccc} 720 & = & 2^4 & \times & 3^2 & \times & 5^1 & \times & 7^0 \\ 350 & = & 2^1 & \times & 3^0 & \times & 5^2 & \times & 7^1 \\ \mathrm{hcf}(720,350) & = & 2^1 & \times & 3^0 & \times & 5^1 & \times & 7^0 \\ \mathrm{lcm}(720,350) & = & 2^4 & \times & 3^2 & \times & 5^2 & \times & 7^1 \end{array}$$

Proposition 2.12. *If*

$$\begin{array}{rcccccccccc} m & = & 2^{i_2} & \times & 3^{i_3} & \times & 5^{i_5} & \times & \cdots & \times & p_r^{i_{p_r}} \\ n & = & 2^{j_2} & \times & 3^{j_3} & \times & 5^{j_5} & \times & \cdots & \times & p_r^{j_{p_r}} \end{array}$$

(with exponents ≥ 0), then

$$\mathrm{hcf}(m,n) = 2^{\min\{i_2,j_2\}} \times 3^{\min\{i_3,j_3\}} \times 5^{\min\{i_5,j_5\}} \times \cdots \times p_r^{\min\{i_{p_r},j_{p_r}\}},$$

$$\mathrm{lcm}(m,n) = 2^{\max\{i_2,j_2\}} \times 3^{\max\{i_3,j_3\}} \times 5^{\max\{i_5,j_5\}} \times \cdots \times p_r^{\max\{i_{p_r},j_{p_r}\}}.$$

[5]But deceptively easy, since finding the prime factorisations of large numbers is **not** easy! Later we will see another method for finding hcf and lcm which do not require factorisation.

Proof. If q divides both m and n then by Lemma 2.10 the power of each prime p in the prime factorisation of q is less than or equal to both i_p and j_p. Hence it is less than or equal to $\min\{i_p, j_p\}$. The *highest* common factor is thus obtained by taking precisely this power. A similar argument proves the statement for $\mathrm{lcm}(m, n)$. □

Corollary 2.13.

$$\mathrm{hcf}(m, n) \times \mathrm{lcm}(m, n) = m \times n.$$

Proof. For any two integers i, j

$$\min\{i, j\} + \max\{i, j\} = i + j.$$

When $i = i_p$ and $j = j_p$, the left hand side is the exponent of the prime p in $\mathrm{hcf}(m, n) \times \mathrm{lcm}(m, n)$ and the right hand side is the exponent of p in $m \times n$. □

Proposition 2.14. *If g is any common factor of m and n then g divides* $\mathrm{hcf}(m, n)$.

Proof. This follows directly from Proposition 2.12. □

Exercise 2.7. *There is a version of Proposition 2.14 for* lcm*s. Can you guess it? Can you prove it?*

2.3 The Euclidean Algorithm

There is another procedure for finding hcfs and lcms, known as the Euclidean Algorithm. It is based on the following lemma:

Lemma 2.15. *If $m = qn + r$, then* $\mathrm{hcf}(n, m) = \mathrm{hcf}(n, r)$.

Proof. If d divides both n and m then it follows from the equation $m = qn + r$ that d also divides r. Hence,

$$d \mid m \quad \& \quad d \mid n \quad \Longrightarrow \quad d \mid n \quad \& \quad d \mid r$$

Conversely, if $d \mid n$ and $d \mid r$ then d also divides m. Hence

$$d \mid m \quad \& \quad d \mid n \quad \Longleftrightarrow \quad d \mid r \quad \& \quad d \mid n$$

In other words

$$\{d \in \mathbb{N} : d \mid m \quad \& \quad d \mid n\} = \{d \in \mathbb{N} : d \mid n \quad \& \quad d \mid r\}$$

So the greatest elements of the two sets are equal. □

Example 2.16. (i) We find $\mathrm{hcf}(365, 748)$. Long division gives

$$748 = 2 \times 365 + 18$$

so

$$\mathrm{hcf}(365, 748) = \mathrm{hcf}(365, 18).$$

Long division now gives

$$365 = 20 \times 18 + 5,$$

so

$$\mathrm{hcf}(365, 748) = \mathrm{hcf}(365, 18) = \mathrm{hcf}(18, 5).$$

At this point we can probably recognise that the hcf is 1. But let us go on anyway.

$$18 = 3 \times 5 + 3 \quad \Longrightarrow \quad \mathrm{hcf}(365, 748) = \mathrm{hcf}(18, 5) = \mathrm{hcf}(5, 3).$$

$$5 = 1 \times 3 + 2 \quad \Longrightarrow \quad \mathrm{hcf}(365, 748) = \mathrm{hcf}(3, 2)$$

$$3 = 1 \times 2 + 1 \quad \Longrightarrow \quad \mathrm{hcf}(365, 748) = \mathrm{hcf}(2, 1)$$

$$2 = 2 \times 1 + 0 \quad \Longrightarrow \quad \mathrm{hcf}(365, 748) = \mathrm{hcf}(2, 1) = 1.$$

The hcf is *the last non-zero remainder* in this process.

(ii) We find $\mathrm{hcf}(365, 750)$.

$$\begin{array}{rcrcl} 750 & = & 2 \times 365 + 20 & \Longrightarrow & \mathrm{hcf}(365, 750) = \mathrm{hcf}(365, 20) \\ 365 & = & 18 \times 20 + 5 & \Longrightarrow & \mathrm{hcf}(365, 750) = \mathrm{hcf}(20, 5) \end{array}$$

Now something different happens:

$$20 = 4 \times 5 + 0.$$

What do we conclude from this? Simply that $5 \mid 20$, and thus that $\mathrm{hcf}(20, 5) = 5$. So $\mathrm{hcf}(365, 750) = \mathrm{hcf}(20, 5) = 5$. Again, *the hcf is the last non-zero remainder in this process.* This is always true; given the chain of equalities

$$\mathrm{hcf}(n, m) = \cdots = \mathrm{hcf}(r_k, r_{k+1}),$$

the fact that

$$r_k = q r_{k+1} + 0$$

(i.e. r_{k+1} is the last non-zero remainder) means that $\mathrm{hcf}(r_k, r_{k+1}) = r_{k+1}$, and so $\mathrm{hcf}(m, n) = r_{k+1}$.

The Euclidean Algorithm is a vastly more efficient method of finding hcfs than the factorisation method when the numbers concerned are large. You should only use the factorisation method when the numbers are small enough for their prime factorisations to be obvious.

Exercise 2.8. *Find the hcf and lcm of*

1. $10^6 + 144$ *and* 10^3
2. $10^6 + 144$ *and* $10^3 - 12$
3. 90090 *and* 2200.

3 Integers and Modular Arithmetic

The set of integers, $\mathbb{Z}$, consists of the natural numbers together with their negatives and the number 0:

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots,\}.$$

If m and n are integers, just as with natural numbers we say that n divides m if there exists $q \in \mathbb{Z}$ such that $m = qn$. The notions of hcf and lcm can be generalised from $\mathbb{N}$ to $\mathbb{Z}$ without much difficulty, though we have to be a little careful. For example, if we allow negative multiples, then there is no longer a *lowest* common multiple of two integers. For example, -10 is a common multiple of 2 and 5; but so are -100 and -1000. We can avoid the difficulty by setting

$$\mathrm{hcf}(m, n) = \mathrm{hcf}(|m|, |n|) \qquad \text{and} \qquad \mathrm{lcm}(m, n) = \mathrm{lcm}(|m|, |n|)$$

for $m, n \in \mathbb{Z}$. So (for non-zero m, n) $\mathrm{lcm}(m, n)$ is the lowest *positive* common multiple of m and n.

3.1 Subgroups of $\mathbb{Z}$

The following special subsets of $\mathbb{Z}$ will play a major role in what follows.

Definition 3.1. *A subset of $\mathbb{Z}$ is called a subgroup*[6] *if it is nonempty, and the sum and difference of any two of its members is also a member.*

Obvious examples include $\mathbb{Z}$ itself, the set of even integers, which we denote by $2\mathbb{Z}$, the set of integers divisible by 3, $3\mathbb{Z}$, and in general the set of integers divisible by n (for a fixed n) which is denoted $n\mathbb{Z}$. In fact we'll soon show (Proposition 3.2) that these are the only examples. First note that from the definition it easily follows that for any subgroup S:

- $0 \in S$;
- if $a \in S$ then also $-a \in S$;
- if $a \in S$ then every multiple of a is in S, i.e. $a\mathbb{Z} \subseteq S$.

Proposition 3.2. *If $S \subseteq \mathbb{Z}$ is a subgroup, then there is a natural number g such that $S = g\mathbb{Z} = \{gn : n \in \mathbb{Z}\}$.*

Proof. If $S = \{0\}$, we simply take $g = 0$. Otherwise, S contains at least one strictly positive number (since $a \in S \Longleftrightarrow -a \in S$). Let S_+ be the set of strictly positive members of S, and let g be the smallest member of S_+ (which exists by the WOP). I claim that $S = g\mathbb{Z}$.

Proving this involves proving the inclusions $g\mathbb{Z} \subseteq \mathbb{Z}$ and $S \subseteq g\mathbb{Z}$. The first is easy: as S is closed under addition, it contains all positive (integer) multiples of g, and as it is closed under subtraction it contains 0 and all negative integer multiples of g also.

To prove the opposite inclusion, suppose that $n \in S$. Then unless $n = 0$ (in which case $n = 0 \times g \in g\mathbb{Z}$), either n or $-n$ is in S_+.

Suppose that $n \in S_+$. We can write $n = qg + r$ with $q \geq 0$ and $0 \leq r < g$; since $g \in S$, so is qg, and as S is closed under the operation of subtraction, it follows that $r \in S$. If $r > 0$

[6] In this course we will **not** study *groups* though they will occasionally be mentioned. You are not expected to know what they are, and don't need to, to understand the definition of "subgroup" of $\mathbb{Z}$ given here.

then r is actually in S_+. But g is the smallest member of S_+ and $r < g$, so this cannot happen, r cannot be greater than 0, so $r = 0$. Hence $n = qg \in g\mathbb{Z}$.

If $-n \in S_+$, then by the argument of the previous paragraph there is some $q \in \mathbb{N}$ such that $-n = qg$. Then $n = (-q)g$, and again lies in $g\mathbb{Z}$.

This completes the proof that $S \subseteq g\mathbb{Z}$, and thus that $S = g\mathbb{Z}$. □

We use the letter g in this theorem because g "generates" $g\mathbb{Z}$: starting just with g, by means of the operations of addition and subtraction, we get the whole subgroup $g\mathbb{Z}$.

We can express Proposition 3.2 by saying that there is a "1-1 correspondence" between subgroups of $\mathbb{Z}$ and the natural numbers:

$$\{\text{subgroups of } \mathbb{Z}\} \quad \longleftrightarrow \quad \mathbb{N} \tag{12}$$

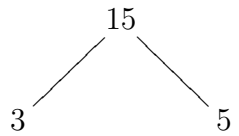
The natural number $g \in \mathbb{N}$ generates the subgroup $g\mathbb{Z}$, and different g's generate different subgroups. Moreover, by Proposition 3.2 *every* subgroup of $\mathbb{Z}$ is a $g\mathbb{Z}$ for a unique $g \in \mathbb{N}$. *Each subgroup of $\mathbb{Z}$ corresponds to a unique natural number, and vice versa.*

There is an interesting relation between divisibility of natural numbers and inclusion of the subgroups of $\mathbb{Z}$ that they generate:

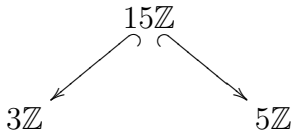
Proposition 3.3. *For any two integers m and n, m divides n if and only if $m\mathbb{Z} \supseteq n\mathbb{Z}$.*

Proof. If $m|n$, then m also divides any multiple of n, so[7] $m\mathbb{Z} \supseteq n\mathbb{Z}$. Conversely, if $m\mathbb{Z} \supseteq n\mathbb{Z}$, then in particular $n \in m\mathbb{Z}$, and so $m|n$. □

So the 1-1 correspondence (12) can be viewed as a translation from the language of natural numbers and divisibility to the language of subgroups of $\mathbb{Z}$ and inclusion. Every statement about divisibility of natural numbers can be translated into a statement about inclusion of subgroups of $\mathbb{Z}$, and vice versa. Suppose we represent the statement $m|n$ by positioning n somewhere above m and drawing a line between them, as in



("3 divides 15 and 5 divides 15"). This statement translates to



("$15\mathbb{Z}$ is contained in $3\mathbb{Z}$ and $15\mathbb{Z}$ is contained in $5\mathbb{Z}$".)

Exercise 3.1. *Draw diagrams representing all the divisibility relations between the numbers $1, 2, 4, 3, 6, 12$, and all the inclusion relations between the subgroups $\mathbb{Z}, 2\mathbb{Z}, 4\mathbb{Z}, 3\mathbb{Z}, 6\mathbb{Z}, 12\mathbb{Z}$.*

Notice that our 1-1 correspondence reverses the order: bigger natural numbers generate smaller subgroups. More precisely, if n is bigger than m in the special sense that $m|n$, then $n\mathbb{Z}$ is smaller than $m\mathbb{Z}$ in the special sense that $n\mathbb{Z} \subseteq m\mathbb{Z}$.

The following proposition follows directly from the definition of subgroup (without using Proposition 3.2).

[7] $A \supseteq B$ means the same as $B \subseteq A$; see the Notation table on the inside front cover.

Proposition 3.4. *(i) If G_1 and G_2 are subgroups of $\mathbb{Z}$, then so is their intersection $G_1 \cap G_2$, and so is the set*

$$\{m + n : m \in G_1, n \in G_2\},$$

(which we denote by $G_1 + G_2$).

(ii) *$G_1 \cap G_2$ contains every subgroup contained in both G_1 and G_2;*
$G_1 + G_2$ is contained in every subgroup containing both G_1 and G_2.

(less precisely:

$G_1 \cap G_2$ is the largest subgroup contained in G_1 and G_2;
$G_1 + G_2$ is the smallest subgroup containing both G_1 and G_2.)

Proof. (i) Both statements are straightforward. The proof for $G_1 \cap G_2$ is simply that if $m \in G_1 \cap G_2$ and $n \in G_1 \cap G_2$ then $m, n \in G_1$ and $m, n \in G_2$, so as G_1 and G_2 are subgroups, $m + n, m - n \in G_1$ and $m + n, m - n \in G_2$. But this means that $m + n$ and $m - n$ are in the intersection $G_1 \cap G_2$, so that $G_1 \cap G_2$ is a subgroup.

For $G_1 + G_2$, suppose that $m_1 + n_1$ and $m_2 + n_2$ are elements of $G_1 + G_2$, with $m_1, m_2 \in G_1$ and $n_1, n_2 \in G_2$. Then

$$(m_1 + n_1) + (m_2 + n_2) = (m_1 + m_2) + (n_1 + n_2)$$

(here the brackets are just to make reading the expressions easier; they do not change anything). Since G_1 is a subgroup, $m_1 + m_2 \in G_1$, and since G_2 is a subgroup, $n_1 + n_2 \in G_2$. Hence $(m_1 + m_2) + (n_1 + n_2) \in G_1 + G_2$.

(ii) It's obvious that $G_1 \cap G_2$ is the largest subgroup contained in both G_1 and G_2 — it's the largest sub*set* contained in both. It's no less obvious that $G_1 \cap G_2$ contains every subgroup contained in both G_1 and G_2. The proof for $G_1 + G_2$ is less obvious, but still uses just one idea. It is this: any subgroup containing G_1 and G_2 must contain the sum of any two of its members, by definition of subgroup. So in particular it must contain every sum of the form $g_1 + g_2$, where $g_1 \in G_1$ and $g_2 \in G_2$. Hence it must contain $G_1 + G_2$. Since every subgroup containing G_1 and G_2 must contain $G_1 + G_2$, $G_1 + G_2$ is the smallest subgroup containing both G_1 and G_2. □

The next theorem links this notion of subgroup to hcf and lcm:

Theorem 3.5. *Let $m, n \in \mathbb{Z}$. Then*

1. *$m\mathbb{Z} + n\mathbb{Z} = h\mathbb{Z}$, where $h = \mathrm{hcf}(m, n)$.*
2. *$m\mathbb{Z} \cap n\mathbb{Z} = \ell\mathbb{Z}$ where $\ell = \mathrm{lcm}(m, n)$.*

Proof.

(1) By Proposition 3.2 $m\mathbb{Z} + n\mathbb{Z}$ is equal to $g\mathbb{Z}$ for some natural number g. This g must be a common factor of m and n, since $g\mathbb{Z} \supseteq m\mathbb{Z}$ and $g\mathbb{Z} \supseteq n\mathbb{Z}$. But which common factor? The answer is obvious: by Proposition 3.4, $m\mathbb{Z} + n\mathbb{Z}$ is contained in every subgroup containing $m\mathbb{Z}$ and $n\mathbb{Z}$, so its generator must be the common factor of m and n which is divisible by every other common factor. This is, of course, the highest common factor. A less precise way of saying this is that $m\mathbb{Z} + n\mathbb{Z}$ is the *smallest* subgroup containing both $m\mathbb{Z}$ and $n\mathbb{Z}$, so it is generated by the *biggest* common factor of m and n.

(2) Once again, $m\mathbb{Z} \cap n\mathbb{Z}$ is equal to $g\mathbb{Z}$ for some g, which is now a common multiple of m and n. Which common multiple? Since $m\mathbb{Z} \cap n\mathbb{Z}$ contains every subgroup contained in both $m\mathbb{Z}$ and $n\mathbb{Z}$, its generator must be the common multiple which divides every other common multiple. That is, it is the least common multiple. □

Corollary 3.6. *For any pair m and n of integers, there exist integers a and b (not necessarily positive) such that*

$$\mathrm{hcf}(m, n) = am + bn.$$

Proof. By Proposition 3.3, $m\mathbb{Z} + n\mathbb{Z} = h\mathbb{Z}$ where $h = \mathrm{hcf}(m, n)$. Hence in particular $h \in m\mathbb{Z} + n\mathbb{Z}$. But this means just that there are integers a and b such that $h = am + bn$.□

Note that this Corollary is a pure existence statement: it gives us no idea as to how we might find the integers a, b. We'll see how to do that using the Euclidean Algorithm below.

Definition 3.7. *The integers m and n are **coprime** if* $\mathrm{hcf}(m, n) = 1$.

As a particular case of Theorem 3.5 we have

Corollary 3.8. *The integers m and n are coprime if and only if there exist integers a and b such that $am + bn = 1$.*

Proof. One implication, that if m and n are coprime then there exist a, b such that $am + bn = 1$, is simply a special case of Corollary 3.6. The opposite implication also holds, however: for if k is a common factor of m and n then any number that can be written $am + bn$ must be divisible by k. If 1 can be written in this way then every common factor of a and b must divide 1, so no common factor of a and b can be greater than 1. □

3.2 The Extended Euclidean Algorithm

The Euclidean Algorithm is an efficient method not only to compute $\mathrm{hcf}(m, n)$ and also find integers a and b such that $am + bn = \mathrm{hcf}(m, n)$. To find a and b, we follow the Euclidean algorithm, (as in Lemma 2.15), but in reverse. Here is an example: take $m = 365,\ n = 750$ (Example 2.16(ii)). We know that $\mathrm{hcf}(365, 750) = 5$. So we must find integers a and b such that $a \times 365 + b \times 748 = 5$. To economise space, write $h = \mathrm{hcf}(750, 365)$. The Euclidean algorithm goes:

Step	**Division**		**Conclusion**
1	$750 = 2 \times 365 + 20$	;	$h = \mathrm{hcf}(365, 20)$
2	$365 = 18 \times 20 + 5$	;	$h = \mathrm{hcf}(20, 5)$
3	$20 = 4 \times 5$	;	$h = 5$

Step 3 can be read as saying

$$h = 1 \times 5.$$

Now use Step 2 to replace 5 by $365 - 18 \times 20$. We get

$$h = 365 - 18 \times 20.$$

Now use Step 1 to replace 20 by $750 - 2 \times 365$; we get

$$h = 365 - 18 \times (750 - 2 \times 365) = 37 \times 365 - 18 \times 750.$$

So $a = 37,\ b = -18$.

Exercise 3.2. *Find a and b when m and n are*

1. 365 *and* 748 *(cf Example 2.16(i))*
2. 365 *and* 760
3. $10^6 + 144$ *and* 10^3 *(cf Exercise 2.8)*
4. $90,090$ *and* $2,200$. *(cf Exercise 2.8).*

Exercise 3.3. *Are the integers a and b such that $am + bn = \mathrm{hcf}(m, n)$ unique?*

3.3 Modular Arithmetic

Both the number systems we have looked at so far ($\mathbb{N}$ and $\mathbb{Z}$) have been infinite, and the same is true of the systems of rational, real and complex numbers which will take up the next two Chapters. But there are finite number systems which are also very useful (and interesting).

We start with a positive[8] integer n, which will be called the *modulus*. Given n, we take the finite set

$$\{0,\ 1,\ \ldots,\ n-1\}$$

(which has n elements) and define a new kind of addition and multiplication on it called "addition modulo n" and "multiplication modulo n". These are given by the rules

$$r +_n s = \text{ remainder of (ordinary sum) } r + s \text{ after division by } n$$

$$r \times_n s = \text{ remainder of (ordinary product) } r \times s \text{ after division by } n$$

which we could write more concisely as

$$r +_n s = r + s \pmod{n}, \qquad r \times_n s = r \times s \pmod{n}.$$

For example, addition and multiplication modulo 4 are given in the following tables:

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

The operations $+_n$ and $\times_n$ on the set $\{0, 1, \ldots, n-1\}$ are examples of *binary operations*. Here is the formal definition:

Definition 3.9. *Let X be a set. A* **binary operation** *on X is a rule which, to each ordered pair of elements of X, associates a single element of X.*

Binary operations are usually (but not always, see the exercise below) denoted by a symbol such as $*$ between the two operands, so the result of applying $*$ to the pair (x, y) is then written $x * y$. Addition, multiplication and subtraction in $\mathbb{Z}$ are all examples of binary operations on $\mathbb{Z}$. (In the case of multiplication, we sometimes use a symbol such as $\cdot$ or $*$,

[8] usually $n \geq 2$ since the case $n = 1$ leads to a rather trivial arithmetic.

so the product of x and y may be written $x \cdot y$ or $x * y$, but usually no symbol at all is used and we just write xy.) Division is not a binary operation on $\mathbb{Z}$, because m/n is necessarily in $\mathbb{Z}$ for *every* pair (m, n) of elements of $\mathbb{Z}$; neither is it one on $\mathbb{R}$, since the second operand is not allowed to be 0, but it does give a binary operation on $\mathbb{R}^*$, the set of nonzero reals.

We will see more examples later in the course, and there have been other examples already:

Exercise 3.4. *Two binary operations on $\mathbb{N}$ are described on page 13 of the lecture notes. What are they?*

We will not discuss general binary operations in general here: mathematics students will see more of them in MA136 (Introduction to Abstract Algebra) and beyond. For now we'll stick to addition and multiplication. These both have two important properties: they are *commutative* and *associative*:

Definition 3.10. *A* **binary operation** $*$ *on X is*

- ***commutative*** *if $x * y = y * x$ for all $x, y \in X$;*
- ***associative*** *if $x * (y * z) = (x * y) * z$ for all $x, y, x \in X$;*

Obviously addition and multiplication of numbers are both commutative and associative—but be warned that there are important non-commutative forms of multiplication which you will encounter, such as matrix multiplication!

The operations of addition and multiplication modulo n have both these properties:

Proposition 3.11. *Addition and multiplication modulo n are associative.*

Proof. Both $a +_n (b +_n c)$ and $(a +_n b) +_n c$ are equal to the remainder of $a + b + c$ on division by n. To see this, observe first that if $p, q \in \mathbb{N}$ and $p = q + kn$ for some k then $a +_n p = a +_n q$. This is easy to see. It follows in particular that $a +_n (b +_n c) = a +_n (b + c)$, which is equal, by definition, to the remainder of $a + b + c$ after dividing by n. The same argument shows that $(a +_n b) +_n c$ is equal to the remainder of $a + b + c$ on division by n.

The argument for multiplication is similar: both $a \times_n (b \times_n c)$ and $(a \times_n b) \times_n c$ are equal to the remainder of abc on division by n. I leave this for you to show. □

We need to give a name for the structure consisting of the finite set $\{0, \ldots, n-1\}$ with the two operations $+_n$ and $\times_n$. For reasons which will be explained later, we call this structure $\mathbb{Z}/n$ (pronounced "Zed mod n") or $\mathbb{Z}/n\mathbb{Z}$ (pronounced "Zed mod n zed"). Some people denote it by $\mathbb{Z}_n$, but this symbol has a completely different meaning to some mathematicians when n is prime, so the notation $\mathbb{Z}/n$ is preferable.

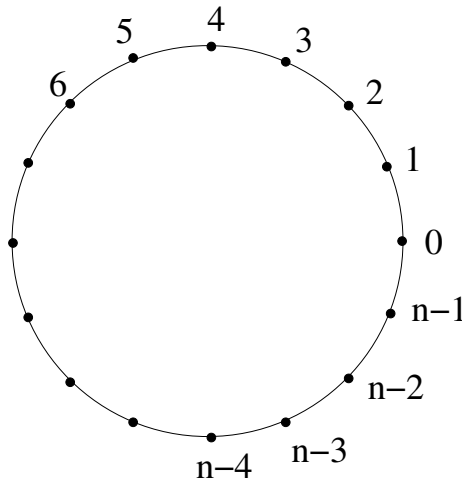
The additive structure of $\mathbb{Z}/n$ is extremely simple. The element 0 behaves as you would expect: adding it to any other element does not change it. We can also "subtract modulo n" simply by setting $a -_n b = a - b \pmod{n}$, the remainder on dividing $a - b$ modulo n. Explicitly, if $0 \leq a, b \leq n-1$ then $a -_n b = a - b$ if $a \geq b$ and $a -_n b = a - b + n$ if $a < b$. As a special case, taking $a = 0$ gives "negatives mod n": for $0 < b < n$ we have $-_n b = n - b$.

We've already seen a table of addition in $\mathbb{Z}/4$. Here are tables for $\mathbb{Z}/5$ and $\mathbb{Z}/6$:

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Notice that every number in $\mathbb{Z}/n$ appears once in each row and once in each column, and that the entries "cycle" round one step to the left, going from each row to the next. $\mathbb{Z}/n$ is an example of a "cyclic group[9] of order n". The reason for the word "cyclic" is because of the way that by repeatedly adding 1, one cycles through all the elements, with period n. This suggests displaying the elements of $\mathbb{Z}/n$ in a circle:



Visual representation of $\mathbb{Z}/n$

Adding 1 takes you one step anticlockwise (which is usually taken to be the "positive" direction), with $n-1$ stepping up to 0, and subtracting 1 takes you one step clockwise (in the "negative" direction".

Arithmetic Modulo n again, from a different viewpoint

Here is a different take on arithmetic modulo n. Declare two numbers $m_1, m_2 \in \mathbb{Z}$ to be "the same or **congruent** modulo n" if they leave the same remainder on division by n. The symbol[10] used to denote this "modulo n" form of equality is $\equiv$; so in other words,

$$m_1 \equiv m_2 \pmod{n} \quad \text{if} \quad m_1 - m_2 \in n\mathbb{Z}.$$

The remainder after dividing m by n is always between 0 and $n-1$. It follows that

every integer is congruent mod n *to exactly one of* $0, 1, \ldots, n-1$.

Doing computations modulo n is easy! Here are some examples (we'll justify these later).

[9] In this course we will not give a general definition of what a "group" is, but many of you will learn that later this term in MA136.

[10] the congruence symbol $\equiv$ was invented by Gauss in 1800; it deliberately looks rather like an equal sign $=$.

Example 3.12. 1. We work out $5^6 \pmod 7$. We have $5 \equiv -2 \pmod 7$, so

$$\begin{aligned} 5^6 &\equiv (-2)^6 \pmod 7 \\ &\equiv 64 \pmod 7 \\ &\equiv 1 \pmod 7. \end{aligned}$$

2. Similarly,

$$\begin{aligned} 5^5 &\equiv (-2)^5 \pmod 7 \\ &\equiv -32 \pmod 7 \\ &\equiv 3 \pmod 7. \end{aligned}$$

3. Working modulo 15:

$$\begin{aligned} 12^{15} &\equiv (-3)^{15} \pmod{15} \\ &\equiv ((-3)^3)^5 \pmod{15} \\ &\equiv (-27)^5 \pmod{15} \\ &\equiv 3^5 \pmod{15} \\ &\equiv 9 \times 27 \pmod{15} \\ &\equiv (-6) \times (-3) \pmod{15} \\ &\equiv 18 \pmod{15} \\ &\equiv 3 \pmod{15}. \end{aligned}$$

Exercise 3.5. *Compute (i)* $5^4 \pmod 7$*; (ii)* $8^{11} \pmod 5$*; (iii)* $98^7 \pmod{50}$*; (iv)* $11^{16} \pmod{17}$*; (v)* $13^{16} \pmod{17}$.

These calculations are rather exhilarating, but are they right? For example, what justifies the first step in Example 3.12 (1)? That is, is it correct that

$$5 \equiv -2 \pmod 7 \quad \Longrightarrow \quad 5^6 \equiv (-2)^6 \pmod 7? \tag{13}$$

To make the question clearer, let me paraphrase it. It says: if 5 and -2 have in common that they leave the same remainder after division by 7, then do 5^6 and $(-2)^6$ also have this in common? A stupid example might help to dislodge any residual certainty that the answer is obviously Yes: the numbers 5 and 14 also have something in common, namely that when written in English they begin with the same letter. Does this imply that their 6'th powers begin with the same letter? Although the implication in (13) is written in official looking mathematical notation, so that it doesn't look silly, we should not regard its truth as in any way obvious.

This is why we need the following lemma, which provides a firm basis for all of the preceding calculations.

Lemma 3.13.

$$\left.\begin{array}{rcll} a_1 & \equiv & b_1 & \pmod n \\ a_2 & \equiv & b_2 & \pmod n \end{array}\right\} \quad \Longrightarrow \left\{\begin{array}{rcll} a_1 + a_2 & \equiv & b_1 + b_2 & \pmod n \\ a_1 a_2 & \equiv & b_1 b_2 & \pmod n. \end{array}\right.$$

Proof. If $a_1 - b_1 = k_1 n$ and $a_2 - b_2 = k_2 n$ then

$$\begin{aligned} a_1 a_2 - b_1 b_2 &= a_1 a_2 - a_1 b_2 + a_1 b_2 - b_1 b_2 \\ &= a_1(a_2 - b_2) + b_2(a_1 - b_1) \\ &= (a_1 k_2 + b_2 k_1) n, \end{aligned}$$

so $a_1a_2 \equiv b_1b_2 \pmod{n}$. The argument for the sum is similar (and easier). $\square$

The lemma says that we can safely carry out the kind of simplification we used in calculating, say, $5^6 \pmod 7$. Applying the lemma to the question I asked above, we have

$$\begin{aligned} 5 \equiv -2 \pmod 7 \quad &\Longrightarrow \quad 5 \times 5 \equiv (-2) \times (-2) \pmod 7 \quad \Longrightarrow \\ &\Longrightarrow \quad 5 \times 5 \times 5 \equiv (-2) \times (-2) \times (-2) \pmod 7 \quad \Longrightarrow \cdots \\ &\Longrightarrow 5^6 \equiv (-2)^6 \pmod 7. \end{aligned}$$

Notation: Denote by $[m]$ the set of all the integers congruent to m modulo n. Thus,

$$[1] = \{1,\ n+1,\ 2n+1,\ 1-n,\ 1-2n,\ \ldots\}$$

$$[n+2] = \{2,\ 2+n,\ 2+2n,\ 2-n,\ 2-2n,\ \ldots\}$$

and by the same token

$$[n-3] = [-3] = [-(3+n)] = \cdots$$

because each denotes the set

$$\{-3, n-3, -(n+3), 2n-3, -(2n+3), \ldots\}.$$

For example, modulo 2 we have precisely **two** sets of this form, namely

$$[0] = \{0, \pm 2, \pm 4, \ldots\} = \text{the set of all } \textit{even} \text{ integers}$$

and

$$[1] = \{\pm 1, \pm 3, \pm 5, \ldots\} = \text{the set of all } \textit{odd} \text{ integers}.$$

This allows us to cast the finite number system $\mathbb{Z}/n$ in a somewhat different light. Instead of viewing its members as the integers in the range $0, \ldots, n-1$, instead we view its members as the *sets*

$$[0],\ [1],\ [2],\ \ldots,\ [n-1]$$

and combine them under addition and multiplication by the following rule:

$$[a] + [b] = [a+b] \qquad [a] \times [b] = [a \times b]. \tag{14}$$

The rule looks very, very simple, but its apparent simplicity covers up a deeper issue. The problem is this:

If $[a_1] = [b_1]$ and $[a_2] = [b_2]$, then $[a_1 + a_2]$ had better equal $[b_1 + b_2]$, and $[a_1a_2]$ had better equal $[b_1b_2]$, otherwise rule (14) doesn't make any sense.

The point is that in definition (14) both right-hand sides depend on a *choice* of integer a to represent the class $[a]$ (and similarly for b). This problem has been taken care of, however! In the new notation, Lemma 3.13 says precisely this:

$$\left.\begin{array}{rcl} [a_1] & = & [b_1] \\ [a_2] & = & [b_2] \end{array}\right\} \quad \Longrightarrow \left\{\begin{array}{rcl} [a_1 + a_2] & = & [b_1 + b_2] \\ [a_1a_2] & = & [b_1b_2]. \end{array}\right.$$

So our rule (14) *does* make sense. The set

$$\{[0],\ [1],\ \ldots,\ [n-1]\}$$

with addition and multiplication as defined by (14) works *exactly the same way* as the set $\{0, 1, \ldots, n-1\}$ with the operations $+_n$ and $\times_n$ defined on page 20; we've just modified our way of thinking. This new way of thinking has far-reaching generalisations, but I say no more about this here.

We'll come back to congruence and the classes $[a]$ in Chapter 6 when we'll see that congruence is an example of an **equivalence relation**.

We end this section by stating, but not proving, a theorem due to Fermat, and known[11]. as his Little Theorem.

Theorem 3.14. *If p is a prime number then for every integer a not divisible by p,*

$$a^{p-1} \equiv 1 \pmod{p}.$$

[11]Not to be confused with his famous Last Theorem! This one is much easier to prove

4 Rational and Real Numbers

4.1 Rational numbers

Just as the natural numbers arise naturally as counting numbers, we can motivate the introduction of both rational and real numbers by the need to have enough numbers to measure lengths. Beginning with any unit of length, we can measure smaller lengths by subdividing our unit into n equal parts. Each part is denoted $\frac{1}{n}$. By assembling different numbers of these subunits, we get a great range of different quantities. We denote the length obtained by placing m of them together $\frac{m}{n}$. It is clear that $\frac{k}{kn} = \frac{1}{n}$, since n lots of $\frac{k}{kn}$ equals one unit, just as do n lots of $\frac{1}{n}$. More generally, we have $\frac{km}{kn} = \frac{m}{n}$. It follows from this that the lengths $\frac{m_1}{n_1}$ and $\frac{m_2}{n_2}$ are equal if and only if

$$m_1 n_2 = n_1 m_2. \tag{15}$$

For $\frac{m_1}{n_1} = \frac{m_1 n_2}{n_1 n_2}$ and $\frac{m_2}{n_2} = \frac{m_2 n_1}{n_1 n_2}$, so the two are equal if and only if (15) holds. Motivated by this, the set of *rational numbers*, $\mathbb{Q}$, is thus defined, as an abstract "number system", to be the set of quotients $\frac{m}{n}$, where m and n are integers with $n \neq 0$ and two such quotients $\frac{m_1}{n_1}$ and $\frac{m_2}{n_2}$ are equal if and only if (15) holds. Addition is defined in the only way possible consistent with having

$$\frac{m_1}{n} \pm \frac{m_2}{n} = \frac{m_1 \pm m_2}{n},$$

namely

$$\frac{m_1}{n_1} \pm \frac{m_2}{n_2} = \frac{m_1 n_2}{n_1 n_2} \pm \frac{m_2 n_1}{n_1 n_2} = \frac{m_1 n_2 \pm m_2 n_1}{n_1 n_2}.$$

Similar considerations lead to the familiar definition of multiplication and division:

$$\frac{m_1}{n_1} \times \frac{m_2}{n_2} = \frac{m_1 m_2}{n_1 n_2} \qquad \text{and} \qquad \frac{m_1}{n_1} \div \frac{m_2}{n_2} = \frac{m_1 n_2}{n_1 m_2},$$

where for division we require $m_2 \neq 0$ (i.e. $m_2/n_2 \neq 0$) so that $n_1 m_2 \neq 0$.

With these operations we have a number system $\mathbb{Q}$ in which we can add, subtract, multiply and divide any two numbers (with the single restriction that division by 0 is not allowed), and these operations satisfy all the usual algebraic laws. Such a number system is called a *field* (see the end of this chapter (Page 31), and also page 34, for a little more about fields).

One feature of the way we represent rational numbers as quotients m/n is that the representation is not unique: $3/2 = 6/4 = 51/34 = \ldots$. Among all the (infinitely many!) ways of writing any rational number, there is one which is simplest:

Proposition 4.1. *Among all expressions for a given rational number q, there is a unique expression (up to sign) in which the numerator and denominator are coprime. We call this the* ***minimal expression*** *for q or the* ***minimal form*** *of q.*

By "unique up to sign" I mean that if $\frac{m}{n}$ is a minimal expression for q, then so is $\frac{-m}{-n}$, but there are no others. Often we will want to make the minimal expression unique by insisting that the denominator be positive: the minimal forms of $-6/4$ are $-3/2$ and $3/-2$, of which we prefer $-3/2$.

Proof. *Existence:* if $q = m/n$, divide each of m and n by $\mathrm{hcf}(m,n)$. Clearly $m/\mathrm{hcf}(m,n)$ and $n/\mathrm{hcf}(m,n)$ are coprime, and

$$q = \frac{m}{n} = \frac{m/\mathrm{hcf}(m,n)}{n/\mathrm{hcf}(m,n)}.$$

Uniqueness: If $\frac{m}{n} = \frac{m_1}{n_1} = \frac{m_2}{n_2}$ with $\mathrm{hcf}(m_1, n_1) = \mathrm{hcf}(m_2, n_2) = 1$, then using the criterion for equality of rationals (15) we get $m_1 n_2 = n_1 m_2$. This equation in particular implies that

$$m_1 | n_1 m_2 \tag{16}$$

and that

$$m_2 | n_2 m_1. \tag{17}$$

As $\mathrm{hcf}(m_1, n_1) = 1$, (16) implies that $m_1 | m_2$. For none of the prime factors of m_1 divides n_1, so every prime factor of m_1 must divide m_2.

As $\mathrm{hcf}(m_2, n_2) = 1$, (17) implies that $m_2 | m_1$, by the same argument.

The last two lines imply that $m_1 = \pm m_2$, and thus, given that $m_1 n_2 = n_1 m_2$, that $n_1 = \pm n_2$ also. □

We can do a lot with rational numbers, but not everything! They are not sufficient to give us solutions to all equations, even quadratic equations:

Proposition 4.2. *There is no rational number q such that $q^2 = 2$.*

Proof. Suppose that

$$\left(\frac{m}{n}\right)^2 = 2, \tag{18}$$

where $m, n \in \mathbb{Z}$. We may assume that m and n are positive. Multiplying both sides of (18) by n^2 we get

$$m^2 = 2n^2. \tag{19}$$

Replacing both m and n by their prime factorisations we see that the number m^2 on the left of (19) has an *even* number of prime factors, while the number $2n^2$ on the right has an *odd* number. This contradicts the uniqueness of prime factorisations (Theorem 2.8); the contradiction shows that there can exist no such m and n. □

Proposition 4.3. *If $n \in \mathbb{N}$ is not a perfect square, then there is no rational number $q \in \mathbb{Q}$ such that $q^2 = n$.*

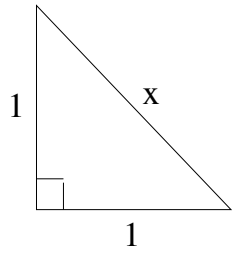
Proof. Pretty much the same as the proof of Proposition 4.2. I leave it as an exercise to work out the details. □

4.2 Real numbers

Proposition 4.2 is often stated as "$\sqrt{2}$ is irrational". This presupposes that there *is* some sort of number whose square is 2, it just is not a rational number. That is true: the rationals $\mathbb{Q}$ can be enlarged, or "completed", to for the (much) larger system $\mathbb{R}$ of **real numbers** in which every positive integer has a square root.

We will not give a construction of the real number system here, since it is quite hard and requires some Analysis. Instead we will give some motivation for the construction, before moving on to how to actually represent real numbers, using decimal expansions.

Remark 4.4. Brief historical discussion, for motivation As already stated, Proposition 4.2 is often stated in the form "$\sqrt{2}$ is not rational". But what makes us think that there is such a number as $\sqrt{2}$, i.e. a number whose square is 2? For the Greeks, the reason was Pythagoras's Theorem. They believed that once a unit of length is chosen, then it should be possible to assign to every line segment a number, its length. Pythagoras's Theorem told them that in the diagram below, $1^2 + 1^2 = x^2$, in other words $x^2 = 2$.

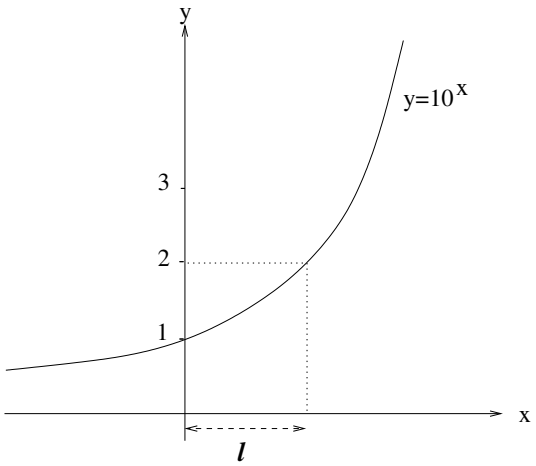


This was a problem, because up until that moment the only numbers they had discovered (invented?) were the rationals, and they knew that no rational can be a square root of 2. In a geometrical context the rationals make a lot of sense: given a unit of length, you can get a huge range of other lengths by subdividing your unit into as many equal parts as you like, and placing some of them together. Greek geometers at first expected that by taking suitable multiples of fine enough subdivisions they would be able to measure every length. Pythagoras's theorem showed them that this was wrong. Of course, in practice it works pretty well - to within the accuracy of any given measuring device. One will never get *physical* evidence that there are irrational lengths.

If we place ourselves at the crossroads the Greeks found themselves at, it seems we have two alternatives. Either we give up our idea that every line segment has a length, or we make up some new numbers to fill the gaps the rationals leave. Mathematicians have in general chosen the second alternative. But which gaps should we fill? For example: should we fill the gap

$$10^\ell = 2 \tag{20}$$

(i.e. $\ell = \log_{10} 2$)? This also occurs as a length, in the sense that if we draw the graph of $y = 10^x$ then ℓ is the length of the segment shown on the x-axis in the diagram below.



Should we fill the gap

$$x^2 = -1? \tag{21}$$

Should we fill the gaps left by the solutions of polynomial equations like $x^2 = 2$, or, more generally,

$$x^n + q_{n-1}x^{n-1} + \cdots + q_1 x + q_0 = 0 \tag{22}$$

where the coefficients $q_0, \ldots, q_{n-1}$ are rational numbers? The answer adopted by modern mathematics is to define the set of real numbers, $\mathbb{R}$, to be 'the smallest complete number system containing the rationals'. This means in one sense that we throw into $\mathbb{R}$ solutions to every equation *where we can approximate those solutions, as close as we wish, by rational numbers*. In particular, we fill the gap (20) and some of the gaps (22) but not the gap (21) (you cannot find a sequence of rationals whose squares approach -1, since the square of every rational number is greater than or equal to 0). As you will see at some point in Analysis, the real numbers are precisely the numbers that can be obtained as the limits of convergent sequences of rational numbers. In fact, this is exactly how we all first encounter them. When we are told that

$$\sqrt{2} = 1.414213562\ldots$$

what is really meant is that $\sqrt{2}$ is the limit of the sequence of rational numbers

$$1, \quad \frac{14}{10}, \quad \frac{141}{100}, \quad \frac{1414}{1,000}, \quad \frac{14142}{10,000}, \ldots$$

If you disagree with this interpretation of decimals, can you give a more convincing one?

4.3 Decimal expansions and irrationality

A real number that is not rational is called *irrational*. As we will see in a later section, although there are infinitely many of each kind of real number, there are, in a precise sense, many more irrationals than rationals.

So an irrational number is one which, though not rational (i.e. expressible as a quotient or ration of two integers), can be approximated arbitrarily closely by rationals. But then how do we write down such a number? Not many have simple expressions such as $\sqrt{2}$. But they all have **decimal expansions**, which do precisely what is required! Every decimal expansion encodes a convergent sequence of rational numbers (as with the example of $\sqrt{2}$ above) and hence a real number.

The decimal

$$m_k\, m_{k-1} \cdots m_1\, m_0 \cdot n_1\, n_2 \ldots n_t \ldots \tag{23}$$

(in which all of the m_i's and n_j's are between 0 and 9) denotes the real number

$$(m_k \times 10^k) + \cdots + (m_1 \times 10) + m_0 + \frac{n_1}{10} + \frac{n_2}{100} + \cdots + \frac{n_t}{10^t} + \cdots \tag{24}$$

Notice that there are only finitely many non-zero m_i's, but there may be infinitely many non-zero n_j's.

Theorem 4.5. *The number (24) is rational if and only if the sequence*

$$m_k,\ m_{k-1},\ \ldots,\ m_0,\ n_1,\ n_2,\ \ldots,\ n_t,\ \ldots$$

is eventually[12] *periodic.*

[12] "Eventually periodic" means that after some point the sequence becomes periodic.

Proof. The proof has two parts, corresponding to the two implications. We can restrict our attention to positive numbers x (why?).

First suppose that x has a periodic expansion, say of period d, so to the right of the decimal point the digits $n_1, n_2, \ldots, n_d$ repeat. Then the decimal expansion of $y = 10^d x$ has *exactly the same digits* to the right of the decimal point as x (since multiplying by 10 shifts the decimal point by one place, so multiplying by 10^d shifts it by d places). That means that $y - x$ has 0 to the right of the decimal point, and is therefore an *integer*. Thus

$$(10^d - 1)x = y - x = n \in \mathbb{Z},$$

so $x = n/(10^d - 1)$ which is rational.

Next, if the decimal expansion of x is only eventually periodic, say that the periodicity only starts after e decimal places and then has period d. Then $10^e x$ and $10^{d+e}x$ have the same decimal part, so differ by an integer n, and hence $x = n/(10^{d+e} - 10^e)$ which is rational.

Now for the other direction. Given a positive rational $x = m/n$, if we can find $d > 0$ and $e \geq 0$ such that $(10^{d+e} - 10^e)x \in \mathbb{Z}$ then it will follow, as in the previous paragraph, that the decimal expansion of x has period d starting after e digits. Why should such d, e exist?

Consider the sequence of integers

$$m, 10m, 100m, 1000m, \ldots, 10^k m, \ldots$$

and for each integer in the sequence, take its remainder on division by n. Since the sequence is infinite, but there are only finitely many different remainders possible, there must be repeats in the sequence of remainders! That means that there must be two values of k, say $k_1 \geq 0$ and $k_2 > k_1$ such that

$$10^{k_1} m \equiv 10^{k_2} m \pmod{n}.$$

Writing $e = k_1$ and $d = k_2 - k_1$, we have $e \geq 0$ and $d > 0$, and

$$(10^{d+e} - 10^e)x = (10^{k_2} - 10^{k_1})(m/n) \in \mathbb{Z},$$

as required, finishing the proof. □

Some examples may help you follow the general argument:

Example 4.6. *1. Express* $0.12\overline{34}$ *as a rational number.* (Here the line over the digits 34 indicates that these two digits repeat, so $x = 0.1234343434\ldots$).

We have $100x = 12.\overline{34}$ and $10000x = 1234.\overline{34}$, which have the same decimal part. Subtract to get $9900x = 1234 - 12 = 1222$, so $x = 1222/9900 = 611/4950$.

2. Find the decimal expansion of $x = 3/7$.

You can use long division for this if you prefer. Following the steps of the proof (which is really long division in disguise), we take $m = 3$ and $n = 7$, and then list the numbers $10^k m \pmod{n}$ in sequence until we see a repeat:

$$3,\ 30 \equiv 2,\ 20 \equiv 6,\ 60 \equiv 4,\ 40 \equiv 5,\ 50 \equiv 1,\ 10 \equiv 3,\ \ldots$$

where at each step we multiply by 10 and reduce modulo 7. The upshot is that $3 \cdot 10^6 \equiv 3 \pmod{7}$. Now $10^6 - 1 = 999999 = 7 \cdot 142857$, so $(10^6 - 1)x = 3 \cdot 142857 = 428571$, which means that $x = 0.\overline{428571}$.

Exercise 4.1. *Find decimal expansions for the rational numbers*

$$\frac{2}{7},\ \frac{3}{11},\ \frac{1}{6},\ \frac{1}{37}$$

Exercise 4.2. *Express as rational numbers the decimals*

$$0 \cdot \overline{23}, \qquad 0 \cdot \overline{234}, \qquad \textit{and} \qquad 0 \cdot 1\overline{23}.$$

Exercise 4.3. *(i) Can you find an upper bound for the length of the cycle in the decimal expansion of the rational number $\frac{m}{n}$ (where m and n are coprime natural numbers)? (ii) Can you find an upper bound for the denominator of a rational number if the decimal representing it becomes periodic with period ℓ after an initial decimal segment of length k? Try with $k = 0$ first.*

Further study of the real number system would lead us into Analysis, which is not the subject of this course. Instead, we end this chapter with a summary of where we are, and where we will be going next.

4.4 Summary

So far we have studied the four "number systems" $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$. Obviously each contains its predecessor. It is interesting to compare the jump we make when we go from each one to the next. In $\mathbb{N}$ there are two operations, $+$ and $\times$. There is an "additive neutral element" 0, with the property that adding it to any number leaves that number unchanged, and there is a "multiplicative neutral element" 1, with the property that multiplying any number by it leaves that number unchanged. In going from $\mathbb{N}$ to $\mathbb{Z}$ we throw in the negatives of the members of $\mathbb{N}$. These are more formally known as the "additive inverses" of the members of $\mathbb{N}$: adding to any number its additive inverse gives the additive neutral element 0. The "multiplicative inverse" of a number is what you must multiply it by to get the neutral element for multiplication, 1. In $\mathbb{Z}$, most numbers do not have multiplicative inverses, and we go from $\mathbb{Z}$ to $\mathbb{Q}$ by throwing in the multiplicative inverses of the non-zero elements of $\mathbb{Z}$. Actually we throw in a lot more too, since we want to have a number system which contains the sum and product of any two of its members. The set of rational numbers $\mathbb{Q}$ is in many ways a very satisfactory number system, with its two operations $+$ and $\times$, and containing, as it does, the additive and multiplicative inverses of all of its members (except for a multiplicative inverse of 0). It is an example of a **field**. Other examples of fields are the real numbers $\mathbb{R}$ and the complex numbers $\mathbb{C}$, which we obtain from $\mathbb{R}$ by throwing in a solution to the equation

$$x^2 = -1,$$

together with everything else that results from addition and multiplication of this element with the members of $\mathbb{R}$. The complex numbers will be the topic of the next chapter. There are other examples of fields arising from modular arithmetic.

Exercise 4.4 (Optional)**.** *Can you say for which $n > 0$ the structure $\mathbb{Z}/n$ is a field? Remember that every nonzero element must be invertible.*

Exercise 4.5 (Optional)**.** *Actually, in our discussion of filling gaps in $\mathbb{Q}$, we implicitly mentioned at least one other field, intermediate between $\mathbb{Q}$ and $\mathbb{C}$ but not containing all of $\mathbb{R}$. Can you guess what it might be? Can you show that the sum and product of any two of its members are still members? In the case of the field I'm thinking of, this is rather hard.*

5 Complex Numbers

5.1 What are ℂomplex Numbers?

A *complex number* is represented by $a+bi$ where a and b are real numbers and i is a symbol that satisfies $i^2 = -1$. We add and multiply complex numbers as you would expect; every time we see an i^2 we replace it by -1.

Example 5.1. *Let α and β be the complex numbers $\alpha = 2+3i$ and $\beta = -7+4i$. Addition is straightforward:*

$$\alpha + \beta = -5 + 7i, \qquad \alpha - \beta = 9 - i.$$

Multiplication involves the usual expansion of brackets and then replacing i^2 by -1:

$$\begin{aligned} \alpha\beta &= (2+3i)(-7+4i) \\ &= -14 - 13i + 12i^2 \qquad \textit{usual expansion of brackets} \\ &= -14 - 13i + 12(-1) \qquad \textit{replace } i^2 \textit{ by } -1 \\ &= -26 - 13i \end{aligned}$$

The set of complex numbers is denoted by $\mathbb{C}$. In set notation we can write

$$\mathbb{C} = \{a + bi \ : \quad a, b \in \mathbb{R}\}.$$

Definition 5.2. *Let α be a complex number and write $\alpha = a + bi$ where a and b are real numbers. We call a the real part of α and b the imaginary part of α. We write $\Re(\alpha) = a$ and $\Im(\alpha) = b$.*

Example 5.3. *$\Re(2-4i) = 2$ and $\Im(2-4i) = -4$.*

The Complex Plane

The complex number $a+bi$ is represented by the point (a, b) in the coordinate plane. The x-axis is called the real axis and the y-axis is called the imaginary axis. When used to represent complex numbers in this way, the coordinate plane is called 'The Argand diagram', or 'the complex plane'. See Figure 1.

Addition can be described geometrically (i.e. on the complex plane) by completing the parallelogram. If z and w are complex numbers, then the points representing 0 (the origin), z, w and $z+w$ form a parallelogram; see Figure 2.

Some Formal Definitions

Equality of complex numbers is straightforward.

Definition 5.4. *Two complex numbers are equal if and only if their real parts are equal and their imaginary parts are equal. Another way of saying this is: if $\alpha = a + b\,i$ and $\beta = c + d\,i$ are complex numbers (with a, b, c, d real) then $\alpha = \beta$ if and only if $a = b$ and $c = d$.*

We saw examples of addition and multiplication above, but let us write the definition of addition and multiplication more formally.

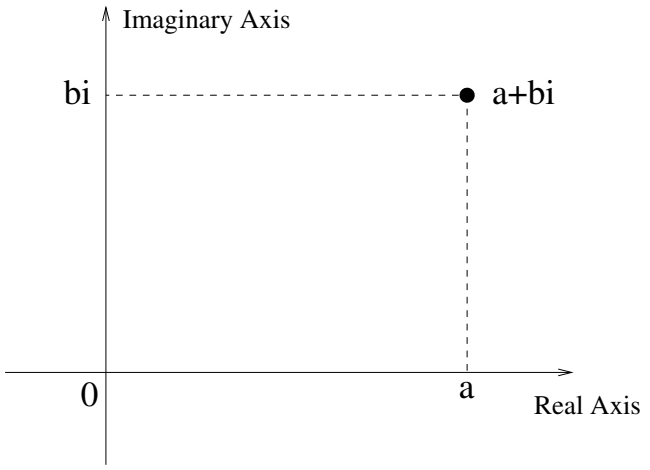


Figure 1: The Complex Plane (or The Argand Diagram).

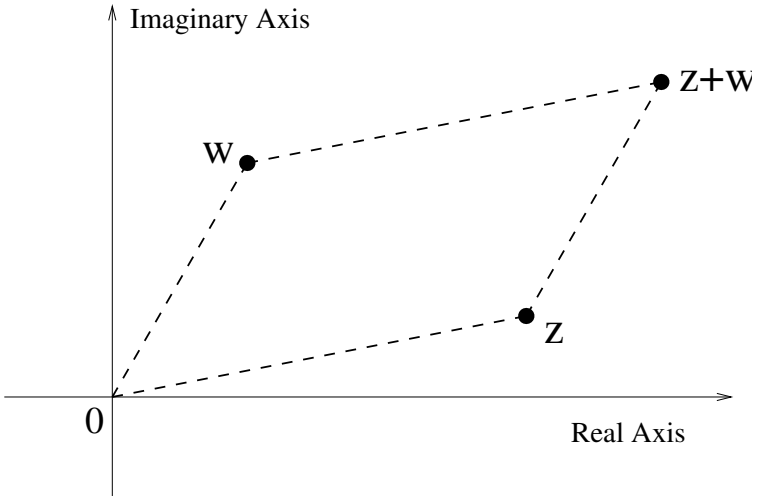


Figure 2: If z and w are complex numbers, then the points on the complex plane representing 0 (the origin), z, w and $z + w$ form a parallelogram.

Definition 5.5. *Suppose $\alpha = a + bi$ and $\beta = c + di$ are complex numbers, where a, b, c, d are real numbers. We define the sum $\alpha + \beta$ by*

$$\alpha + \beta = (a + c) + (b + d)i$$

and the product $\alpha\beta$ by

$$\alpha\beta = (ac - bd) + (ad + bc)i.$$

Notice that real numbers are also complex numbers. Indeed if a is a real number, we can think of it as the complex number $a + 0.i$. A complex number of the form bi (i.e. $0 + bi$), with b real, is called an imaginary number. Thus real numbers and imaginary numbers are special types of complex numbers.

Example 5.6. *Suppose r is a positive real number. We denote by $\sqrt{r}$ the positive square-root of r. Notice that*

$$(\pm\sqrt{r}i)^2 = -r.$$

We see that positive real numbers have two real square-roots, whereas negative real numbers have two imaginary square-roots.

Exercise 5.1. *Which number is both real and imaginary?*

Fields

Like the set $\mathbb{Q}$ of rational numbers and the set $\mathbb{R}$ of real numbers, the set $\mathbb{C}$ of complex numbers is an example of the mathematical structure called a **field**. All this means is that on each of these sets or number systems, all four of the basic arithmetic operations (additions and subtraction, multiplication and division except by zero) may be carried out *without going outside the system*; moreover, the usual properties of these operations (called the *commutative*, *distributive* and *associative laws*) all hold. These facts should be proved, and it is not at all hard to do so for the field of complex numbers (assuming that you already know all the properties for the field of real numbers), but we will not do that here.

Nevertheless, a few remarks are in order: neither $\mathbb{Z}$ nor $\mathbb{N}$ are fields, since in neither case can we (for example) divide 2 by 3 within the system, so while addition and multiplication are always possible in these systems, division is not (and in the case of $\mathbb{N}$, neither is subtraction). If you take Algebra courses (as all Mathematics students do, starting with MA136 Introduction to Abstract Algebra this term) you will learn more about these and other algebraic systems.

Here is one more big difference between the real and complex systems: there is no good definition of "less than" or "greater than" for complex numbers, and there are no positive or negative complex numbers. You may like to think about why this must be so: the clue is that wherever "positive" makes sense, squares are always positive–but all complex numbers are squares (see Example 5.6)!

So remember: *Inequalities between complex numbers have no meaning.* This is a point that needs special care. Never write $\alpha > \beta$ if either α or β is a non-real complex number!

5.2 Powers, conjugates, reciprocals and division

How do we define exponentiation? In other words, what does α^n mean? Well if n is a positive integer then this is easy to define.

Definition 5.7. *If α is a complex number and n a positive integer then we define*

$$\alpha^n = \underbrace{\alpha \cdot \alpha \cdots \alpha}_{n \text{ times}}.$$

The definition is correct, but involves a subtle point that should really be checked: when forming the product α^n by repeated multiplication, does it matter how we group the factors? For example, when $n = 4$, are $\alpha(\alpha(\alpha^2))$ and $(\alpha^2)(\alpha^2)$ equal? The answer (luckily) is "yes", and it can be proved using the associative law, but the proof is exceedingly tedious and will be omitted.

Example 5.8. *Let $\alpha = 1 + i$. Then (check this):*

$$\alpha^2 = 2i, \qquad \alpha^4 = (2i)^2 = -4.$$

Notice that -4 is not the square of a real number but it is the square and fourth power of certain complex numbers. We see from the calculation above that $\alpha = 1 + i$ is a root of the

polynomial $X^4 + 4$. This polynomial does not have any real roots but has 4 complex roots which are $\pm 1 \pm i$ (check). [13]

Exercise 5.2. *For which positive integral values of n is i^n real?*

Next we come to a simple but important operation on complex numbers: conjugation. We will see later that the conjugate helps us in defining the division of complex numbers.

Definition 5.9. *Let $\alpha = a + bi$ be a complex number, where a, b are real numbers. We define the conjugate of α (denoted by $\overline{\alpha}$) to be $\overline{\alpha} = a - bi$.*

Theorem 5.10. *Suppose α, β are complex numbers. Then*

(i) The equality $\alpha = \overline{\alpha}$ holds if and only if α is a real number.

(ii) Conjugation distributes over addition and multiplication: in other words

$$\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta} \qquad \text{and} \qquad \overline{\alpha \cdot \beta} = \overline{\alpha} \cdot \overline{\beta}.$$

(iii) If $\alpha = a + bi$ with a, b real numbers then

$$\alpha \cdot \overline{\alpha} = a^2 + b^2.$$

In particular $\alpha \cdot \overline{\alpha}$ is a non-negative real number, which is 0 if and only if $\alpha = 0$.

Proof. The proof is left as an exercise. □

Exercise 5.3. *What is the geometric meaning*[14] *of conjugation? I.e. if z is a complex number, describe the geometric operation on the complex plane that takes z to its conjugate $\overline{z}$.*

Next, and before defining division more generally, we would like to define reciprocals of complex numbers. In other words, if α is a non-zero complex number, what do we mean by $1/\alpha$? There are certain reasonable things that we should expect from this definition. Of course we want to define reciprocal in such a way that $\alpha \cdot (1/\alpha) = 1$. The key to discovering the correct definition is part (iii) of Theorem 5.10. This can be rewritten as follows: if a, b are real and $\alpha = a + bi$ then

$$\alpha\overline{\alpha} = (a + bi)(a - bi) = a^2 + b^2.$$

We instantly see that the following definition is reasonable.

Definition 5.11. *Let α be a non-zero complex number and write $\alpha = a + bi$ where a, b are real and not both 0. Define the reciprocal of α to be*

$$\frac{1}{\alpha} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i = \frac{1}{a^2 + b^2}\overline{\alpha}.$$

[13] An important theorem which we will see later is the Fundamental Theorem of Algebra which says that a polynomial of degree n has n complex roots (counting multiplicities). This is clearly not true if we work just with real numbers.

[14] You should get used to thinking geometrically, and to drawing pictures. The true meaning of most mathematical concepts is geometrical. If you spend all your time manipulating symbols (i.e. doing algebra) without understanding the relation to the geometric meaning, then you will have very little in terms of mathematical insight.

You can easily check that multiplying out

$$(a+bi)\left(\frac{a}{a^2+b^2}-\frac{b}{a^2+b^2}i\right)$$

and simplifying gives 1, and also that (since a and b are real!) the expression a^2+b^2 cannot be 0 unless $a=b=0$, but this is exactly what we excluded by insisting that $\alpha \neq 0$. So the definition makes sense.

Recall that we defined α^n only for positive integer values of n. Now if n is negative we can define $\alpha^n = 1/\alpha^{-n}$. So (with $\alpha^0 = 1$) we have defined[15] α^n for all $n \in \mathbb{Z}$ whenever α is a non-zero complex number; the usual laws for working with exponents apply.

It is now clear how to define division: if α and β are complex and $\alpha = a+bi$ is non-zero, then we define

$$\beta/\alpha = \beta \cdot 1/\alpha = \frac{\beta\overline{\alpha}}{a^2+b^2}.$$

The last expression here gives us the following standard way to divide complex numbers: multiply top and bottom by the conjugate of the denominator; *this makes the denominator real*, so we may easily simplify.

Example 5.12.

$$\begin{aligned}\frac{3+i}{2-4i} &= \frac{(3+i)(2+4i)}{(2-4i)(2+4i)}\\ &= \frac{2+14i}{2^2+4^2}\\ &= \frac{1}{10}+\frac{7}{10}i.\end{aligned}$$

Exercise 5.4. *Solve the equation* $(5-i)X+7=2i$.

Exercise 5.5. *Write*

$$\frac{1}{\cos\theta + i\,\sin\theta}$$

in the form $a+i\,b$. *(You might already know the answer, but do this question using the definition of reciprocal).*

5.3 The Absolute Value and Argument of complex numbers

Let a be a real number. We recall the definition of the modulus (also called the absolute value) $|a|$ as follows:

$$|a| = \begin{cases} a & \text{if } a \geq 0\\ -a & \text{if } a < 0.\end{cases}$$

From now on we say absolute value instead of modulus. We would like to extend the notion of absolute value to complex numbers. The above definition will not do because the inequalities $a \geq 0$ and $a < 0$ do not have a meaning when a is a complex number. There is, however, another—more geometric—definition of the absolute value of a real number: if a is a real number then $|a|$ is the distance on the real line between the numbers a and 0. This definition

[15] to define α^x for real x, or α^β for complex β is much harder and is a question of analysis, not algebra.

can be extended to complex numbers. In geometric terms we define, for a complex number α, its absolute value $|\alpha|$ to be the distance between α and 0 (the origin) in the complex plane. This definition is not suitable for calculations, however it is easy to see how to turn it into an algebraic definition; if $\alpha = a + bi$ with a, b real then the distance of α from the origin is $\sqrt{a^2 + b^2}$. We finally arrive at our definition.

Definition 5.13. *Let $\alpha = a + bi$ be a complex number with a, b real. We define the absolute value of α to be*

$$|\alpha| = \sqrt{a^2 + b^2}.$$

Note that when we speak of the square-root of a positive real, we always mean the *positive* square-root.

Theorem 5.14. *Let α, β be complex numbers.*

(i) $\alpha\overline{\alpha} = |\alpha|^2$.

(ii) $|\alpha| = 0$ *if and only if* $\alpha = 0$.

(iii) $|\alpha\beta| = |\alpha||\beta|$.

(iv) $|\alpha + \beta| \leq |\alpha| + |\beta|$ *(this is the triangle inequality).*

(v) $|\alpha - \beta| \geq \big||\alpha| - |\beta|\big|$.

Proof. The proof is left as an exercise. □

Recall that there are two coordinate systems which one may employ to specify points in the plane. The first is the Cartesian system and the second the polar system. In the Cartesian system we represent a point by a pair (a, b): here a and b are distances we have to move parallel to the x- and y-axes to reach our point, having started at the origin. In the polar system we represent points by a pair (r, θ): here r is the distance of the point from the origin. Moreover, if we denote the point by P then θ is the angle[16] measured from the positive x-axis to the ray $\overrightarrow{OP}$ in an anti-clockwise direction. This the polar system.

Converting between Cartesian and polar coordinates is easy. Let (a, b) and (r, θ) represent the same point. We deduce from Figure 3 that

$$a = r\,\cos\theta, \qquad b = r\,\sin\theta.$$

Previously we used the Cartesian system to represent the complex number $\alpha = a + bi$ on the complex plane. But we can also use the polar system. Now r is the distance from the origin, so $r = |\alpha| = |a + bi|$ is just the absolute value of α. The angle θ has a special name: it is the *argument* of α.

Definition 5.15. *Let $\alpha = a + bi$ be a non-zero complex number, and suppose that α is represented in the complex plane by the point P. Let θ be the angle the ray $\overrightarrow{OP}$ makes with the positive real axis (or the positive x-axis). We call θ the argument of α. Note that we can take $0 \leq \theta < 2\pi$, or alternatively $-\pi \leq \theta < \pi$; each of these choices is sometimes called the Principal Argument of α.*

We collect the above facts in a useful Lemma.

[16]Normally, when we talk of angles, we are using the radian measure.

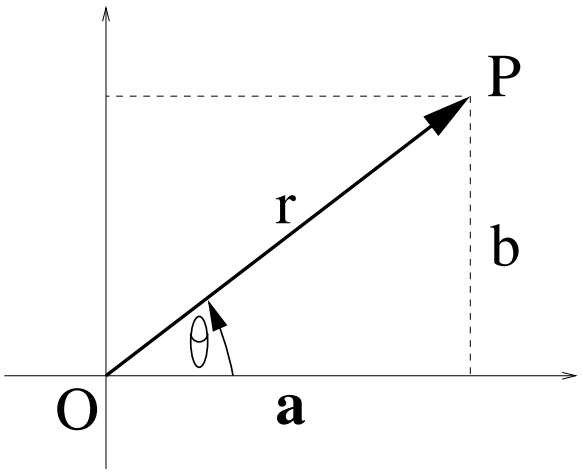


Figure 3: Cartesian coordinates (a, b), and by polar coordinates (r, θ) for the point P.

Lemma 5.16. *If $\alpha = a + bi$ is a non-zero complex number, r is its absolute value, and θ is its argument, then*

$$a = r\,\cos\theta, \qquad b = r\,\sin\theta,$$

and

$$\alpha = r(\cos\theta + i\,\sin\theta). \tag{25}$$

Moreover,

$$r = |\alpha| = \sqrt{a^2 + b^2}, \qquad b = a\tan\theta.$$

The expression on the right-hand side of (25) is called the (r, θ)-form of α. It is important to note that the equation $b = a\tan\theta$ is **not** by itself enough to determine θ, since $\tan(\theta) = \tan(\theta + 2\pi)$.

Example 5.17. *Write the following numbers in (r, θ)-form:*

$$3i, \qquad -2, \qquad -5i, \qquad -1 + i, \qquad \sqrt{3} + i.$$

Answer. For the first four of the complex numbers, a quick sketch will give us the argument and it is easy to get the (r, θ)-form. For example,

$$|-1 + i| = \sqrt{(-1)^2 + 1^2} = \sqrt{2}.$$

From the sketch, the argument of $-1 + i$ is $\pi/4 + \pi/2 = 3\pi/4$. Thus

$$-1 + i = \sqrt{2}\left(\cos\frac{3\pi}{4} + i\,\sin\frac{3\pi}{4}\right).$$

Similarly

$$3i = 3\left(\cos\frac{\pi}{2} + i\,\sin\frac{\pi}{2}\right), \qquad -2 = 2\left(\cos\pi + i\,\sin\pi\right),$$
$$-5i = 5\left(\cos\frac{3\pi}{2} + i\,\sin\frac{3\pi}{2}\right).$$

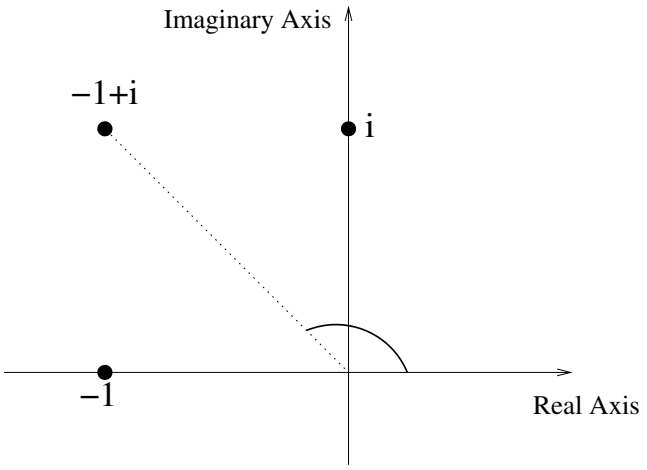


Figure 4: It is clear that the argument of $-1+i$ is $3\pi/4$.

Now let $\alpha = \sqrt{3}+i$. We see that

$$r = |\alpha| = \sqrt{\left(\sqrt{3}\right)^2 + 1^2} = \sqrt{4} = 2.$$

A sketch will not immediately give us the value of θ, but it is useful to make one anyway. Note that $\sin\theta = 1/2$ and $\cos\theta = \sqrt{3}/2$. Thus $\theta = \pi/6$. Hence the (r,θ)-form of α is

$$\alpha = 2\left(\cos\frac{\pi}{6} + i\,\sin\frac{\pi}{6}\right).$$

Multiplying and Dividing the (r,θ)-Form

Lemma 5.18. *Suppose θ_1, θ_2, θ are real. Then*

$$(\cos\theta_1 + i\,\sin\theta_1)(\cos\theta_2 + i\,\sin\theta_2) = \cos(\theta_1+\theta_2) + i\,\sin(\theta_1+\theta_2), \tag{26}$$

$$\frac{\cos\theta_1 + i\,\sin\theta_1}{\cos\theta_2 + i\,\sin\theta_2} = \cos(\theta_1-\theta_2) + i\,\sin(\theta_1-\theta_2), \tag{27}$$

and

$$\frac{1}{\cos\theta + i\,\sin\theta} = \cos\theta - i\,\sin\theta. \tag{28}$$

Proof. These are simple exercises based on the (hopefully) familiar identities

$$\begin{aligned}\sin(\theta_1+\theta_2) &= \sin\theta_1\cos\theta_2 + \sin\theta_2\cos\theta_1,\\ \cos(\theta_1+\theta_2) &= \cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2.\end{aligned}$$

For example, to prove (26):

$$\begin{aligned}&(\cos\theta_1 + i\,\sin\theta_1)(\cos\theta_2 + i\,\sin\theta_2)\\ &\qquad = (\cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2) + i\,(\sin\theta_1\cos\theta_2 + \sin\theta_2\cos\theta_1)\\ &\qquad = \cos(\theta_1+\theta_2) + i\,\sin(\theta_1+\theta_2).\end{aligned}$$

□

Theorem 5.19. *(De Moivre's Theorem) Suppose θ is real and n is an integer. Then*

$$(\cos\theta + i\,\sin\theta)^n = \cos n\theta + i\,\sin n\theta. \tag{29}$$

Proof. We shall first prove De Moivre's Theorem for non-negative n, using induction. It is clearly true for $n = 0$ since $1 = \cos 0 + i\sin 0$. Now suppose that (29) holds for a certain non-negative n. Then

$$\begin{aligned}(\cos\theta + i\,\sin\theta)^{n+1} &= (\cos\theta + i\,\sin\theta)^n\,(\cos\theta + i\,\sin\theta)\\ &= (\cos n\theta + i\,\sin n\theta)\,(\cos\theta + i\,\sin\theta)\\ &= \cos\{(n+1)\theta\} + i\,\sin\{(n+1)\theta\} \qquad \text{using (26).}\end{aligned}$$

This shows that (29) is true with n replaced by $n+1$. By induction, the identity (29) holds for all non-negative integers n. To prove (29) for negative n, use (28) and the identities:

$$\sin(-x) = -\sin(x), \qquad \cos(-x) = \cos(x).$$

□

Example 5.20. *Let n be an integer. We will show that*

$$\left(\sqrt{3}+i\right)^n + \left(\sqrt{3}-i\right)^n = 2^{n+1}\cos\frac{1}{6}n\pi.$$

Let $\alpha = \sqrt{3}+i$. Since we will be exponentiating, it is convenient to use the (r,θ)-form for α, which we have already worked out in Example 5.17:

$$\alpha = 2\left(\cos\frac{\pi}{6} + i\,\sin\frac{\pi}{6}\right).$$

By De Moivre's Theorem

$$\alpha^n = 2^n\left(\cos\frac{n\pi}{6} + i\,\sin\frac{n\pi}{6}\right)$$

Hence

$$\begin{aligned}\left(\sqrt{3}+i\right)^n + \left(\sqrt{3}-i\right)^n &= \alpha^n + \overline{\alpha^n}\\ &= 2^n\left(\cos\frac{n\pi}{6} + i\,\sin\frac{n\pi}{6}\right) + 2^n\left(\cos\frac{n\pi}{6} - i\,\sin\frac{n\pi}{6}\right)\\ &= 2^n\left(2\cos\frac{n\pi}{6}\right)\\ &= 2^{n+1}\cos\frac{n\pi}{6}.\end{aligned}$$

Example 5.21. *Simplify*

$$\frac{(\cos\theta - i\,\sin\theta)^5}{\cos 7\theta + i\,\sin 7\theta}.$$

Answer. From (28)

$$(\cos\theta - i\,\sin\theta)^5 = (\cos\theta + i\,\sin\theta)^{-5}.$$

By De Moivre,

$$\cos 7\theta + i\,\sin 7\theta = (\cos\theta + i\,\sin\theta)^7.$$

Thus

$$\begin{aligned}\frac{(\cos\theta - i\,\sin\theta)^5}{\cos 7\theta + i\,\sin 7\theta} &= \frac{(\cos\theta + i\,\sin\theta)^{-5}}{(\cos\theta + i\,\sin\theta)^7}\\ &= (\cos\theta + i\,\sin\theta)^{-12}\\ &= \cos(-12\,\theta) + i\,\sin(-12\,\theta)\\ &= \cos(12\,\theta) - i\,\sin(12\,\theta).\end{aligned}$$

Example 5.22. *De Moivre's Theorem is useful for reconstructing many formulae involving trigonometric functions. For example, letting $n = 2$ in De Moivre's Theorem we see that*

$$\begin{aligned}\cos 2\theta + i\,\sin 2\theta &= (\cos\theta + i\,\sin\theta)^2\\ &= \cos^2\theta - \sin^2\theta + i\cdot 2\sin\theta\cos\theta.\end{aligned}$$

Comparing the real and imaginary parts, we get the well-known identities

$$\cos 2\theta = \cos^2\theta - \sin^2\theta, \qquad \sin 2\theta = 2\,\sin\theta\cos\theta.$$

If you forget these identities, you can easily reconstruct them using De Moivre's Theorem.

It is useful to know that the identity for $\cos 2\theta$ is often given in the alternative form

$$\cos 2\theta = 2\cos^2\theta - 1 = 1 - 2\sin^2\theta$$

which may be deduced from the previous identity for $\cos 2\theta$ using $\cos^2\theta + \sin^2\theta = 1$.

Exercise 5.6. *Let α, β be non-zero complex numbers. Suppose that the points P, Q represent α and β on the complex plane. Show that OP is perpendicular to OQ if and only if α/β is imaginary.*

5.4 The Exponential Form of Complex Numbers

Definition 5.23. *Let θ be a real number. Define $e^{i\,\theta}$ by*

$$e^{i\theta} = \cos\theta + i\,\sin\theta.$$

Let $\alpha = t + i\theta$, where t and θ are real numbers. Define

$$e^{\alpha} = e^{t}\cdot e^{i\theta} = e^{t}\,(\cos\theta + i\,\sin\theta)$$

where e^t has the usual meaning for real t.

You may have seen this definition of $e^{i\theta}$ before, but it is surprising, and in need of some justification. One way to see that it is reasonable is to use the power series expansion (Taylor series) for e^z with $z = i\theta$, and compare to the series expansions of $\sin\theta$ and $\cos\theta$.

Taking $\theta = \pi$ gives $e^{i\pi} = -1$, which we may write as a remarkable identity linking five of the most important numbers in mathematics: $0, 1, i, e$ and π!

Euler's Identity. $e^{i\pi} + 1 = 0.$

Exercise 5.7. *Let $z = \pi/6 + i\log 2$. Write $e^{i\,z}$ in the form $a + b\,i$. (Careful! This is a trick question.)*

Exercise 5.8. *Let $\alpha = t + i\,\theta$ where t and θ are real.*

(i) Simplify $|e^{\alpha}|$ and $|e^{i\,\alpha}|$.

(ii) Show that the conjugate of e^{α} is $e^{\overline{\alpha}}$.

Now let α be any non-zero complex number. Lemma 5.16 tells us that we may write

$$\alpha = r(\cos\theta + i\,\sin\theta)$$

where r and θ are respectively the absolute value and the argument of α. We also recall that $e^{i\theta} = \cos\theta + i\,\sin\theta$. Thus we arrive at a very convenient representation of complex numbers.

Lemma 5.24. *Let α be a non-zero complex number. Then*

$$\alpha = re^{i\,\theta} \tag{30}$$

where $r = |\alpha| > 0$ and θ is the argument of α.

We call $re^{i\,\theta}$ the *exponential form* of the (non-zero) complex number α. The exponential form of complex numbers is very useful for multiplication, division and exponentiation of complex numbers.

Lemma 5.25. *Suppose r_1, r_2, r, θ_1, θ_2, θ_3 are real with $r_1, r_2 > 0$. Then*

$$r_1e^{i\theta_1}\cdot r_2e^{i\theta_2} = r_1r_2e^{i\,(\theta_1+\theta_2)}, \tag{31}$$

$$\frac{r_1e^{i\theta_1}}{r_2e^{i\theta_2}} = \frac{r_1}{r_2}e^{i\,(\theta_1-\theta_2)}, \tag{32}$$

and

$$\overline{(re^{i\,\theta})} = re^{-i\,\theta}. \tag{33}$$

Moreover, for n an integer,

$$\left(re^{i\,\theta}\right)^n = r^ne^{i\,n\theta}. \tag{34}$$

Proof. You should be able to deduce this theorem from Lemma 5.18 and Theorem 5.19. □

Example 5.26. *Use what you know about $e^{i\,\theta}$ to simplify*

$$\sum_{n=0}^{\infty}\frac{\cos(n\theta)}{2^n}.$$

Answer: *Note that the required sum is the real part of*

$$\begin{aligned}\sum_{n=0}^{\infty}\frac{\cos(n\theta)+i\sin(n\theta)}{2^n} &= \sum_{n=0}^{\infty}\left(\frac{e^{i\theta}}{2}\right)^n\\ &= \frac{1}{1-\frac{e^{i\theta}}{2}}\\ &= \frac{2}{2-\cos\theta-i\sin\theta}\\ &= \frac{2(2-\cos\theta+i\sin\theta)}{(2-\cos\theta)^2+\sin^2\theta}\\ &= \frac{2(2-\cos\theta+i\sin\theta)}{5-4\cos\theta}.\end{aligned}$$

Hence

$$\sum_{n=0}^{\infty} \frac{\cos(n\theta)}{2^n} = \frac{4 - 2\cos\theta}{5 - 4\cos\theta}.$$

Example 5.27. *Use what you know about $e^{i\,\theta}$ to simplify*

$$1 + \cos\left(\frac{\pi}{10}\right) + \cos\left(\frac{2\pi}{10}\right) + \cdots + \cos\left(\frac{9\pi}{10}\right). \tag{35}$$

We know that $\cos n\theta$ is the real part of $e^{i\,n\,\theta}$. Thus the sum (35) is the real part of

$$\begin{aligned}
1 + e^{\pi i/10} + e^{2\pi i/10} + \cdots + e^{9\pi i/10} &= \frac{e^{10\pi i/10} - 1}{e^{\pi i/10} - 1} \\
&= \frac{-2}{\cos(\pi/10) - 1 + i\,\sin(\pi/10)} \\
&= -2\frac{\cos(\pi/10) - 1 - i\,\sin(\pi/10)}{(\cos(\pi/10) - 1)^2 + \sin^2(\pi/10)} \\
&= -2\frac{\cos(\pi/10) - 1 - i\,\sin(\pi/10)}{\cos^2(\pi/10) + \sin^2(\pi/10) - 2\cos(\pi/10) + 1} \\
&= -2\frac{\cos(\pi/10) - 1 - i\,\sin(\pi/10)}{2 - 2\cos(\pi/10)} \\
&= \frac{\cos(\pi/10) - 1 - i\,\sin(\pi/10)}{\cos(\pi/10) - 1}.
\end{aligned}$$

Taking the real part we get

$$1 + \cos\left(\frac{\pi}{10}\right) + \cos\left(\frac{2\pi}{10}\right) + \cdots + \cos\left(\frac{9\pi}{10}\right) = \frac{\cos(\pi/10) - 1}{\cos(\pi/10) - 1} = 1.$$

Exercise 5.9. *Let α be a complex number. Describe geometrically what happens to α (in the complex plane) when it is multiplied by e^{it} (where t is real).*
Hint: *write α in exponential form.*

5.5 Roots of Complex Equations

Square roots and Quadratic Equations

The well-known method for solving quadratic equations work even when dealing with equations with complex coefficients. Since all complex numbers have square roots, all quadratic equations have solutions!

Theorem 5.28. *(Quadratic formula) Suppose a, b, c are complex numbers with $a \neq 0$. Then the (complex!) solutions to the quadratic equation*

$$ax^2 + bx + c = 0$$

are

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Proof. We complete the square and reorganise to get

$$\left(x + \frac{b}{2a}\right)^2 = \frac{b^2 - 4ac}{4a^2}.$$

Square-rooting both sides gives

$$x + \frac{b}{2a} = \pm\frac{\sqrt{b^2 - 4ac}}{2a}$$

from which the quadratic formula follows. □

To use this formula in practice you need to know how to find complex square roots. This is simplest in polar form:

Lemma 5.29. *The square roots of $z = re^{i\theta}$ are $\pm\sqrt{r}e^{i\theta/2}$.*

This is not hard to verify; we will consider more general nth roots later.

Make sure you have understood the argument in the proof of the quadratic formula before you answer this question.

Exercise 5.10. *Solve the equation $(x-i+1)^2 = -4$. (**Do not say, "expand the brackets, rearrange and use the quadratic formula"!!!**).*

n-th Roots

Just as the exponential form makes it easy to multiply and divide complex numbers, so it also makes it easy to find the n-th roots of complex numbers.

The trigonometric function $\sin\theta$ is periodic with period 2π. Thus if $\theta_1 - \theta_2 = 2\pi k$ where k is an integer, then $\sin\theta_1 = \sin\theta_2$. However the converse does not have to be true. By this we mean, if $\sin\theta_1 = \sin\theta_2$ then it is not necessarily true that $\theta_1 - \theta_2 = 2\pi k$ for some integer k. For example $\sin\pi/4 = \sin 3\pi/4$.

However, the function $e^{i\,\theta}$ has a very attractive property.

Lemma 5.30. *The function $e^{i\,\theta}$ is periodic with period 2π. Moreover, $e^{i\,\theta_1} = e^{i\,\theta_2}$ if and only if $\theta_1 - \theta_2 = 2\pi k$ for some integer k.*

The lemma follows from the properties of sin and cos.

Lemma 5.31. *Suppose α and β are non-zero complex numbers with exponential forms*

$$\alpha = re^{i\,\theta}, \qquad \beta = se^{i\,\phi}.$$

Suppose that n is a positive integer. Then $\alpha^n = \beta$ if and only if

$$r = s^{1/n}, \qquad \theta = \frac{\phi + 2\pi k}{n} \tag{36}$$

for some integer k.

Proof. Suppose that $\alpha^n = \beta$. Note that

$$r^n = |\alpha^n| = |\beta| = s.$$

But r and s are positive, so $r = s^{1/n}$. Cancelling $r^n = s$ from $\alpha^n = \beta$, we get

$$e^{i\,n\theta} = e^{i\,\phi}.$$

From Lemma 5.30 we see that

$$n\theta = \phi + 2\pi k,$$

for some integer k. Dividing by n gives (36).

Conversely, suppose that (36) holds for some integer k. Then

$$\alpha^n = r^n e^{i\,n\theta} = s\,e^{i\,\phi} \cdot e^{2\pi i\,k} = s\,e^{i\,\phi} = \beta,$$

as required. □

Apparently, the Lemma gives us infinitely many n-th roots of a complex number β: one for each value of k. This is not so! There is repetition, and there are only n *distinct* nth roots. The following theorem gives the n-th roots without repetition.

Theorem 5.32. *Let β be a non-zero complex number and let its exponential form be*

$$\beta = se^{i\,\phi}.$$

The n-th roots of β are

$$s^{1/n} \exp\left(\frac{(\phi + 2\pi\,k)i}{n}\right), \qquad k = 0, 1, 2, \ldots, n-1.$$

Proof. Exercise □

Example 5.33. *Find (all) the cube roots of -2.*

Answer. We note first that

$$-2 = 2\exp(\pi i).$$

Thus from the Theorem, the cube roots of -2 are

$$2^{1/3} \exp\left(\frac{(\pi + 2\pi k)i}{3}\right), \qquad k = 0, 1, 2.$$

These are

$$2^{1/3} \exp\left(\frac{\pi i}{3}\right) = 2^{1/3}\left(\cos \pi/3 + i\,\sin \pi/3\right) = 2^{1/3}\left(\frac{1}{2} + i\,\frac{\sqrt{3}}{2}\right)$$

$$2^{1/3} \exp\left(\pi\,i\right) = -2^{1/3}$$

$$2^{1/3} \exp\left(\frac{5\pi i}{3}\right) = 2^{1/3}\left(\cos 5\pi/3 + i\,\sin 5\pi/3\right) = 2^{1/3}\left(\frac{1}{2} - i\,\frac{\sqrt{3}}{2}\right).$$

The n-th Roots of Unity

It is worthwhile looking a little more closely at the n-th roots of 1. We can write 1 in exponential form as $1 = 1\exp(0 \cdot i)$. Theorem 5.32 tells us that the n-th roots of 1 are

$$\exp\left(\frac{2\pi\, k\, i}{n}\right) = \cos\frac{2\pi\, k}{n} + i\, \sin\frac{2\pi\, k}{n}, \qquad k = 0, 1, 2, \ldots, n-1.$$

If we write

$$\zeta = \exp\left(\frac{2\pi\, i}{n}\right)$$

then we see that the n-th roots of unity are

$$1, \zeta, \zeta^2, \ldots, \zeta^{n-1}.$$

It is easy to sketch the n-th roots of unity on the complex plane. They all have absolute value 1, so they lie on the circle with radius 1 and centre at the origin. The first one to draw is 1; you know where that one is. The next one is ζ. This is the one you get if start at 1 go around the circle in an anticlockwise direction through an angle of $2\pi/n$. To get ζ^2, start at ζ and go around the circle in an anticlockwise direction through an angle of $2\pi/n$, and so on. The points 1, ζ,...,ζ^{n-1} are equally spaced around the circle with an angle $2\pi/n$ between each one and the next. See Figure 5 for the cube and fourth roots of unity.

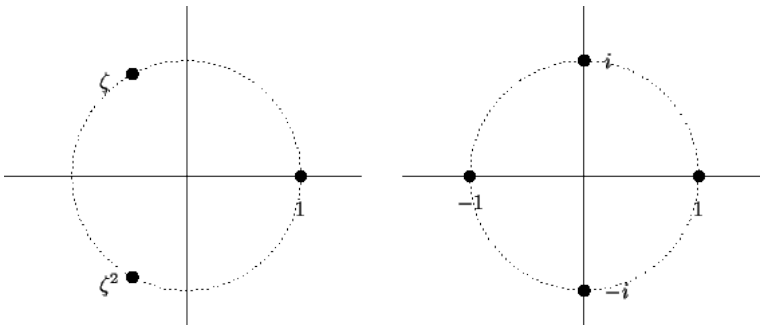


Figure 5: On the left, the three cube roots of unity: here $\zeta = e^{2\pi i/3}$. On the right, the fourth roots of unity. Note that $e^{2\pi i/4} = e^{\pi i/2} = i$, so the fourth roots of unity are 1, i, $i^2 = -1$, and $i^3 = -i$.

Example 5.34. *What is the sum of the n-th roots of unity?*

Answer.

$$1 + \zeta + \zeta^2 + \cdots + \zeta^{n-1} = \frac{\zeta^n - 1}{\zeta - 1} = \frac{1 - 1}{\zeta - 1} = 0.$$

Example 5.35. *Write down all the cube roots of unity.*

Answer. We can (and will) use the above recipe to write the cube roots of unity. But there is another (easier) way: the cube roots of unity are the roots of the polynomial $X^3 - 1$. By factoring

$$X^3 - 1 = (X - 1)(X^2 + X + 1).$$

and using the quadratic formula on the second factor, we see that the cube roots of unity are

$$1, \qquad \frac{-1+i\sqrt{3}}{2}, \qquad \frac{-1-i\sqrt{3}}{2}.$$

Having found them, what is the point of using the general recipe to find the cube roots of unity? Well, knowing the solution beforehand will allow us to check that the recipe that we wrote down is correct.

Using the general formula we find that the cube roots of unity are

$$\exp\left(\frac{2\pi\, k\, i}{3}\right) = \cos\frac{2\pi\, k}{3} + i\, \sin\frac{2\pi\, k}{3}, \qquad k = 0, 1, 2, \ldots, n-1.$$

These are

$$\begin{aligned} \cos 0 + i\, \sin 0 &= 1, \\ \cos\frac{2\pi}{3} + i \sin\frac{2\pi}{3} &= \frac{-1+i\sqrt{3}}{2}, \\ \cos\frac{4\pi}{3} + i \sin\frac{4\pi}{3} &= \frac{-1-i\sqrt{3}}{2}. \end{aligned}$$

For larger n, while it is always true that the n-th roots of unity are the roots of $X^n - 1$, for large values of n it is not convenient to use this fact to write down the n-th roots.

Summary. There are two square-roots of unity[17] and they add up to 0; there are three cube-roots of unity and they add up to 0; there are four fourth-roots of unity and they add up to 0; there are five fifth-roots of unity and they add up to 0; ...

Exercise 5.11. *Sketch the fifth and sixth roots of unity.*

General polynomial equations

The nth roots of unity are the roots of the polynomial equation $X^n - 1 = 0$. This equation has degree n and (as we have seen) has exactly n complex roots. In fact *every* equation of degree n has exactly n roots, provided that we count them correctly! To see why we have to count roots properly, note that the equation $X^2 = 0$ has only one root, 0, despite having degree 2. In the chapter on polynomials (see section 7.3) we'll see that $X = 0$ is a root of multiplicity 2, and the count comes out correctly.

[17] "Unity" is just another name for 1.

6 Sets, functions and relations

6.1 The languages of sets and logic

Mathematics has many pieces of notation which are impenetrable to the outsider. Some of these are just notation, and we have already met quite a few. See the table on page 1 (right at the beginning of these notes) for a quick reference.

The operations of union, $\cup$, and intersection, $\cap$, behave in some ways rather like $+$ and $\times$, and indeed in some early 20th century texts $A \cup B$ is written $A + B$ and $A \cap B$ is written AB. Let us first highlight some parallels:

Property	**Name**
$A \cup B = B \cup A \quad A \cap B = B \cap A$	Commutativity of $\cup$ and $\cap$
$x + y = y + x \qquad x \times y = y \times x$	Commutativity of $+$ and $\times$
$(A \cup B) \cup C = A \cup (B \cup C) \quad (A \cap B) \cap C = A \cap (B \cap C)$	Associativity of $\cup$ and $\cap$
$(x + y) + z = x + (y + z) \qquad (x \times y) \times z = x \times (y \times z)$	Associativity of $+$ and $\times$
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Distributivity of $\cap$ over $\cup$
$x \times (y + z) = (x \times y) + (x \times z)$	Distributivity of $\times$ over $+$

However there are also some sharp contrasts:

Property	**Name**
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	Distributivity of $\cup$ over $\cap$
$x + (y \times z) \neq (x + y) \times (x + z)$	Non-distributivity of $+$ over $\times$

Each of the properties of $\cup$ and $\cap$ listed is fairly easy to prove. For example, to show that

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \tag{37}$$

we reason as follows. First, saying that sets X and Y are equal is the same as saying that $X \subseteq Y$ and $Y \subseteq X$. So we have to show

1. $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$, and
2. $A \cap (B \cup C) \supseteq (A \cap B) \cup (A \cap C)$.

To show the first inclusion, suppose that $x \in A \cap (B \cup C)$. Then $x \in A$ and $x \in B \cup C$. This means $x \in A$ and *either* $x \in B$ *or* $x \in C$ (or both[18]). Therefore *either*

$$x \in A \text{ and } x \in B$$

[18] we will *always* use "or" in this inclusive sense, as meaning one or the other or both, and will stop saying "or both" from now on

or

$$x \in A \text{ and } x \in C$$

That is, $x \in (A \cap B) \cup (A \cap C)$.

To show the second inclusion, suppose that $x \in (A \cap B) \cup (A \cap C)$. Then either $x \in A \cap B$ or $x \in A \cap C$, so either

$$x \in A \text{ and } x \in B$$

or

$$x \in A \text{ and } x \in C.$$

Both alternatives imply $x \in A$, so this much is sure. Moreover, the first alternative gives $x \in B$ and the second gives $x \in C$, so as one alternative or the other must hold, x must be in B or in C. That is, $x \in B \cup C$. As $x \in A$ and $x \in B \cup C$, we have $x \in A \cap (B \cup C)$, as required. We have proved "distributivity of $\cap$ over $\cup$".

In this proof we have simply translated our terms from the language of $\cup$ and $\cap$ to the language of *or* and *and*. In logic, the symbols $\vee$, meaning "or", and $\wedge$, meaning "and" are used (see the table on page 1); the resemblance they bear to $\cup$ and $\cap$ is not a coincidence. For example, it is the definition of the symbols $\cup$ and $\cap$ that

$$x \in A \cup B \iff (x \in A) \vee (x \in B).$$

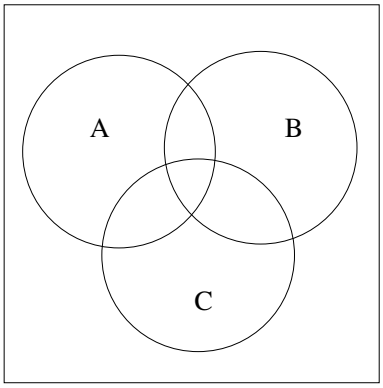
and

$$x \in A \cap B \iff (x \in A) \wedge (x \in B).$$

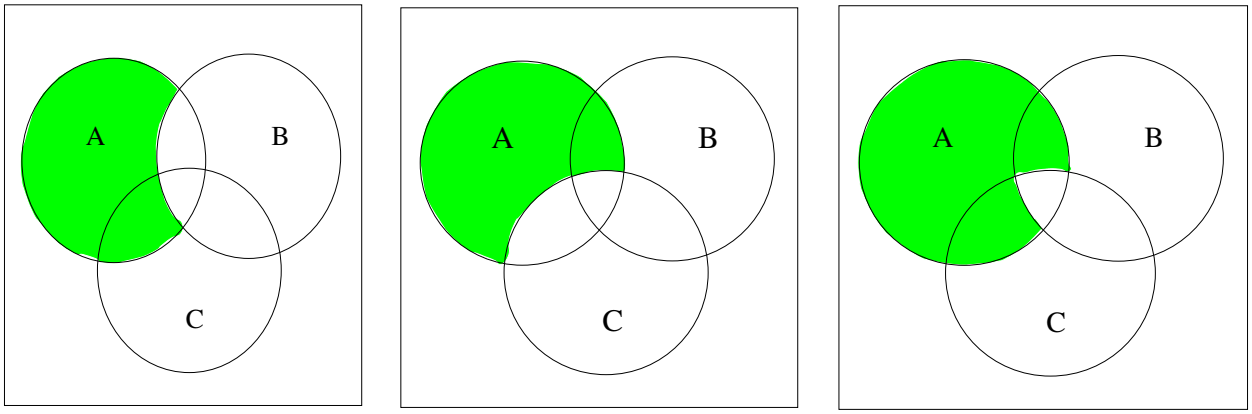
Many proofs in this area amount to little more than making this translation.

Exercise 6.1. *(i) Prove that $x \notin B \cap C$ if and only if $x \notin B$ or $x \notin C$.*
(ii) Go on to show that $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$.

In deciding whether equalities like the one you've just been asked to prove are true or not, *Venn diagrams* can be very useful. A typical Venn diagram looks like this:



It shows three sets A, B, C as discs contained in a larger rectangle, which represents the set of all the things being discussed. For example we might be talking about sets of integers, in which case the rectangle represents $\mathbb{Z}$, and A, B and C represent three subsets of $\mathbb{Z}$. Venn diagrams are useful because we can use them to guide our thinking about set-theoretic equalities. The three Venn diagrams below show, in order, $A \setminus B$, $A \setminus C$ and $A \setminus (B \cap C)$. They certainly *suggest* that $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$ is always true.



Exercise 6.2. *Let $A, B, C, \ldots$ be sets.*
(i) Which of the following is always true?

1. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
2. $A \setminus (B \setminus C) = (A \setminus B) \cup C$
3. $A \setminus (B \cup C) = (A \setminus B) \setminus C$
4. $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$

(ii) For each statement in (i) which is not always true, draw Venn diagrams showing three sets for which the equality does not hold.

The general structure of the proof of an equality in set theory is exemplified with our proof of distributivity of $\cap$ over $\cup$, (37). Let us consider another example. Distributivity of $\cup$ over $\cap$ is the statement

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C). \tag{38}$$

We translate this to

$$x \in A \vee (x \in B \wedge x \in C) \Longleftrightarrow (x \in A \vee x \in B) \wedge (x \in A \vee x \in C). \tag{39}$$

Let us go a stage further. There is an underlying logical statement here:

$$a \vee (b \wedge c) \Longleftrightarrow (a \vee b) \wedge (a \vee c). \tag{40}$$

In (40), the particular statements making up (39), "$x \in A$", "$x \in B$" etc., are replaced by letters a, b, etc. denoting completely general statements, which could be anything at all — "It is raining", "8 is a prime number", etc. Clearly (39) is a particular instance of (40). If we succeed in showing that (40) is always true, regardless of the statements making it up, then we will have proved (39) and therefore (38).

We broke up the proof of distributivity of $\cap$ over $\cup$, (37), into two parts. In each, after translating to the language of $\vee, \wedge$ and $\Longrightarrow$, we did a bit of work with "and" and "or", at the foot of page 48 and the top of page 49, which was really just common sense. Most of the time common sense is enough to for us to see the truth of the not very complex logical statements underlying the set-theoretic equalities we want to prove, and perhaps you can see that (40) is always true, no matter what a, b and c are[19]. But occasionally common sense deserts us, or we would like something a little more reliable. We now introduce a thoroughly reliable technique for checking these statements, and therefore for proving set theoretic equalities.

[19] or of the implications from left to right and right to left separately, as we did in the proof of (37)

6.2 Truth Tables

The significance of the logical connectives $\vee$, $\wedge$ and $\Longleftrightarrow$ is completely specified by the following tables, which show what are the "truth value" (True or False) of $a \vee b$, $a \wedge b$ and $a \Longleftrightarrow b$, given the various possible truth-values of a and b. Note that since there are two possibilities for each of a and b, there are $2^2 = 4$ possibilities for the two together, so each table has 4 rows.

a	$\vee$	**b**
T	**T**	T
T	**T**	F
F	**T**	T
F	**F**	F

a	$\wedge$	**b**
T	**T**	T
T	**F**	F
F	**F**	T
F	**F**	F

a	$\Longleftrightarrow$	**b**
T	**T**	T
T	**F**	F
F	**F**	T
F	**T**	F

(41)

We now use these tables to decide if (40) is indeed always true, whatever are the statements a, b and c. Note first that now there are now $2^3 = 8$ different combinations of the truth values of a, b and c, so 8 rows to the table. I've added a last row showing the order in which the columns are filled in: the columns marked 0 contain the truth assignments given to the three atomic statements a, b and c. The columns marked 1 are calculated from these; the left hand of the two columns marked 2 is calculated from a column marked 0 and a column marked 1; the right hand column marked 2 is calculated from two columns marked 1; and the column marked 3 is calculated from the two columns marked 2. The different type faces are just for visual display.

$\big(a$	$\vee$	$(b$	$\wedge$	$c)\big)$	$\Longleftrightarrow$	$\big(a$	$\vee$	$b)$	$\wedge$	$(a$	$\vee$	$c)\big)$
T	**T**	T	T	T	**T**	T	T	T	**T**	T	T	T
T	**T**	T	F	F	**T**	T	T	T	**T**	T	T	F
T	**T**	F	F	T	**T**	T	T	F	**T**	T	T	T
T	**T**	F	F	F	**T**	T	T	F	**T**	T	T	F
F	**T**	T	T	T	**T**	F	T	T	**T**	F	T	T
F	**F**	T	F	F	**T**	F	T	T	**F**	F	F	F
F	**F**	F	F	T	**T**	F	F	F	**F**	F	T	T
F	**F**	F	F	F	**T**	F	F	F	**F**	F	F	F
0	2	0	1	0	3	0	1	0	2	0	1	0

(42)

Because the central column consists entirely of T's, we conclude that it *is* true that (40) always holds.

The parallel between the language of set theory and the language of $\vee$ and $\wedge$ goes further if we add to the latter the words "implies" and "not". These two are denoted $\Longrightarrow$ and $\neg$. The symbol $\neg$ is used to negate a statement: $\neg(x \in X)$ means the same as $x \notin X$; "$\neg$ (n is prime)" means the same as "n is not prime". Here are some translations from one language

to the other.

Language of $\cup, \cap, \smallsetminus, \subseteq$		**Language of** $\vee, \wedge, \neg, \implies$
$\{x \in X : \mathrm{P}(x)\} \cup \{x \in X : \mathrm{Q}(x)\}$	$=$	$\{x \in X : \mathrm{P}(x) \vee \mathrm{Q}(x)\}$
$\{x \in X : \mathrm{P}(x)\} \cap \{x \in X : \mathrm{Q}(x)\}$	$=$	$\{x \in X : \mathrm{P}(x) \wedge \mathrm{Q}(x)\}$
$X \smallsetminus \{x \in X : \mathrm{P}(x)\}$	$=$	$\{x \in X : \neg\, \mathrm{P}(x)\}$
$\{x \in X : \mathrm{P}(x)\} \smallsetminus \{x \in X : \mathrm{Q}(x)\}$	$=$	$\{x \in X : \mathrm{P}(x) \wedge \neg \mathrm{Q}(x)\}$
$\{x \in X : \mathrm{P}(x)\} \subseteq \{x \in X : \mathrm{Q}(x)\}$	$\iff$	$\forall x \in X \ \big(\mathrm{P}(x) \implies \mathrm{Q}(x)\big)$
$\{x \in X : \mathrm{P}(x)\} = \{x \in X : \mathrm{Q}(x)\}$	$\iff$	$\forall x \in X \ \big(\mathrm{P}(x) \iff \mathrm{Q}(x)\big)$

In the table we introduce the symbol $\forall$, meaning "for all". This symbol is called a *quantifier* (specifically, it the *universal quantifier*) and a statement which starts with it (such as (44) below) is called a quantified statement. There is a second quantifier, $\exists$, which means "there exists". For example, the statement

$$\exists z \in \mathbb{C} : z^2 = -1$$

asserts the existence of a square root of minus one in the field $\mathbb{C}$ of complex numbers. (There are in fact two, but that does not matter.)

The truth tables for $\implies$ and $\neg$ are as follows:

a	$\implies$	**b**
T	**T**	T
T	**F**	F
F	**T**	T
F	**T**	F

$\neg$	**a**
F	T
T	F

(43)

The truth table for $\implies$ often causes surprise. The third row seem rather odd: if a is false, then how can it claim the credit for b's being true? The last line is also slightly peculiar, although possibly less than the third. There are several answers to these objections. The first is that in ordinary language we are not usually interested in implications where the first term is known to be false, so we don't usually bother to assign them any truth value. The second is that in fact, in many cases we *do* use "implies" in this way. For example, we have no difficulty in agreeing that the statement

$$\forall x \in \mathbb{Z} \ \ (x > 1 \implies x^2 > 2) \tag{44}$$

is true. But among the infinitely many implications it contains (one for each integer!) are

$$0 > 1 \implies 0^2 > 2,$$

an instance of an implication with both first and second term false, as in the last line in the truth table for $\implies$, and

$$-3 > 1 \implies 9 > 2,$$

an implication with first term false and second term true, as in the third line in the truth table for $\implies$. If we were to give these implications any truth value other than T, then we could no longer use the universal quantifier in (44).

Exercise 6.3. *Use truth tables to show*

1. $(a \implies b) \iff (\neg a \vee b)$
2. $(a \implies b) \iff (\neg b \implies \neg a)$
3. $\neg(a \implies b) \iff (a \wedge \neg b)$

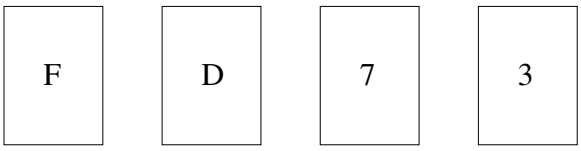
Exercise 6.4. *Another justification for the (at first sight surprising) truth table for* $\implies$ *is the following: we would all agree that*

$$\Big(a \wedge \big(a \implies b\big)\Big) \implies b$$

should be a tautology. Show that

1. *It is, if the truth table for* $\implies$ *is as stated.*
2. *It is not, if the third or fourth lines in the truth table for* $\implies$ *are changed.*

Exercise 6.5. *Each of the four cards shown has a number on one side and a letter on the other.*



Which cards do you need to turn over to check whether it is true that every card with a "D" on one side has a "7" on the other?

Tautologies and Contradictions

The language of $\vee, \wedge, \implies, \iff, \neg$ is called the Propositional Calculus, which is part of Logic. Mathematicians use some of the logical symbols we have introduced all the time (including $\forall$, $\exists$, $\implies$, $\iff$) but do not use $\vee$, $\wedge$ and $\neg$ much. In fact the symbol $\wedge$ has other uses in mathematics (for example, in vector calculus) which are much more common. Since this is a course in Mathematics and not Logic, we will not use those three after this chapter.

There are two more ideas from logic which are useful and common in mathematical discussion which we will mention briefly here. A statement in the Propositional Calculus is a *tautology* if it always holds, no matter what the truth-values of the atoms $a, b, c, \ldots$ of which it is composed. We have shown above that (40) is a tautology, and the statements of Exercise 6.3 are also examples. The word "tautology" is also used in ordinary language to mean a statement that is true but conveys no information, such as "all bachelors are unmarried" or "it takes longer to get up north the slow way".

The opposite of a tautology is a *contradiction*, a statement that is always false. The simplest is

$$a \wedge \neg a.$$

If a statement implies a contradiction, then we can see from the truth table that it must be false: consider, for example,

a	$\Longrightarrow$	$\Big(b$	$\wedge$	$(\neg$	$b)\Big)$
T	F	T	F	F	T
T	F	F	F	T	F
F	T	T	F	F	T
F	T	F	F	T	F

The only circumstance under which the implication can be true is if a is false. This is the logic underlying a proof by contradiction. We *prove* that some statement a implies a contradiction (so that the *implication* is true) and deduce that a must be false.

Dangerous Complements and de Morgan's Laws

If you have seen any set theory before, you may have spotted one operation which has missing from our discussion so far, namely the *complement* of a set. We would like to define A^c, the complement of A, as "everything that is not in A." But statements involving "everything" are dangerous, for reasons having to do with the logical consistency of the subject. Indeed, Bertrand Russell provoked a crisis in the early development of set theory with his idea of *the set of all sets which are not members of themselves.* If this set is not a member of itself, then by its definition it is a member of itself, which implies that it is not, which means that it is, ... One result of this self-contradictory definition (known as *Russell's paradox*) was that mathematicians became wary of speaking of "the set of all x with property P". Instead, they restricted themselves to the elements of sets they were already sure about: "the set of all $x \in X$ with property P" is OK provided X itself is already a well defined set.

Therefore for safety reasons, when we speak of the *complement* of a set, we always mean its complement *in whatever realm of objects we are discussing* [20]. In fact many people never use the term "complement" on its own, but always qualify it by saying with reference to what. Rather than saying "the complement of the set of even integers", we say "the complement in $\mathbb{Z}$ of the set of even integers". Otherwise, the reader has to guess what the totality of the objects we are discussing is. Are we talking about integers, or might we be talking about rational numbers (of which integers are a special type)? The complement in $\mathbb{Q}$ of the set of integers is the set of rationals with denominator greater than 1; the complement in $\mathbb{Z}$ of the set of integers is obviously the empty set. It is important to be precise.

The problem with precision is that it can lead to ponderous prose. Sometimes the elegance and clarity of a statement can be lost if we insist on making it with maximum precision. A case in point is the two equalities in set theory which are known as "de Morgan's Laws", after the nineteenth century British mathematician Augustus de Morgan. Both involve the complements of sets. Rather than qualifying the word "complement" every time it occurs, we adopt the convention that all occurrences of the word "complement" refer to the same universe of discourse. It does not matter what it is, so long as it is the same one at all points in the statement.

With this convention, we state the two laws. They are

$$(A \cap B)^c = A^c \cup B^c \tag{45}$$

[20] The term "universe of discourse" is sometimes used in place of the vague "realm of objects we are discussing".

and

$$(A \cup B)^c = A^c \cap B^c \tag{46}$$

Using the more precise notation "$X \setminus A$" (for the set $\{x \in X : x \notin A\}$) in place of A^c, these can be restated, less succinctly, as

$$X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B) \tag{47}$$

and

$$X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B) \tag{48}$$

Complements are the set-theoretic counterparts to negation in logic. In fact, proving de Morgan's laws simply amounts to showing that the statements

$$\neg(a \wedge b) \Longleftrightarrow \neg a \vee \neg b$$

and

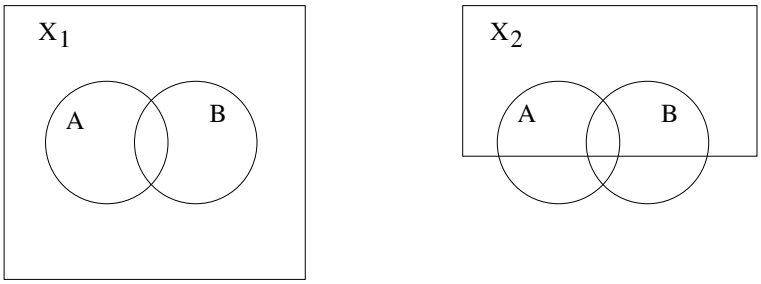
$$\neg(a \vee b) \Longleftrightarrow \neg a \wedge \neg b$$

are tautologies.

Exercise 6.6. *1. On a Venn diagram draw $(A \cap B)^c$ and $(A \cup B)^c$.*

2. Prove de Morgan's Laws. You can use truth tables, or you can use an argument, like the one we used to prove distributivity of $\cap$ over $\cup$, (37), which involves an appeal to common sense. Which do you prefer?

It is worth noting that for de Morgan's Laws to hold we do not need to assume that A and B are contained in X. The diagram overleaf shows a universe X_1 containing A and B, and another, X_2, only partially containing them. De Morgan's laws hold in both cases.



6.3 Functions and mappings

What is counting? The standard method we all learn as children is to assign, to each of the objects we are trying to count, a natural number, in order, beginning with 1, and leaving no gaps. The last natural number used is "the number of objects". This process can be summarised as "establishing a one-to-one correspondence between the set of objects we are counting and an initial segment of the natural numbers".

Definition 6.1. *(i) Let A and B be sets. A* **one-to-one correspondence** *between the two sets is the assignment, for each member of the set A, of a member of the set B, in such a way that the elements of the two sets are paired off. Each member of A must be paired with one, and only one, member of B, and vice-versa.*

(ii) The set A is **finite** *if there is a one-to-one correspondence between A and some subset*[21] *$\{1, 2, \ldots, n\}$ of $\mathbb{N}$. In this case n is the* **cardinality** *(or* **number of elements***) of A.*

(iii) The set A is **infinite** *if it is not finite.*

When we count the oranges in a basket, we are determining a one-to-one correspondence between some initial segment $\{1, 2, \ldots, n\}$ of $\mathbb{N}$ and the set {oranges in the basket}.

The set of integers modulo n consists of $\{0, 1, 2, \ldots, n-1\}$. The complex nth roots of 1 are $1, e^{2\pi i/n}, \ldots, e^{2k\pi i/n}, \ldots, e^{2(n-1)\pi i/n}$. There is a one-to-one correspondence between the integers modulo n and the set of n'th roots of unity: we simply map $k \mapsto e^{2k\pi i/n}$ for $0 \leq k \leq n-1$.

Example 6.2. There can be one-to-one correspondences between pairs of infinite sets as well as between pairs of finite sets.

1. We saw on page 17 that there is a one-to-one correspondencebetween the natural numbers $\mathbb{N}$ and the set $\mathcal{S}$ of subgroups of $\mathbb{Z}$. The natural number n can be paired, or associated with, the subgroup $n\mathbb{Z}$. Proposition 3.2 proves that each member of $\mathcal{S}$ is generated by some natural number, so the assignment

$$n \in \mathbb{N} \mapsto n\mathbb{Z} \in \mathcal{S}$$

   determines a one-to-one correspondence.

2. Let $\mathbb{R}_{>0}$ denote the set of strictly positive real numbers. The rule

$$x \in \mathbb{R} \mapsto \log x \in \mathbb{R}$$

   determines a one-to-one correspondence between $\mathbb{R}_{>0}$ and $\mathbb{R}$.

3. The rule

$$x \in \mathbb{R} \mapsto e^x \in \mathbb{R}_{>0}$$

   also determines a one-to-one correspondence.

4. The mapping $f(n) = 2n$ determines a one-to-one correspondence from $\mathbb{Z}$ to $2\mathbb{Z}$.

[21] This is what we mean by "initial segment". When $n - 0$, this is the empty set.

5. One can construct a bijection from $\mathbb{N}$ to $\mathbb{Z}$. For example, one can map the even numbers to the positive integers and the odd numbers to the negative integers, by the rule

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

One-one correspondences are examples of *functions* or *mappings*. If A and B are sets then a mapping from A to B is a rule which associates to each element of A **one and only one** element of B. In this case A is the *domain* of the mapping, and B is its *codomain*[22]. We usually give mappings a label, such as f or g, and use the notation $f : A \to B$ to indicate that f is a mapping from A to B. We say that f *maps* the element $a \in A$ to the element $f(a) \in B$. We also say that $f(a)$ is the *image* of the element a under f. The image of the whole set A under f is the set $\{b \in B : \exists a \in A \text{ such that } f(a) = b\}$, which can also be described as $\{f(a) : a \in A\}$; this set is denoted $f(A)$ or $\mathrm{im}(f)$ and is called the *image of* f.

Example 6.3. There is a mapping $m : \{\text{Men}\} \to \{\text{Women}\}$ defined by $m(x) =$ mother of x. It is a well-defined mapping, because each man has precisely one mother. But it is not a one-to-one correspondence, first because the same woman may be the mother of several men, and second because not every woman is the mother of some man.

2. The recipe

$$x \mapsto \text{ son of } x$$

does *not* define a mapping from {Women} to {Men}. The reasons are the same as in the previous example: not every woman has a son, so the rule does not succeed in assigning to each member of {Women} a member of {Men}, and moreover some women have more than one son, and the rule does not tell us which one to assign.

Definition 6.4. *Let $f : A \to B$ be a mapping.*

- *f is* **injective***, or* **one-to-one***, if different elements of A are mapped to different elements of B. That is, f is injective if*

$$a_1 \neq a_2 \quad \Longrightarrow \quad f(a_1) \neq f(a_2),$$

or equivalently if

$$f(a_1) = f(a_2) \implies a_1 = a_2$$

for all $a_1, a_2 \in A$.

- *f is* **surjective***, or* **onto***, if every element of B is the image of some element of A. That is, f is surjective if for all $b \in B$ there exists $a \in A$ such that $f(a) = b$, or, in other words, if $f(A) = B$.*

- *f is* ***bijective*** *if it is both injective and surjective.*

The corresponding nouns are **injection**, **surjection** *and* ***bijection****. A one-to-one correspondence is nothing other than a bijective map or bijection:*

Proposition 6.5. *The mapping $f : A \to B$ is a one-to-one correspondence if and only if it is both injective and surjective.* □

[22]The words *source* and *target* are sometimes used in place of domain and codomain.

Example 6.6. The mapping (function) $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$ is neither injective nor surjective. However, if we restrict its codomain to $\mathbb{R}_{\geq 0}$ (the non-negative reals) then it becomes surjective: $f : \mathbb{R} \to \mathbb{R}_{\geq 0}$ is surjective. And if we restrict its domain to $\mathbb{R}_{\geq 0}$, it becomes injective.

Exercise 6.7. *Which of the following is injective, surjective or bijective:*

1. $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^3$
2. $f : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$, $f(x) = \frac{1}{x}$
3. $f : \mathbb{R} \setminus \{0\} \to \mathbb{R}$, $f(x) = \frac{1}{x}$
4. $f : \mathbb{R} \setminus \{0\} \to \mathbb{R} \setminus \{0\}$, $f(x) = \frac{1}{x}$
5. $f : \{Countries\} \to \{Cities\}$, $f(x) =$ *Capital city of* x
6. $f : \{Cities\} \to \{Countries\}$, $f(x) =$ *Country in which* x *lies*

Proposition 6.7. The pigeonhole principle. *If A and B are finite sets with the same number of elements, and $f : A \to B$ is a mapping then*

$$f \text{ is injective} \iff f \text{ is surjective.}$$

Proof. Let $n = |A| = |B|$ and label the elements $A = \{a_1, a_2, \ldots, a_n\}$, $B = \{b_1, b_2, \ldots, b_n\}$. Now f maps A to the set $f(A) = \{f(a_1), f(a_2), \ldots, f(a_n)\} \subseteq B$.

If f is injective then there are no repeats in this list, so $f(A)$ contains n distinct elements; hence $f(A) = B$ and f is surjective.

If f is not injective, then $f(a_i) = f(a_j)$ for some i, j with $i \neq j$. But then the list contains at most $n - 1$ elements so does not contain all elements of B, and so f is not surjective. □

This is one of those proofs which may either seem completely obvious to you, or incomprehensible (or even both, depending on the day of the week it is). So I will give a second proof, in case you prefer it.

Proof. Label the elements of B as $b_1, \ldots, b_n$. For $1 \leq i \leq n$ let m_i be the number of elements $a \in A$ such that $f(a) = b_i$. Then $m_1 + m_2 + \cdots + m_n = n$ and all $m_i \geq 0$.

Now f is surjective $\iff$ all $m_i \geq 1$, while f is injective $\iff$ all $m_i \leq 1$. But these are both clearly equivalent to $m_1 = m_2 = \cdots = m_n = 1$. □

The pigeonhole principle is false for infinite sets. For example,

- the map $\mathbb{N} \to \mathbb{N}$ defined by $f(n) = n + 1$ is injective but not surjective.
- The map $\mathbb{N} \to \mathbb{N}$ defined by

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

  is surjective but not injective.
- The map $\mathbb{N} \to \mathbb{N}$ defined by $n \mapsto 2^n$ is injective but not surjective.

Definition 6.8. *Let A, B and C be sets, and let $f : A \to B$ and $g : B \to C$ be mappings. Then the* **composition** *of f and g, denoted $g \circ f$, is the mapping $A \to C$ is defined by*

$$g \circ f(a) = g(f(a)).$$

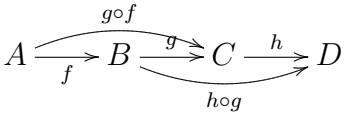
Note that $g \circ f$ means "do f first and then g".

Example 6.9. *1. Consider $f : \mathbb{R}_{>0} \to \mathbb{R}$ defined by $f(x) = \log x$ and $g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = \cos x$. Then $g \circ f(x) = \cos(\log x)$ is a well defined function, but $f \circ g$ is not: where $\cos x < 0$, $\log(\cos x)$ is not defined.*

2. In order that $g \circ f$ be well-defined, it is necessary that the image of f should be contained in the domain of g.

(ii) The function $h : \mathbb{R} \to \mathbb{R}$ defined by $h(x) = x^2 + x$ can be written as a composition: define $f : \mathbb{R} \to \mathbb{R}^2$ by $f(x) = (x, x^2)$ and $a : \mathbb{R}^2 \to \mathbb{R}$ by $g(x, y) = x + y$; then $h = a \circ f$.

Proposition 6.10. *If $f : A \to B, g : B \to C$ and $h : C \to D$ are mappings, then the compositions $h \circ (g \circ f)$ and $(h \circ g) \circ f$ are equal.*



Proof. For any $a \in A$,

$$(h \circ (g \circ f))(a) = h((g \circ f)(a)) = h(g(f(a)) = (h \circ g)(f(a)) = ((h \circ g) \circ f)(a).$$

□

Exercise 6.8. *Suppose that $f : A \to B$ and $g : B \to C$ are mappings. Show that*

1. *f and g both injective $\implies$ $g \circ f$ injective*
2. *f and g both surjective $\implies$ $g \circ f$ surjective*
3. *f and g both bijective $\implies$ $g \circ f$ bijective*

and find examples to show that

1. *f injective, g surjective $\not\implies$ $g \circ f$ surjective*
2. *f surjective, g injective $\not\implies$ $g \circ f$ surjective*
3. *f injective, g surjective $\not\implies$ $g \circ f$ injective*
4. *f surjective, g injective $\not\implies$ $g \circ f$ injective*

Suppose that I want to show that two sets A and B have the same number of elements. One way would be to count the elements of each and then compare the results. But suppose instead that I can find a a 1-1 correspondence $\varphi : A \to B$. Then *A and B must have the same number of elements.* The reason is simple: suppose that B has n elements. Then there is a 1-1 correspondence $\psi : B \to \{1, 2, \ldots, n\}$. Because the composite of 1-1 correspondences is a 1-1 correspondence (6.8(3)), $\psi \circ \varphi : A \to \{1, 2, \ldots, n\}$ is also a 1-1-correspondence, so that A too has n elements. A substantial part of mathematics is devoted to finding clever 1-1 correspondences between sets, in order to be able to conclude that they have the same number of elements without having to count them.

Example 6.11. 1. A silly example: the rule

$$x \in \{\text{Husbands}\} \mapsto \quad \text{wife of } x \in \{\text{Wives}\}$$

determines a one-to-one correspondence between the set of husbands and the set of wives, assuming, that is, that everyone who is married, is married to just one person, of the opposite sex. Although the example is lighthearted, it does illustrate the point: if you want to show that two sets have the same number of elements, it may be more interesting to look for a one-to-one correspondencebetween them, using some understanding of their structure and relation, than to count them individually and then compare the numbers. This is especially the case in mathematics, where structure permeates everything.

2. For a natural number n, let $\mathscr{D}(n)$ (for "divisors") denote the set of natural numbers which divide n (with quotient a natural number). There is a one-to-one correspondence between the set $\mathscr{D}(144)$ of factors of 144 and the set $\mathscr{D}(2025)$ of factors of 2025. One can establish this by counting the elements of both sets; each has 15 members. More interesting is to appreciate that the coincidence is due to the similarity of the prime factorisations of 144 and 2025:

$$144 = 2^4 \times 3^2, \qquad 2025 = 3^4 \times 5^2;$$

once one has seen this, it becomes easy to describe a one-to-one correspondence without needing to enumerate the members of the sets $\mathscr{D}(144)$ and $\mathscr{D}(2025)$: every divisor of 144 is equal to $2^i 3^j$ for some i between 0 and 4 and some j between 0 and 2. It is natural to make $2^i 3^j$ correspond to $3^i 5^j \in \mathscr{D}(2025)$.

Exercise 6.9. *Which pairs among*

$$64, 144, 729, 900, 11025$$

have the same number of factors?

Exercise 6.10. *Show the number of ways of choosing k from n objects is equal to the number of ways of choosing $n-k$ from n objects. Can you do this without making use of a formula for the number of choices?*

Exercise 6.11. *Denote the number of elements in a finite set X by $|X|$. Suppose that A and B are finite sets. Then*

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

(i) Can you explain why? Can you write out a proof? If this is too trying, go on to
(ii) What is the corresponding formula for $|A \cup B \cup C|$ when A, B and C are all finite sets? And for $|A \cup B \cup C \cup D|$? For $|A_1 \cup \cdots \cup A_n|$?

6.4 Inverses

Here's a definition which does not look to be very useful at first sight, but will turn out to be.

Definition 6.12. *For any set A the **identity map** $A \to A$ is the map $\mathrm{id}_A : A \to A$ defined by $\mathrm{id}_A(x) = x$ for all $x \in A$.*

The identity map has the property that when we compose it with any other map there is no change; rather like multiplying by the number 1:

Lemma 6.13. *Let A, X, Y be any sets and $f : X \to A$ and $g : A \to Y$ any maps. Then*

$$\mathrm{id}_A \circ f = f \qquad \text{and} \qquad g \circ \mathrm{id}_A = g.$$

Proof. The is obvious from the definition, as this picture should make clear.

$$X \xrightarrow{f} A \xrightarrow{\mathrm{id}_A} A \xrightarrow{g} Y$$
$$\mathrm{id}_A \circ f \qquad g \circ \mathrm{id}_A$$

□

Definition 6.14. *If $f : A \to B$ is a mapping then a mapping $g : B \to A$ is*

- *a* **left inverse** *to f if $g \circ f = \mathrm{id}_A$ (that is, if $g(f(a)) = a$ for all $a \in A$),*
- *a* **right inverse** *to f if $f \circ g = \mathrm{id}_B$ (that is, if $f(g(b)) = b$ for all $b \in B$).*
- *an* **inverse** *of f if it is both a right and a left inverse of f, (that is, $g \circ f = \mathrm{id}_A$ and $f \circ g = \mathrm{id}_B$).*

Be careful! A right inverse or a left inverse is not necessarily an inverse. This is a case where mathematical use of language differs from ordinary language. A large cat is always a cat, but a left inverse is not always an inverse.

It is immediate from the definition that f is a left inverse to g if and only if g is a right inverse to f and vice versa.

As a matter of fact we almost never say *an* inverse, because if a mapping f has an inverse then this inverse is necessarily unique — so we call it *the* inverse of f.

Proposition 6.15. *(i) If $g : B \to A$ is a left inverse of $f : A \to B$, and $h : B \to A$ is a right inverse of f, then $g = h$, and each is an inverse to f. (ii) If g and h are both inverses of f, then $g = h$.*

Proof. (i) We are given $g \circ f = \mathrm{id}_A$ and $f \circ h = \mathrm{id}_B$. Now we compute $g \circ f \circ h$ in two ways, using associativity (Proposition 6.10):

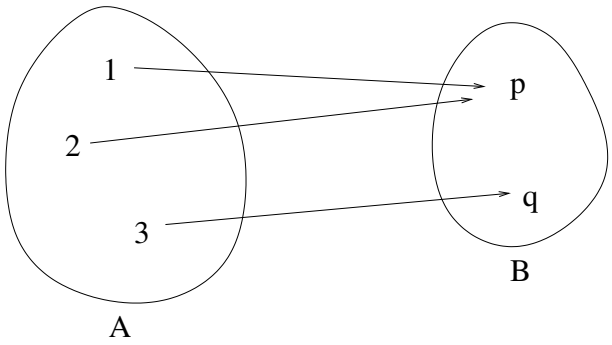
$$g = g \circ \mathrm{id}_B = g \circ (f \circ h) = (g \circ f) \circ h = \mathrm{id}_A \circ h = h.$$

(ii) The second statement is a special case of the first. □

The same mapping may have more than one left inverse (if it is not surjective) and more than one right inverse (if it is not injective). For example, if $A = \{1, 2, 3\}$ and $B = \{p, q\}$, and $f(1) = f(2) = p, f(3) = q$ then both g_1 and g_2, defined by

$$\begin{array}{rcl} g_1(p) & = & 1 \\ g_1(q) & = & 3 \end{array} \qquad \text{and} \qquad \begin{array}{l} g_2(p) = 2 \\ g_2(q) = 3 \end{array},$$

are right inverses to f.



On the other hand, a non-injective map cannot have a left inverse. In this example, f has mapped 1 and 2 to the same point, p. If $g : B \to A$ were a left inverse to f, it would have

- to map p to 1, in order that $g \circ f(1) = 1$, and
- to map p to 2, in order that $g \circ f(2) = 2$.

Clearly the definition of mapping prohibits this: a mapping $g : B \to A$ must map p to just one point in A.

Essentially the same argument can also be used to prove the first of the following two statements. To get an idea for the proof of the second, see what goes wrong when you try to find a right inverse for a simple non-surjective map (e.g. g_1 in the previous example).

Exercise 6.12. *Let $f : A \to B$ be a map. Show that*

1. *if f has a left inverse then it is injective.*
2. *If f has a right inverse then it is surjective.*

The converse to Exercise 6.12 is also true:

Proposition 6.16. *(i) If $p : X \to Y$ is a surjection then there is an injection $i : Y \to X$ which is a right inverse to p.*
(ii) If $i : Y \to X$ is an injection then there is a surjection $p : X \to Y$ which is a left inverse to i.

Proof. (i) If $p : X \to Y$ is a surjection, define $i : Y \to X$ by choosing, for each $y \in Y$, one element $x \in X$ such that $p(x) = y$, and define $i(y)$ to be this chosen x. Then i is an injection; for if $i(y_1) = i(y_2)$ then $p(i(y_1)) = p(i(y_2)$, which means that $y_1 = y_2$. Clearly, i is a right inverse to p.

(ii) If $i : Y \to X$ is an injection, define a map $p : X \to Y$ as follows:

$$p(x) = \begin{cases} y & \text{if } i(y) = x \\ \text{any point in } X & \text{if there is no } y \in Y \text{ such that } i(y) = x \end{cases}$$

(I clarify: in the second case, where x is not the image of any point y, we have to choose *some* y in Y to map x to, but it does not matter which.) Then p is a surjection: if $y \in Y$, then there is an $x \in X$ such that $p(x) = y$, namely $x = i(y)$. Again, it is clear that p is a left inverse to i. □

Proposition 6.17. *A map $f : A \to B$ has an inverse if and only if it is a bijection.*

Proof. Suppose f is a bijection. Then it is surjective, and so has a right inverse g, and injective, and so has a left inverse h. By Proposition 6.15, $g = h$ and is the inverse of f. Conversely, if f has an inverse then in particular it has a left inverse, and so is injective, and a right inverse, and so is surjective. Hence it is bijective. □

The inverse of a bijection f is very often denoted f^{-1}. This notation is suggested by the analogy between composition of mappings and multiplication of numbers: if $g : B \to A$ is the inverse of $f : A \to B$ then

$$g \circ f = \mathrm{id}_A$$

just as for multiplication of real numbers,

$$x^{-1} \times x = 1.$$

Warning. *In mathematics we use the symbol f^{-1} even when f does not have an inverse (because it is not injective or not surjective).* The meaning is as follows: if $f : A \to B$ is a mapping then for $b \in B$,

$$f^{-1}(b) = \{a \in A : f(a) = b\}.$$

It is the "preimage of b under f", and is a *subset* of A, *not* an element of A.

Example 6.18. Let $f : \mathbb{R} \to \mathbb{R}$ be given by $f(x) = x^2$. Then $f^{-1}(1) = \{-1, 1\}$, $f^{-1}(9) = \{-3, 3\}$, $f^{-1}(-1) = \emptyset$.
(ii) In general, $f : A \to B$ is an *injection* if $f^{-1}(b)$ has *no more than one* element for all $b \in B$, and f is a *surjection* if $f^{-1}(b)$ has *no fewer than one* element for all $b \in B$.

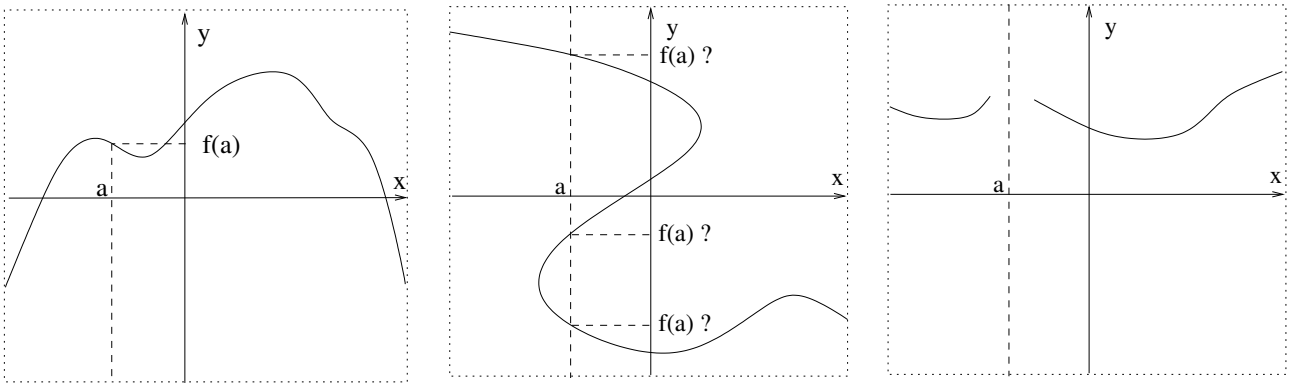
Technically speaking, this f^{-1} is not a mapping from B to A, but *from B to the set of subsets of A*. When f is a bijection and $f(a) = b$, then the preimage of b is the set $\{a\}$, while the image of b under the inverse of f is a. Thus, the two meanings of f^{-1} differ only by the presence of a curly bracket, and the dual meaning of f^{-1} need not cause any confusion.

6.5 Rules and Graphs

If $f : \mathbb{R} \to \mathbb{R}$ is a function, the graph of f is, by definition, the set

$$\{(x, y) \in \mathbb{R}^2 : y = f(x)\}.$$

The graph gives us complete information about f, in the sense that it determines the value of $f(x)$ for each point $x \in \mathbb{R}$, even if we do not know the "rule" by which $f(x)$ is to be calculated.
The requirement, in the definition of function, that a function assign a unique value $f(x)$ to each x, has a geometrical significance in terms of the graph: every line parallel to the y-axis must meet the graph once, and only once. Thus, of the following curves in the plane $\mathbb{R}^2$, only the first defines a function. If we attempt to define a function using the second, we find that at points like the point a shown, it is not possible to define the value $f(a)$, as there are three equally good candidates. The third does not define a function because it does not offer any possible value for $f(a)$.



It is possible to define the graph of an arbitrary mapping $f : A \to B$, by analogy with the graph of a function $\mathbb{R} \to \mathbb{R}$:

Definition 6.19. *(i) Given sets A and B, the* **Cartesian Product** *$A \times B$ is the set of ordered pairs (a, b) where $a \in A$ and $b \in B$.*

(ii) More generally, we define the Cartesian product $A \times B \times C$ as the set of ordered triples $\{(a, b, c) : a \in A, b \in B, c \in C\}$, the Cartesian product $A \times B \times C \times D$ as the set of ordered quadruples $\{(a, b, c, d) : a \in A, b \in B, c \in C, d \in D\}$, and so on.

(iii) Given a map $f : A \to B$, the **graph** *of f is the set*

$$\{(a, b) \in A \times B : b = f(a)\}.$$

Why do we use the $\times$ sign for the Cartesian product?

Proposition 6.20. *Suppose A and B are sets with m and n members respectively. Then $A \times B$ has $m \times n$ members.*

Proof. Let $A = \{a_1, \ldots, a_m\}$ and $B = \{b_1, \ldots, b_n\}$. Then we can list the elements of $A \times B$ as

$$\begin{array}{cccc} (a_1, b_1) & (a_2, b_1) & \cdots & (a_m, b_1) \\ (a_1, b_2) & (a_2, b_2) & \cdots & (a_m, b_2) \\ \cdots & \cdots & \cdots & \cdots \\ (a_1, b_n) & (a_2, b_n) & \cdots & (a_m, b_n) \end{array}$$

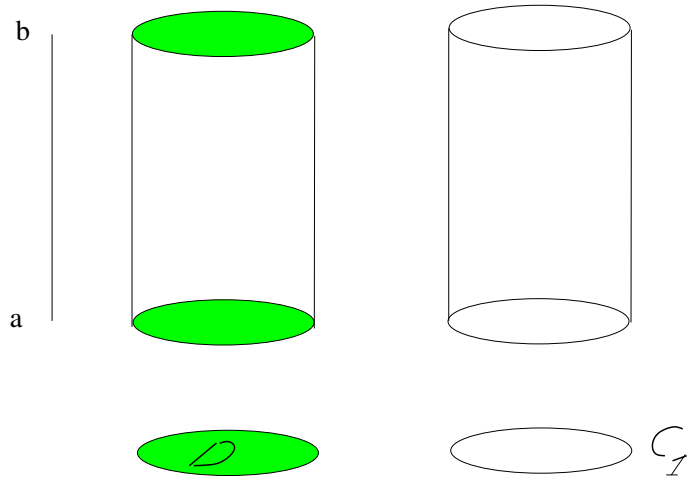
Each column contains n members, and there are m columns, so altogether $A \times B$ has $m \times n$ members. (This is how multiplication is defined: $m \times n$ means "add together m sets of n objects"). □

Example 6.21. 1. $\mathbb{R} \times \mathbb{R}$ is $\mathbb{R}^2$, which we think of as a plane.

2. $\mathbb{R}^2 \times \mathbb{R} = \{((x, y), z) : (x, y) \in \mathbb{R}^2, z \in \mathbb{R}\}$. Except for the brackets, $((x, y), z)$ is the same thing as the ordered triple (x, y, z), so we can think of $\mathbb{R}^2 \times \mathbb{R}$ as being the same thing as $\mathbb{R}^3$.

3. If $[-1, 1]$ is the interval in $\mathbb{R}$, then $[-1, 1] \times [-1, 1]$ is a square in $\mathbb{R}^2$, and $[-1, 1] \times [-1, 1] \times [-1, 1]$ is a cube in $\mathbb{R}^3$.

4. Let D be the unit disc $\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 \leq 1\}$, and let C_1 be its boundary, the circle $\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$. Then $D \times \mathbb{R}$ is an infinite solid cylinder, while $C_1 \times \mathbb{R}$ is an infinite tube.



The solid cylinder $D \times [a, b]$ and the hollow cylinder $C_1 \times [a, b]$

Whereas the graph of a function $f : \mathbb{R} \to \mathbb{R}$ is a geometrical object which we can draw, in general we cannot draw the graphs just defined. One exception is where $f : \mathbb{R}^2 \to \mathbb{R}$, for then the Cartesian product of its domain and codomain, $\mathbb{R}^2 \times \mathbb{R}$, is the same as $\mathbb{R}^3$. The graph therefore is a subset of $\mathbb{R}^3$, and so in principle, we can make a picture of it. The same holds if $f : X \to \mathbb{R}$ where $X \subset \mathbb{R}^2$. The following pictures show the graphs of

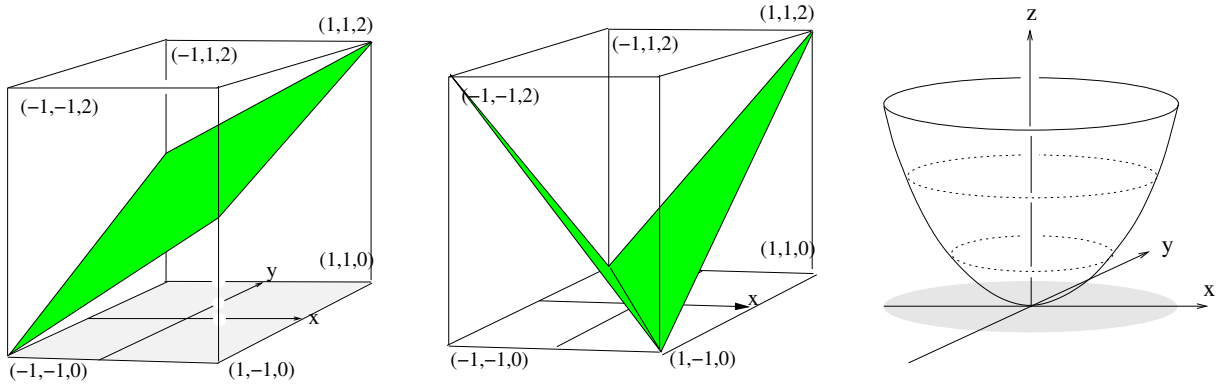
$$f : [-1, 1] \times [-1, 1] \to \mathbb{R} \quad \text{defined by} \quad f(x, y) = \frac{x + y + 2}{2},$$

$$g : [-1, 1] \times [-1, 1] \to \mathbb{R} \quad \text{defined by } g(x, y) = |x + y|.$$

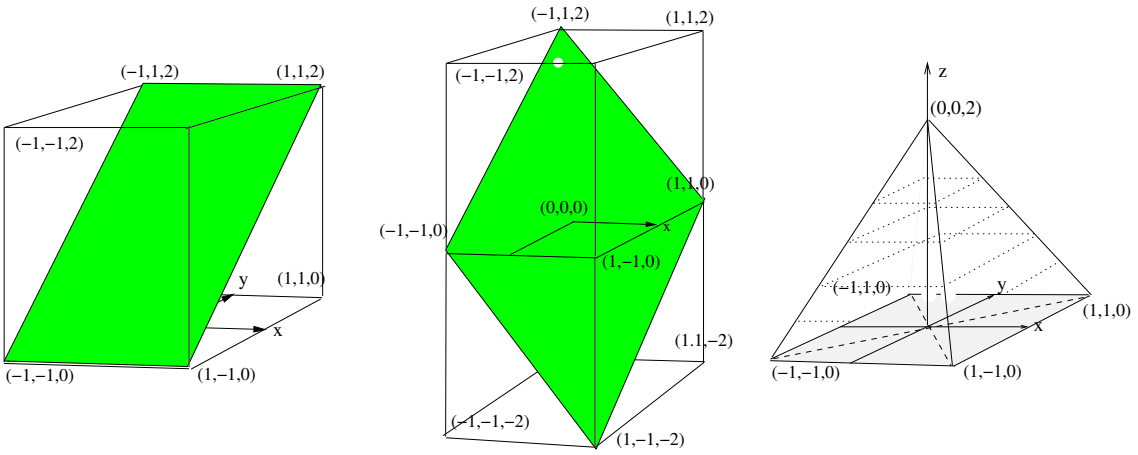
and

$$h : D \to \mathbb{R} \quad \text{defined by} \quad h(x, y) = x^2 + y^2,$$

where D is the unit disc in $\mathbb{R}^2$. I've drawn the first and the second inside the cube $[-1, 1] \times [-1, 1] \times [0, 2]$ in order to make the perspective easier to interpret.



Exercise 6.13. *The following three pictures show the graphs of three functions* $[-1, 1] \times [-1, 1] \to \mathbb{R}$. *Which functions are they?*



Hint: The third picture shows a pyramid. Divide the square $[-1,1]\times[-1,1]$ *into four sectors as indicated by the dashed lines. There is a different formula for each sector.*

6.6 Graphs and inverse functions

If $f : A \to B$ is a bijection, with inverse $f^{-1} : B \to A$, what is the relation between the graph of f and the graph of f^{-1}? Let us compare them:

$$\text{graph}(f) = \{(a,b) \in A \times B : f(a) = b\}, \quad \text{graph}(f^{-1}) = \{(b,a) \in B \times A : f^{-1}(b) = a\}.$$

Since

$$f(a) = b \iff f^{-1}(b) = a,$$

it follows that

$$(a,b) \in \text{ graph}(f) \iff (b,a) \in \text{ graph}(f^{-1}).$$

So $\text{graph}(f^{-1})$ is obtained from $\text{graph}(f)$ simply by interchanging the order of the ordered pairs it consists of. That is: the bijection

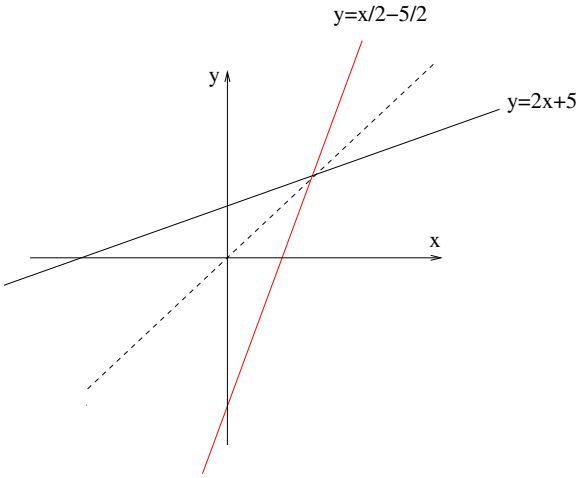
$$i : A \times B \to B \times A, \quad i(a,b) = (b,a)$$

maps the graph of f onto the graph of f^{-1}.

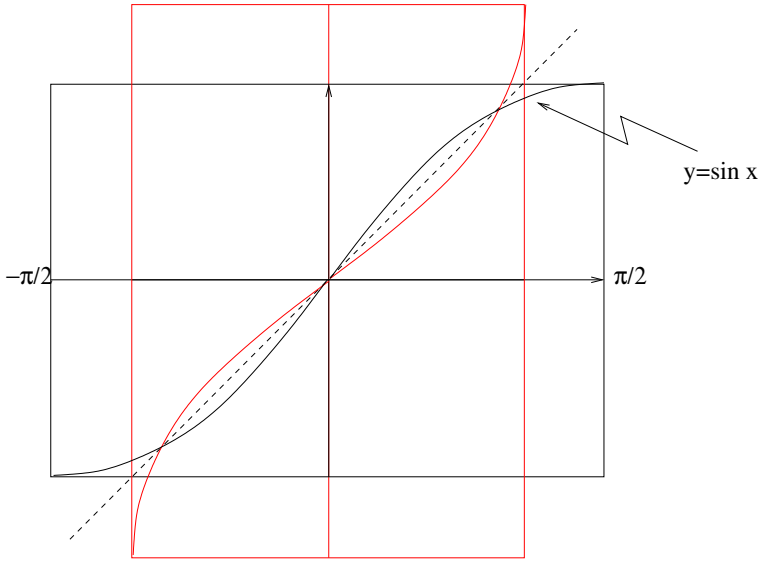
In the case where $f : \mathbb{R} \to \mathbb{R}$ is a bijection with inverse f^{-1}, then provided the scale on the the two axes is the same, the bijection $i(x,y) = (y,x)$ is simply reflection in the line $y = x$. That is, with this proviso, *if* $f : \mathbb{R} \to \mathbb{R}$ *is a bijection, then the graph of its inverse is obtained by reflecting graph*(f) *in the line* $y = x$.

The same holds if f is a bijection from $D \subset \mathbb{R}$ to $T \subset \mathbb{R}$.

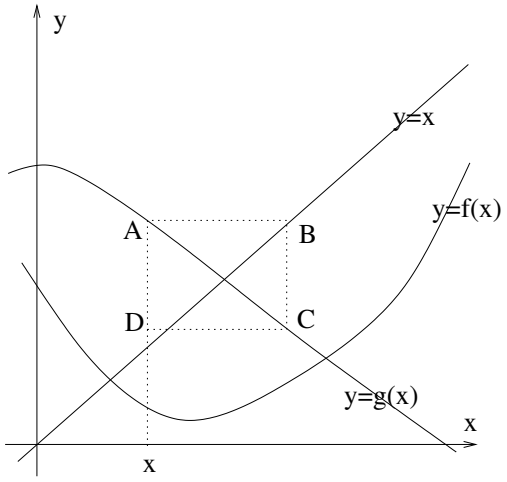
Example 6.22. The function $F : \mathbb{R} \to \mathbb{R}$, $f(x) = 2x + 5$, is a bijection, with inverse $g(x) = \frac{1}{2}x - \frac{5}{2}$. The graphs of the two functions, *drawn with respect to the same axes*, are

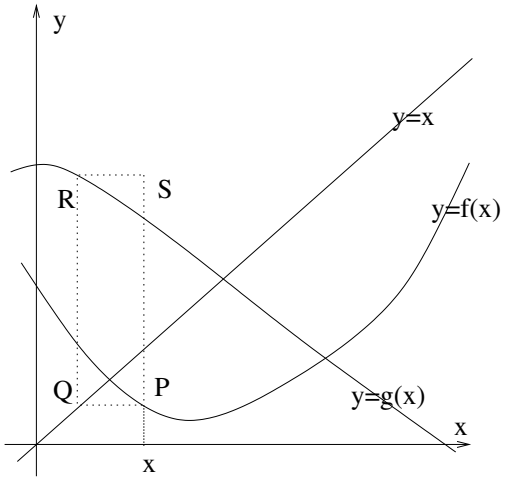


The function $\sin : [\frac{-\pi}{2}, \frac{\pi}{2}] \to [-1, 1]$ is a bijection, with inverse $\arcsin : [-1, 1] \to [\frac{-\pi}{2}, \frac{\pi}{2}]$.

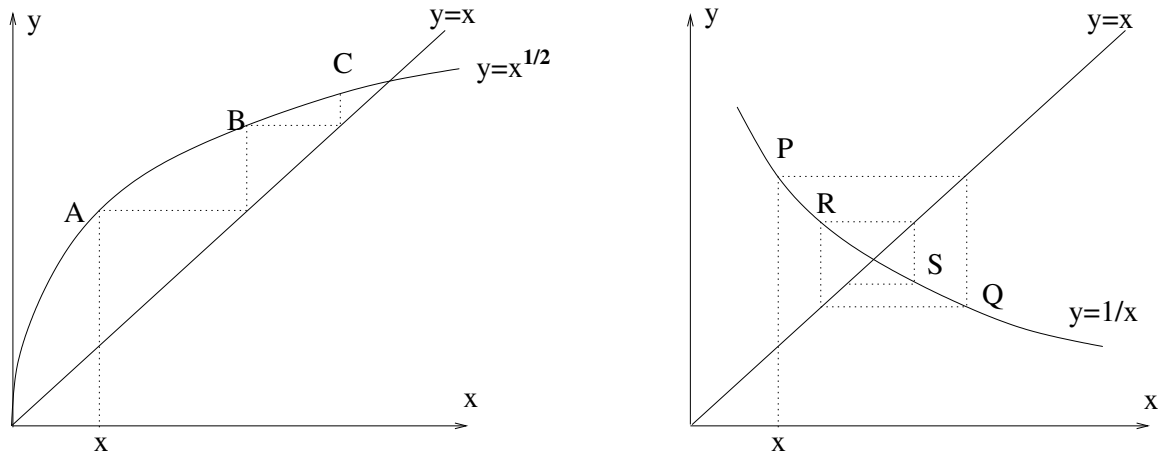


Exercise 6.14. *(i) The diagram below shows the graphs of two functions f and g, and also the line $y = x$, which is of course the graph of the function $i(x) = x$. Find the coordinates of the points A, B, C, D, and P, Q, R, S, in terms of f, g and x.*





(ii) Find the coordinates of the points A, B, C, and P, Q, R, S in terms of x.



6.7 Relations

A relation on a set X is a condition which either does or does not hold for each (ordered) pair of elements in the set. One could define this formally to be a function from $X \times X$ to the two element set $\{T, F\}$ (with T denoting True and F denoting False). It is more common, though, to use some symbol, say $\heartsuit$, for the relation so that $x \heartsuit y$ means "x is related to y" while $x \not\heartsuit y$ means "x is not related to y".

The most obvious example (for any set X) is *equality* which (of course) uses the symbol $=$, so that $x = y$ is true if x and y are the same and not otherwise. (Things do not get much more obvious than that!) There are other relations which behave very much like equality, though, and we will discuss these in detail below (Equivalence relations).

Another familiar example is the relation "less than" with symbol $<$, on the set of real numbers (or any subset of $\mathbb{R}$ –but not on $\mathbb{C}$!). Similarly $>$, $\leq$ and $\geq$ are all relations. In an earlier chapter we used the symbol $|$ to denote "divides" on $\mathbb{N}$ and on $\mathbb{Z}$; this is another example of a relation. And of course among people there is the relation $A \heartsuit B$ meaning "A loves B".

Equivalence Relations

When we re-formulated arithmetic modulo n, we said what it means for two integers to be "the same" (or congruent) modulo n, we were defining a relation on the integers which has special properties, and is an example of an *equivalence relation* on the set of integers. Another equivalence relation is the relation, among sets, of being in bijection with one another. A geometric example is the relation "being parallel to each other" between straight lines in the plane.

An example from everyday life: when we're shopping, we don't distinguish between packets of cereal with the same label and size. As far as doing the groceries is concerned, they are equivalent. Or again, the relation "having the same age (in years)" is an equivalence relation on the set of all people.

Equivalence relations are relations which "behave like equality" without actually being the equality relation (though equality certainly is an equivalence relation). The crucial features of an equivalence relation are

- **Symmetry:** If a is equivalent to b then b is equivalent to a, and
- **Transitivity:** If a is equivalent to b and b is equivalent to c then a is equivalent to c.

The formal definition of equivalence relation contains these two clauses, and one further clause:

- **Reflexivity:** Every object is equivalent to itself.

Formally, an equivalence relation is a relation which satisfies these three defining properties (*symmetry*, *transitivity* and *reflexivity*). It is easy to check that each of the examples of relations described above have all of these three properties. For example, for congruence modulo n:

Reflexivity: For every integer m, $m - m$ is divisible by n, so $m \equiv m \pmod{n}$.

Symmetry: If $m_1 - m_2$ is divisible by n then so is $m_2 - m_1$. So if $m_1 \equiv m_2 \pmod{n}$ then $m_2 \equiv m_1 \pmod{n}$.

Transitivity: If $m_1 - m_2 = kn$ and $m_2 - m_3 = \ell n$ then $m_1 - m_3 = (k + \ell)n$. In other words, if $m_1 \equiv m_2 \pmod{n}$ and $m_2 \equiv m_3 \pmod{n}$ then $m_1 \equiv m_3 \pmod{n}$.

When discussing equivalence relations in the abstract, it is common to use the symbol $\sim$ to mean "related to". Using this symbol, the three defining properties of an equivalence relation on a set X can be written as follows:

E1 Reflexivity: for all $x \in X$: $x \sim x$.

E2 Symmetry: for all $x_1, x_2 \in X$: if $x_1 \sim x_2$ then $x_2 \sim x_1$.

E3 Transitivity: for all x_1, x_2 and x_3 in X: if $x_1 \sim x_2$ and $x_2 \sim x_3$ then $x_1 \sim x_3$.

Exercise 6.15. *(i) Check that the relation among sets A, B defined by*

$$A \sim B \quad \textit{if there is a bijection} \quad \varphi : A \to B$$

has the properties of reflexivity, symmetry and transitivity.

(ii) Ditto for the relation, among positive integers, of having the same prime factors.

(iii) Let $f : X \to Y$ be any function, and define the relation $\sim$ on X by

$$x_1 \sim x_2 \Longleftrightarrow f(x_1) = f(x_2).$$

Show that this is an equivalence relation on X. Is the relation in (ii) of this form (for suitable f, Y with $X = \mathbb{N}$)?

An equivalence relation on a set X splits up X into *equivalence classes*, consisting of elements that are mutually equivalent. Two elements are in the same equivalence class if and only if they are equivalent. Denoting the equivalence class containing the element x by $[x]$:

$$[x] = \{y \in X \mid y \sim x\}.$$

For example, in the case of congruence modulo n, we denoted the equivalence class of an integer m by $[m]$. (This notation ignores the modulus n, so should only be used in a context where the modulus is known and fixed.)

Two distinct equivalence classes have empty intersection — in other words, any two equivalence classes either do not meet at all, or are the same. This is easy to see: if X_1 and X_2 are equivalence classes, and there *is* some x in their intersection, then for every $x_1 \in X_1$, $x_1 \sim x$, as $x \in X_1$, and for every $x_2 \in X_2$, $x \sim x_2$ as $x \in X_2$. It follows by transitivity that for every $x_1 \in X_1$ and for every $x_2 \in X_2$, $x_1 \sim x_2$. As all the elements of X_1 and X_2 are equivalent to one another, X_1 and X_2 must be the same equivalence class.

The fact we have just mentioned is sufficiently important to be stated as a proposition:

Proposition 6.23. *If $\sim$ is an equivalence relation in the set X then any two equivalence classes of $\sim$ are either disjoint, or equal.* □

In other words, an equivalence relation on a set X partitions X into disjoint subsets, the equivalence classes. For example, with the relation of congruence modulo n there are exactly n classes, namely $[0], [1], \ldots, [n-1]$. When $n = 2$, the two classes are the sets $[0]$ of all even integers and the set $[1]$ of all odd integers.

You will see many more examples of equivalence relations in other mathematics courses.

Order Relations

Order relations are another common and important kind of relation in mathematics. Consider the following relations:

1. $\leq$ among real numbers;
2. $\subseteq$ among sets;
3. $\mid$ (divisibility) among positive integers;

None of them is an equivalence relation, even though each has two of the three necessary properties: reflexivity and transitivity. Crucially, they do not have the property of symmetry. For example, $a \leq b$ does *not* imply $b \leq a$. In fact all except the last have a property almost opposite to that of symmetry, that *the relation points both ways only when the two objects are in fact one and the same* (this property is known as *antisymmetry*):

1. if $a \leq b$ and $b \leq a$ then $a = b$
2. if $A \subseteq B$ and $B \subseteq A$ then $A = B$
3. if $m, n \in \mathbb{N}$ are positive, and if $m \mid n$ and $n \mid m$ then $m = n$. [However if m and n are integers and $m \mid n$ and $n \mid m$, then we can only conclude that $m = \pm n$ (prove this!); we cannot quite say that they are equal.]

Relations 1, 2 and 3 here are examples of *order* relations. You will see many more examples in other mathematics courses.

7 Polynomials

A *polynomial* is an expression like

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

in which $a_0, a_1, \ldots, a_n$, the *coefficients*, are (usually) constants, x is the *variable* or *indeterminate*, and all the powers to which x is raised are natural numbers. For example

$$P_1(x) = 3x^3 + 15x^2 + x - 5, \quad P_2(x) = x^5 + \frac{3}{17}x^2 - \frac{1}{9}x + 8$$

are polynomials; P_1 has integer coefficients, and P_2 has rational coefficients. The set of all polynomials (of any degree) with, respectively, integer, rational, real and complex coefficients are denoted $\mathbb{Z}[x], \mathbb{Q}[x], \mathbb{R}[x]$ and $\mathbb{C}[x]$. Because $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$, we have

$$\mathbb{Z}[x] \subseteq \mathbb{Q}[x] \subseteq \mathbb{R}[x] \subseteq \mathbb{C}[x].$$

If we assign a numerical value to x then any polynomial in x acquires a numerical values; for example $P_1(1) = 14$, $P_1(0) = -5$, $P_2(0) = 8$. So every polynomial determines a *polynomial function* with domain and codomain equal to the coefficient number system; however, here we will be concerned with polynomials more as algebraic objects than as special functions.

A lot of what we say about polynomials here is completely obvious, but there is a lot of standard terminology and notation which goes with polynomials which it is important to absorb. We'll also see that the algebra of polynomials has a lot in common with the arithmetic of the integers, and we will consider questions of divisibility and factorisation for polynomials, as well as hcf and lcm for polynomials, and even the Euclidean Algorithm.

The *degree* of a non-zero polynomial is the highest power of x appearing in it *with non-zero coefficient*. The degrees of the polynomials P_1 and P_2 above are $\deg P_1 = 3$ and $\deg P_2 = 5$. The degree of the polynomial $2x + 0x^5$ is 1. A polynomial of degree 0 is a non-zero constant. The zero polynomial 0 (i.e. having all coefficients equal to 0) does not have a degree. This is merely a convention[23]. You may think that there is not much that is worth saying about this particular polynomial, but it is necessary to include it if we want to avoid complicating later statements by having to exclude it. (For example we want the sum of two polynomials always to be a polynomial; try adding x to $-x$!) The *leading term* in a non-zero polynomial is the term of highest degree. In P_1 it is $3x^3$ and in P_2 it is x^5. The coefficient of the leading term is called the *leading coefficient*; polynomials withe leading coefficient 1 are called *monic*. For example, P_2 is monic but P_1 is not, as it has leading coefficient 3. Every polynomial (other than 0) has a leading term, and, obviously, its degree is equal to the degree of the polynomial.

Polynomials can be added and multiplied together, according to the following natural rules:
Addition: To add together two polynomials you simply add the coefficients of each power of x. Thus the sum of the polynomials P_1 and P_2 above is

$$x^5 + 3x^3 + (15 + \frac{3}{17})x^2 + \frac{8}{9}x + 3.$$

[23] other conventions for $\deg 0$ are -1 and $-\infty$!

If we allow that some of the coefficients a_i or b_j may be zero, we can write the sum of two polynomials using the formula

$$(a_n x^n + \cdots + a_1 x + a_0) + (b_n x^n + \cdots + b_1 x + b_0) = (a_n + b_n)x^n + \cdots + (a_1 + b_1)x + (a_0 + b_0) \quad (49)$$

or, more briefly

$$\left(\sum_i a_i x^i\right) + \left(\sum_i b_i x^i\right) = \sum_i (a_i + b_i) x^i.$$

We are not assuming that the two polynomials have the same degree, n, here: if one polynomial has degree, say, 3 and the other degree 5, then we can write them as $a_5 x^5 + \cdots + a_0$ and $b_5 x^5 + \cdots + b_0$ by setting $a_4 = a_5 = 0$.

Multiplication: To multiply together two polynomials we multiply each of the terms independently, using the rule

$$x^m \times x^n = x^{m+n},$$

and then group together all of the terms of the same degree. For example the product of the two polynomials P_1 and P_2, $(3x^3 + 15x^2 + x - 5)(x^5 + \frac{3}{17}x^2 - \frac{1}{9}x + 8)$, is equal to

$$3x^8 + 15x^7 + x^6 + \big(\frac{9}{17} - 5\big)x^5 + \big(\frac{45}{17} - \frac{1}{3}\big)x^4 + \big(24 - \frac{5}{3} + \frac{3}{17}\big)x^3 + \big(120 - \frac{1}{9} - \frac{15}{17}\big)x^2 + \big(8 + \frac{5}{9}\big)x - 40.$$

The general formula is

$$\begin{aligned} &\big(a_m x^m + \cdots + a_0\big)\big(b_n x^n + \cdots + b_0\big) \qquad (50)\\ &\quad = \big(a_m b_n\big)x^{m+n} + \big(a_m b_{n-1} + a_{m-1} b_n\big)x^{m+n-1} + \cdots \\ &\qquad\qquad \cdots + \big(a_0 b_k + a_1 b_{k-1} + \cdots + a_{k-1} b_1 + a_k b_0\big)x^k + \cdots \\ &\qquad\qquad\qquad \cdots + \big(a_1 b_0 + a_0 b_1\big)x + a_0 b_0. \end{aligned}$$

This can be written more succinctly

$$\Big(\sum_{i=0}^{m} a_i x^i\Big)\Big(\sum_{j=0}^{n} b_k x^j\Big) = \sum_{k=0}^{m+n}\Big(\sum_{i=0}^{k} a_i b_{k-i}\Big)x^k.$$

The coefficient of x^k here can also be written in the form

$$\sum_{i+j=k} a_i b_j \quad .$$

The sum and the product of P_1 and P_2 are denoted $P_1 + P_2$ and $P_1 P_2$ respectively. Each is, evidently, a polynomial. Note that the sum and product of polynomials are both defined so that for any *value* c we give to x, we have

$$(P_1 + P_2)(c) = P_1(c) + P_2(c), \quad (P_1 P_2)(c) = P_1(c) P_2(c).$$

The following proposition is obvious:

Proposition 7.1. *If P_1 and P_2 are polynomials then* $\deg(P_1 P_2) = \deg(P_1) + \deg(P_2)$*, and provided* $P_1 + P_2 \neq 0$*,* $\deg(P_1 + P_2) \leq \max\{\deg(P_1), \deg(P_2)\}$.

Proof. Obvious from the two formulae (49) and (50). □

We note that the inequality in the formula for the degree of the sum is due to the possibility of cancellation, as, for example, in the case

$$P_1(x) = x^2 + 1, \quad P_2(x) = x - x^2,$$

where $\max\{\deg(P_1), \deg(P_2)\} = 2$ but $\deg(P_1 + P_2) = 1$.

7.1 Polynomial hcf and lcm

Less obvious is that there is a polynomial version of division with remainder. We first state this for polynomials with real coefficients (see below for other cases):

Proposition 7.2. *If $P_1, P_2 \in \mathbb{R}[x]$ and $P_2 \neq 0$, then there exist $Q, R \in \mathbb{R}[x]$ such that*

$$P_1 = QP_2 + R,$$

with either $R = 0$ (the case of exact division) or $\deg(R) < \deg(P_2)$.

Before giving a proof, let's look at an example. We take

$$P_1(x) = 3x^5 + 2x^4 + x + 11 \quad \text{and} \quad P_2(x) = x^3 + x^2 + 2.$$

Step 1:

$$P_1(x) - 3x^2P_2(x) = 3x^5 + 2x^4 + x + 11 - 3x^2(x^3 + x^2 + 2) = -x^4 - 6x^2 + x + 11$$

Note that the leading term of P_1 has cancelled with the leading term of $3x^2P_2$. We chose the coefficient of $P_2(x)$, $3x^2$, to make this happen.

Step 2:

$$\big(P_1(x) - 3x^2P_2(x)\big) + xP_2(x) = -x^4 - 6x^2 + x + 11 + x(x^3 + x^2 + 2) = x^3 - 6x^2 + 3x + 11$$

Here the leading term of $P_1(x) - 3x^2P_2(x)$ has cancelled with the leading term of $-xP_2(x)$.

Step 3:

$$\big(P_1(x) - 3x^2P_2(x) + xP_2(x)\big) - P_2(x) = x^3 - 6x^2 + 3x + 11 - x^3 - x^2 - 2 = -7x^2 + 3x + 9.$$

Here the leading term of $\big(P_1(x) - x^2P_2(x) - xP_2(x)\big)$ has cancelled with the leading term of $P_2(x)$.

At this point we cannot lower the degree of what's left any further, so we stop. We have

$$P_1(x) = \big(3x^2 - x + 1)P_2(x) + (-7x^2 + 3x + 9).$$

That is, $Q(x) = 3x^2 - x + 1$ and $R(x) = -7x^2 + 3x + 9$.

Proof of Proposition 7.2: Suppose that $\deg(P_2) = m$. Let $\mathcal{R}$ (for "Remainders") be the set of all polynomials of the form $R = P_1 - QP_2$, where Q can be any polynomial in $\mathbb{R}[x]$. If the polynomial 0 is in $\mathcal{R}$, then P_2 divides P_1 exactly. Otherwise, consider the *degrees* of the polynomials in $\mathcal{R}$. By the Well-Ordering Principal, this set of degrees has a least element, r_0. We want to show that $r_0 < m$.

Suppose, to the contrary, that $r_0 \geq m$. Let $R_0 = P_1 - QP_2$ be a polynomial in $\mathcal{R}$ having degree r_0. In other words, R_0 is a polynomial of the lowest degree possible, given that it is in $\mathcal{R}$. Its leading term is some constant multiple of x^{r_0}, say cx^{r_0}. Then if bx^m is the leading term of P_2, the polynomial

$$R_0(x) - \frac{c}{b}x^{r_0-m}P_2(x) = P_1 - \big(Q + \frac{c}{b}x^{r_0-m}\big)P_2 \tag{51}$$

is also in $\mathcal{R}$, and has degree less than r_0. This contradicts the definition of r_0 as the smallest possible degree of a polynomial of the form $P_1 - QP_2$. We are forced to conclude that $r_0 < \deg(P_2)$. □

The idea of the proof is really just what we saw in the example preceding it: that if $P_1 - QP_2$ has degree greater than or equal to $\deg(P_2)$ then by subtracting a suitable multiple of P_2 we can remove its leading term, and thus lower its degree. To be able to do this we need to be able to divide the coefficient of the leading term of R by the coefficient of the leading term of P_2, as displayed in (51). This is where we made use of the fact that our polynomials had *real* coefficients: we can *divide* real numbers by one another. For this reason, the same argument works if we have rational or complex coefficients, but *not* if our polynomials must have *integer* coefficients. We record this as a second proposition:

Proposition 7.3. *The statement of Proposition 7.2 holds with $\mathbb{Q}[x]$ or $\mathbb{C}[x]$ in place of $\mathbb{R}[x]$, but is false if $\mathbb{R}[x]$ is replaced by $\mathbb{Z}[x]$.* □

As with integers, we say that the polynomial P_2 *divides* the polynomial P_1 if there is a polynomial Q such that $P_1 = QP_2$, and we use the same symbol, $P_2|P_1$, to indicate this.

You may have noticed a strong similarity with the proof of division with remainder for natural numbers (Proposition 2.6). In fact there is a remarkable parallel between what we can prove for polynomials and what happens with natural numbers. Almost every one of the definitions we made for natural numbers has its analogue in the world of polynomials.

The quotient Q and the remainder R in Proposition 7.2 are uniquely determined by P_1 and P_2:

Proposition 7.4. *If $P_1 = Q_1P_2 + R_1$ and also $P_1 = Q_2P_2 + R_2$ with $R_1 = 0$ or $\deg(R_1) < \deg(P_2)$ and $R_2 = 0$ or $\deg(R_2) < \deg(P_2)$, then $Q_1 = Q_2$ and $R_1 = R_2$.*

Proof. From $P_2Q_1 + R_1 = P_2Q_2 + R_2$ we get

$$P_2(Q_1 - Q_2) = R_2 - R_1.$$

If $Q_1 \neq Q_2$ then the left hand side is a polynomial of degree *at least* $\deg(P_2)$. The right hand side, on the other hand, is a polynomial of degree $\leq \max\{\deg(R_1), \deg(R_2)\}$ and therefore *less* than $\deg(P_2)$. So they cannot be equal — unless they are both zero. □

Incidentally, essentially the same argument proves uniqueness of quotient and remainder in division of natural numbers, (as in Proposition 2.6).

Before going further, we will fix the kind of polynomials we are going to talk about. All of what we do for the rest of this section will concern polynomials with *real coefficients*. In other words, we will work in $\mathbb{R}[x]$. The reason why we make this restriction will become clear in a moment.

The first definition we seek to generalise from $\mathbb{Z}$ is the notion of *prime number*. We might hope to define a "prime polynomial" as one which is not divisible by any polynomial other than the constant polynomial 1 and itself. However, this definition is unworkable, because *every* polynomial is divisible by the constant polynomial -1, or the constant polynomial $\frac{1}{2}$, or indeed any non-zero constant polynomial. So instead we make the following definition:

Definition 7.5. *The polynomial $P \in \mathbb{R}[x]$ is* **irreducible in $\mathbb{R}[x]$** *if P is non-constant, and whenever it factorises as a product of polynomials $P = P_1P_2$ with $P_1, P_2 \in \mathbb{R}[x]$ then either P_1 or P_2 is a constant. If P is not irreducible in $\mathbb{R}[x]$, we say it is* **reducible in $\mathbb{R}[x]$**.

So reducible polynomials P can be factored as $P = P_1P_2$ where *both* P_1 and P_2 have degree strictly smaller than $\deg P$. To save breath, we shall start calling a factorisation $P = P_1P_2$ of a polynomial P *trivial* if either P_1 or P_2 is a constant, and *non-trivial* if neither is a constant. Thus, a polynomial is irreducible if it is non-constant and only has trivial factorisations. (This is analogous to the definition of a prime as being an integer > 1 with only trivial factorisations.)

Example 7.6. 1. Every polynomial of degree 1 is irreducible.

2. The polynomial $P(x) = x^2 + 1$ is irreducible in $\mathbb{R}[x]$. For if it were reducible, it would have to be the product of polynomials P_1, P_2 of degree 1,

$$x^2 + 1 = (a_1x + a_0)(b_1x + b_0).$$

Now compare coefficients on the right and left hand sides of the equation:

$$\begin{aligned} \text{coefficient of } x^2 : &\quad a_1b_1 = 1 \\ \text{coefficient of } x : &\quad a_0b_1 + a_1b_0 = 0 \\ \text{coefficient of } 1 : &\quad a_0b_0 = 1 \end{aligned}$$

Multiply the middle equation by a_0a_1 and simplify using the first and last equations to get

$$a_0^2 + a_1^2 = 0,$$

whose only **real** solution is $a_0 = a_1 = 0$, but this leads to the contradiction $0 = 1$ when we substitute into the first equation!

The only logical way out of the contradiction is that $x^2 + 1$ must be irreducible in $\mathbb{R}[x]$.

On the other hand, $x^2 + 1$ *is reducible* in $\mathbb{C}[x]$; it factorises as

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

Thus, *reducibility depends on which set of polynomials we are working in.* This is why for the rest of this section we will focus on just the one set of polynomials, $\mathbb{R}[x]$.

Proposition 7.7. *Every polynomial of degree greater than* 0 *is divisible by an irreducible polynomial.*

I gave two proofs of the corresponding statement for natural numbers, Lemma 2.2, which states that a natural number $n > 1$ is divisible by some prime, and set an exercise asking for a third. So you should be reasonably familiar with the possible strategies. I think the best one is to consider the set S of all non-trivial divisors of n (i.e. divisors of n which are greater than 1), and show that the least element d of S is prime. It has to be prime, because if it factors as a product of natural numbers, $d = d_1d_2$, with neither d_1 nor d_2 equal to 1, then each is a divisor of n which is less than d and greater than 1, and this contradicts the definition of d as the *least* divisor of n which is greater than 1.

Exercise 7.1. *Prove Proposition 7.7. Hint: in the set of all non-trivial factors of P in $\mathbb{R}[x]$, choose one of least degree.*

The next thing we will look for is an analogue, for polynomials, of the highest common factor of two natural numbers. What could it be? Which aspect of hcf's is it most natural to try to generalise? Perhaps as an indication that the analogy between the theory of polynomials and the arithmetic of $\mathbb{N}$ and $\mathbb{Z}$ is rather deep, it turns out that the natural generalisation has very much the same properties as the hcf in ordinary arithmetic.

Definition 7.8. *If P_1 and P_2 are polynomials in $\mathbb{R}[x]$, we say that the polynomial $P \in \mathbb{R}[x]$ is a* **highest common factor** *of P_1 and P_2 if it divides both P_1 and P_2 (i.e. it is a common factor of P_1 and P_2) and P_1 and P_2 have no common factor of higher degree (in $\mathbb{R}[x]$).*

Highest common factors definitely do exist. For if P is a common factor of P_1 and P_2 then its degree is bounded[24] above by $\min\{\deg(P_1), \deg(P_2)\}$. As the set of degrees of common factors of P_1 and P_2 is bounded above, it has a greatest element, by the version of the Well-Ordering Principle already discussed on page 10.

I say *a* highest common factor rather than *the* highest common factor because for all we know at this stage, there might be two completely different and unrelated "highest common factors" of P_1 and P_2. Moreover, there is the annoying, though trivial, point that if P is a highest common factor then so is the polynomial λP for each non-zero real number λ. So the highest common factor can't possibly be unique. Of course, this latter is not a serious lack of uniqueness. And, as we will see, it is in fact the only respect in which the hcf of two polynomials is not unique:

Proposition 7.9. *If P and Q are both highest common factors of P_1 and P_2 in $\mathbb{R}[x]$, then there is a non-zero real number λ such that $P = \lambda Q$.*

So *up to multiplication by a non-zero constant*, the hcf of two polynomials is unique. One common convention used to recover uniqueness is to choose the constant scaling factor so that the hcf is monic.

But I can't prove this proposition yet. When we were working in $\mathbb{N}$, then uniqueness of the hcf of two natural numbers was obvious from the definition, but here things are a little more subtle. We will shortly be able to prove it though.

Proposition 7.9 is an easy consequence of the following analogue of Proposition 2.14:

Proposition 7.10. *If P is a highest common factor of P_1 and P_2 in $\mathbb{R}[x]$, then any other common factor of P_1 and P_2 in $\mathbb{R}[x]$ divides P.*

Exercise 7.2. *Deduce Proposition 7.9 from Proposition 7.10. Hint: if P and Q are both highest common factors of P_1 and P_2 then by Proposition 7.9 $P|Q$ (because Q is an* hcf*), and $Q|P$, because P is an* hcf*.*

But I can't prove Proposition 7.10 yet either. If you think back to the arithmetic we did at the start of the course, the corresponding result, Proposition 2.14, followed directly from our description of $\mathrm{hcf}(m, n)$ in terms of the prime factorisations of m and n in Proposition 2.12 (see page 13 of these Lecture Notes). And this made use of the Fundamental Theorem of Arithmetic, the existence and uniqueness of a prime factorisation. Now there is a "Fundamental Theorem of Polynomials" which says very much the same thing, with "irreducible polynomial " in place of "prime number", and we could deduce Proposition 7.10 from it. But first we'd have to prove it, which I don't want to do[25]. Even worse, in order to use factorisation into a product of irreducibles to *find* hcfs, we'd have to develop techniques to factorise polynomials. This turns out to be rather complicated. (You may think that factorising polynomials requires being able to find all their roots. We all know a formula to find the roots of quadratic polynomials, and formulae exist for polynomials of degree 3 and 4, though few people learn them these days, but for degree 5 and beyond no purely algebraic

[24] this does not cover the case $P_1 = P_2 = 0$, but decreeing that $\mathrm{hcf}(0, 0) = 0$ deals with that case.

[25] It's left as an exercise on the next Example sheet

formula can exist (this was proved by Abel and Galois in the nineteenth century). Luckily, though, polynomial factorisation does *not* require root-finding; but the method will not be discussed further here.)

So we use a different tactic: we will develop the Euclidean algorithm for polynomials, and see that it leads us to an essentially unique hcf.

The next lemma is the version for polynomials of Lemma 2.15 on page 14 of these lecture notes. Since we cannot yet speak of *the* hcf of two polynomials, we have to phrase it differently.

Lemma 7.11. *Suppose P_1, P_2, Q and R are all in $\mathbb{R}[x]$, and $P_1 = QP_2 + R$. Then the set of common factors of P_1 and P_2, is equal to the set of common factors of P_2 and R.*

Proof. Suppose F is a common factor of P_1 and P_2. Then $P_1 = FQ_1$ and $P_2 = FQ_2$ for some $Q_1, Q_2 \in \mathbb{R}[x]$. It follows that $R = P_1 - QP_2 = FQ_1 - FQQ_2 = F(Q_1 - QQ_2)$, so F also divides R, and therefore is a common factor of P_2 and R. Conversely, if F is a common factor of P_2 and R, then $P_2 = FQ_3$ and $R = FQ_4$ for some $Q_3, Q_4 \in \mathbb{R}[x]$. Therefore $P_1 = F(QQ_3 + Q_4)$, so F is a common factor of P_1 and P_2. □

It will be useful to have a name for the set of common factors of P_1 and P_2: we will call it $\mathscr{F}(P_1, P_2)$. Similarly, $\mathscr{F}(P)$ will denote the set of all of the factors of P.

As usual, when it comes to understanding what is going on, one example is worth a thousand theorems.

Example 7.12. $P_1(x) = x^2 - 3x + 2, \qquad P_2(x) = x^2 - 4x + 3.$

We divide P_1 by P_2:

$$\begin{array}{rrrr} & & & 1 \\ x^2-4x+3 & x^2 & -3x & +2 \\ & x^2 & -4x & +3 \\ & & x & -1 \end{array}$$

so $\mathscr{F}(x^2-3x+2,\ x^2-4x+3) = \mathscr{F}(x^2-4x+3, x-1)$. Now we divide x^2-4x+3 by $x-1$:

$$\begin{array}{rrrr} & & x & -3 \\ x-1 & x^2 & -4x & +3 \\ & x^2 & -x & \\ & & -3x & +3 \\ & & -3x & +3 \\ & & & 0 \end{array}$$

so $\mathscr{F}(x^2 - 4x + 3, x - 1) = \mathscr{F}(x - 1, 0)$.

Note that $\mathscr{F}(x-1, 0) = \mathscr{F}(x-1)$, since every polynomial divides 0. In $\mathscr{F}(x-1)$ there *is* a uniquely determined highest common factor, namely $x-1$ itself. And it's the only possible choice (other than non-zero constant multiples of itself). Since $\mathscr{F}(P_1, P_2) = \mathscr{F}(x - 1)$, we conclude that the highest common factor of P_1 and P_2 is $x - 1$.

Example 7.13. $P_1(x) = x^4 - x^3 - x^2 - x - 2, \qquad P_2(x) = x^3 + 2x^2 + x + 2.$

We divide P_1 by P_2:

$$\begin{array}{rrrrrr} & & & & x & -3 \\ x^3+2x^2+x+2 & x^4 & -x^3 & -x^2 & -x & -2 \\ & x^4 & +2x^3 & +x^2 & +2x & \\ & & -3x^3 & -2x^2 & -3x & -2 \\ & & -3x^3 & -6x^2 & -3x & -6 \\ & & & 4x^2 & & +4 \end{array}$$

So $\mathscr{F}(P_1,P_2)=\mathscr{F}(P_2,4x^2+4)=\mathscr{F}(P_2,x^2+1)$. Now we divide P_2 by x^2+1:

$$\begin{array}{rrrrr} & & & x & +2 \\ x^2+1 & x^3 & +2x^2 & +x & +2 \\ & x^3 & & +x & \\ & & 2x^2 & & +2 \\ & & 2x^2 & & +2 \\ & & & & 0 \end{array}$$

So $\mathscr{F}(P_1,P_2)=\mathscr{F}(P_2,x^2+1)=\mathscr{F}(x^2+1,0)=\mathscr{F}(x^2+1)$. Once again, there are no two ways about it. Up to multiplication by a non-zero constant[26], there is only one polynomial of maximal degree in here, namely x^2+1. So this is *the* hcf of P_1 and P_2.

Is it clear to you that something like this will always happen? We do one more example.

Example 7.14. $P_1(x)=x^3+x^2+x+1, \qquad P_2(x)=x^2+x+1.$

We divide P_1 by P_2.

$$\begin{array}{rrrrr} & & & x & \\ x^2+x+1 & x^3 & +x^2 & +x & +1 \\ & x^3 & +x^2 & +x & \\ & & & & 1 \end{array}$$

So $\mathscr{F}(P_1,P_2)=\mathscr{F}(P_2,1)$. If we divide P_2 by 1, of course we get remainder 0, so $\mathscr{F}(P_2,1)=\mathscr{F}(1,0)$. This time, the hcf is 1.

Proof. of Proposition 7.10 The idea is to apply the Euclidean algorithm, dividing and replacing the dividend by the remainder at each stage, until at some stage the remainder on division is zero. We label the two polynomials P_1 and P_2 we begin with so that $\deg(P_2)\leq$

[26] I won't say this again

$\deg(P_1)$. The process goes like this:

Step	Division	Conclusion
Step 1	$P_1 = Q_1P_2 + R_1$	$\mathscr{F}(P_1, P_2) = \mathscr{F}(P_2, R_1)$
Step 2	$P_2 = Q_2R_1 + R_2$	$\mathscr{F}(P_2, R_1) = \mathscr{F}(R_1, R_2)$
Step 3	$R_1 = Q_3R_2 + R_3$	$\mathscr{F}(R_1, R_2) = \mathscr{F}(R_2, R_3)$
...	...	...
Step k	$R_{k-2} = Q_kR_{k-1} + R_k$	$\mathscr{F}(R_{k-2}, R_{k-1}) = \mathscr{F}(R_{k-1}, R_k)$
...	...	...
Step N	$R_{N-2} = Q_NR_{N-1}$	$\mathscr{F}(R_{N-2}, R_{N-1}) = \mathscr{F}(R_{N-1})$

The process must come to an end as shown, for when we go from each step to the next, the degree of the remainder decreases:

$$\deg P_2 > \deg R_1 > \deg R_2 > \dots .$$

But degrees are natural numbers, so this sequence must be finite! If $\deg R_{N-1}$ is 0 for some N, then R_{N-1} is a non-zero constant, and the final division goes exactly with reminder $R_N = 0$ as shown; or in any case there must be exact division at some step, say the N'th, and $R_N = 0$ (though R_{N-1} may not be constant). Either way, we must end with an exact division and zero remainder, and the table gives an accurate description of how the process ends.

From the table we read that

$$\mathscr{F}(P_1, P_2) = \dots = \mathscr{F}(R_{N-1}). \tag{52}$$

The right hand set has a unique element of highest degree, R_{N-1}. So this is the unique element of highest degree in the left hand side, $\mathscr{F}(P_1, P_2)$. In other words, it is *the* highest common factor of P_1 and P_2. We *can* speak of *the* highest common factor of P_1 and P_2, and we can rewrite (52) as

$$\mathscr{F}(P_1, P_2) = \mathscr{F}(H), \tag{53}$$

where $H = \mathrm{hcf}(P_1, P_2)$. The equality (53) also tells us that H is divisible by every other common factor of P_1 and P_2, because the polynomials in $\mathscr{F}(H)$ are precisely those that divide H. □

Definition 7.15. We say two polynomials P and Q are *equivalent* if one is a non-zero constant multiple of the other.

For example, Proposition 7.9 says that given two polynomials P_1 and P_2, any two highest common factors of P_1 and P_2 are equivalent. Of course, this equivalence *is* an equivalence relation. We can quite reasonably speak of *the* highest common factor of two polynomials, either by agreeing to scale to make the hcf monic, or by just agreeing not to consider equivalent polynomials as different for this purpose.

Exercise 7.3. *Find the* hcf *of*[27]

1. $P_1(x) = x^4 - 1, \quad P_2(x) = x^2 - 1$
2. $P_1(x) = x^5 - 1, \quad P_2(x) = x^2 - 1$
3. $P_1(x) = x^6 - 1, \quad P_2(x) = x^4 - 1.$

Exercise 7.4. *In each of Examples 7.12, 7.13 and 7.14, find polynomials A and B such that $H = AP_1 + BP_2$, where $H = \mathrm{hcf}(P_1, P_2)$. Hint: review the method for natural numbers (subsection 3.2, page 19).*

Exercise 7.5. *Define a* **lowest common multiple** *of polynomials P_1 and P_2 to be a polynomial divisible by both, whose degree is minimal among all such. (i) Prove that lowest common multiples exist. (ii) Show that*

$$\frac{P_1 P_2}{\mathrm{hcf}(P_1, P_2)}$$

is a lowest common multiple. (iii) Prove that any two lowest common multiples of P_1 and P_2 are equivalent.

Exercise 7.6. *Find the lcm of P_1 and P_2 in each of the examples of Exercise 7.3.*

Exercise 7.7. *Show that if $P_1, P_2 \in \mathbb{R}[x]$ and H is the highest common factor of P_1 and P_2 in $\mathbb{R}[x]$ then there exist $A, B \in \mathbb{R}[x]$ such that $H = AP_1 + BP_2$. Hint: you could build a proof around the table in the proof of Proposition 7.10, that the Euclidean algorithm leads to the hcf of two polynomials, on page 79 of the Lecture Notes. If you can do Exercise 2 then you probably understand what is going on, and writing out a proof here is just a question of getting the notation right.*

Exercise 7.8. *Prove by induction that every polynomial of degree ≥ 1 in $\mathbb{R}[x]$ can be written a product of irreducible polynomials. Hint: do induction on the degree, using POI II. Begin by showing it's true for all polynomials of degree 1 (not hard!). In the induction step, assume it's true for all polynomials of degree ≥ 1 and $< n$ and deduce that it's true for all polynomials of degree n.*

Exercise 7.9. *Prove that the irreducible factorisation in Exercise 7.8 is unique except for reordering and multiplying the factors by non-zero constants. Hint: copy the proof of Part 2 of the Fundamental Theorem of Arithmetic.*

[27] Recall that we are working in $\mathbb{R}[x]$. Does the value of the hcf change if we were to work in $\mathbb{Q}[x]$ or $\mathbb{C}[x]$?

7.2 The Remainder Theorem

The number α is a *root* of the polynomial P if $P(\alpha) = 0$. A polynomial of degree n can have at most n roots, as we will shortly see.

Proposition 7.16. The Remainder Theorem *If $P \in \mathbb{R}[x]$, and $\alpha \in \mathbb{R}$, then on division of P by $x - \alpha$, the remainder is $P(\alpha)$.*

Proof. If

$$P = (x - \alpha)Q + R$$

with $R = 0$ or $\deg(R) < 1 = \deg(x - \alpha)$, then R is in either case constant. Substituting $x = \alpha$ in both sides gives

$$P(\alpha) = 0 \times Q(\alpha) + R,$$

so the constant is $R = P(\alpha)$. □

Corollary 7.17. *If $P \in \mathbb{R}[x]$, $\alpha \in \mathbb{R}$ and $P(\alpha) = 0$ then $x - \alpha$ divides P.* □

Corollary 7.18. *A polynomial $P \in \mathbb{R}[x]$ of degree n can have at most n roots in $\mathbb{R}$.*

Proof. We'll prove this by induction on $n = \deg P$. If $n = 0$ then P is a non-zero constant so certainly has no roots.

Now suppose that $\deg P = n \geq 1$ and that the result holds for polynomials of degree at most $n - 1$. If P has no roots in $\mathbb{R}$ that is fine; otherwise it has a root α and we can write

$$P = (x - \alpha)Q$$

where $\deg Q = n - 1$. By induction, Q has at most $n - 1$ real roots. But any root β of P is either a root of Q, or equals α (or both), since

$$0 = P(\beta) = (\beta - \alpha)Q(\beta).$$

So P has at most one more root than Q, which is at most $1 + (n - 1) = n$ roots. □

Remark 7.19. Proposition 7.16 and Corollaries 7.17,7.18 remain true (and with the same proof) if we substitute $\mathbb{R}$ throughout by $\mathbb{Q}$, or if we substitute $\mathbb{R}$ throughout by $\mathbb{C}$ (or indeed, by any field at all, though since this is a first course, we don't formalise or discuss the definition of "field"). Since $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$, a polynomial with rational or real coefficients can also be thought of as a polynomial in $\mathbb{C}[x]$. So the complex version of Corollaries 7.18 asserts, in particular, that a polynomial of degree n with rational coefficients can have no more than n distinct complex roots. Indeed, a degree n polynomial with coefficients in a field F can have no more than n roots in any field containing F.

For enthusiasts (and not examinable for this course) here are two examples of what can go wrong when our coefficients do not form a field. The polynomial $x^2 - 1$ has more than two roots in $\mathbb{Z}/8$ ($x = 1, 3, 5, 7$ all work, as you may check. You may like to see where the preceding proof breaks down here! For an even worse case, the set $\mathbb{H}$ of "quaternions" behaves exactly like a field *except* that it fails to be commutative; and in $\mathbb{H}$ the equation $x^2 = -1$ has infinitely many solutions!

7.3 The Fundamental Theorem of Algebra

Quite what singles out each Fundamental Theorem as meriting this title is not always clear. But the one we're going to discuss now really does have repercussions throughout algebra and geometry, and even in physics.

Theorem 7.20. *If $P \in \mathbb{C}[x]$ has degree greater than 0, then P has a root in $\mathbb{C}$.*

Corollary 7.21. *If $P \in \mathbb{C}[x]$ has leading coefficient a_n, then P factorises completely into linear factors in $\mathbb{C}[x]$,*

$$P(x) = a_n(x - \alpha_1)\cdots(x - \alpha_n).$$

(Here the α_i do not need to be all distinct from one another).

Proof. By induction on n using Theorem 7.20 and Corollary 7.17. □

Corollary 7.21 is often expressed as the statement:

"Polynomials over $\mathbb{C}$ have as many roots as their degree, counting multiplicities".

Here a number α is said to be a *root of $P(x)$ of multiplicity k* if $x - \alpha$ appears exactly k times in the factorisation of $P(x)$, so that $(x - \alpha)^k \mid P(x)$ but $(x - \alpha)^{k+1} \nmid P(x)$. A root of multiplicity 1 is called a *simple root* while roots of multiplicity $k \geq 2$ are called *multiple roots*. In many applications it is important to be able to detect multiple roots, so the following criterion is useful. It refers to the derivative P' of a polynomial P, which can be defined purely algebraically: the derivative of $P = \sum_k a_k x^k$ is $P' = \sum_k k a_k x^{k-1}$. The usual rules for derivatives of sums and products all apply.

Proposition 7.22. *Let $P(x) \in \mathbb{C}[x]$.*

1. *α is a multiple root of P if and only if $P(\alpha) = P'(\alpha) = 0$.*
2. *P has no multiple roots if* $\mathrm{hcf}(P, P') = 1$.

Proof. (1) If α is a multiple root of P then $P(x) = (x - \alpha)^k R(x)$ with $k \geq 2$ and $R(x) \in \mathbb{C}[x]$. Differentiating gives $P'(x) = (X - \alpha)^{k-1}[(x - \alpha)R'(x) + kR(x)]$, and hence (since $k - 1 > 0$) $P'(\alpha) = 0$.

Conversely if $P(\alpha) = P'(\alpha) = 0$ then $P(x) = (x - \alpha)Q(x)$ for some polynomial Q. Differentiating gives $P'(x) = Q(x) + (x - \alpha)Q'(x)$, so now $P'(\alpha) = 0 \implies Q(\alpha) = 0$ so $(x - \alpha) \mid Q$ and $(x - \alpha)^2 \mid P$.

(2) By (1), P has a multiple root α if and only if P and P' have a common root α, which is if and only if $x - \alpha$ divides both P and P'. This implies (and by Theorem7.20 is equivalent to) $\mathrm{hcf}(P, P')$ having positive degree. □

The remainder of this subsection is devoted to a sketch proof of the Fundamental Theorem of Algebra. It makes use of ideas and techniques that you will not see properly developed until the third year, so is at best impressionistic. *It will not appear on any exam or classroom test, and it will not be covered in lectures.* On the other hand, it is good to stretch your geometric imagination, and it is interesting to see how an apparently algebraic fact can have a geometric proof. So try to make sense of it, but don't be discouraged if in the end you have only gained a vague idea of what it's about. You are welcome to skip the next couple of pages and go straight to Section 7.4.

Sketch proof of Theorem 7.20 Let

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

Because $a_n \neq 0$, we can divide throughout by a_n, so now we can assume that $a_n = 1$. The formula

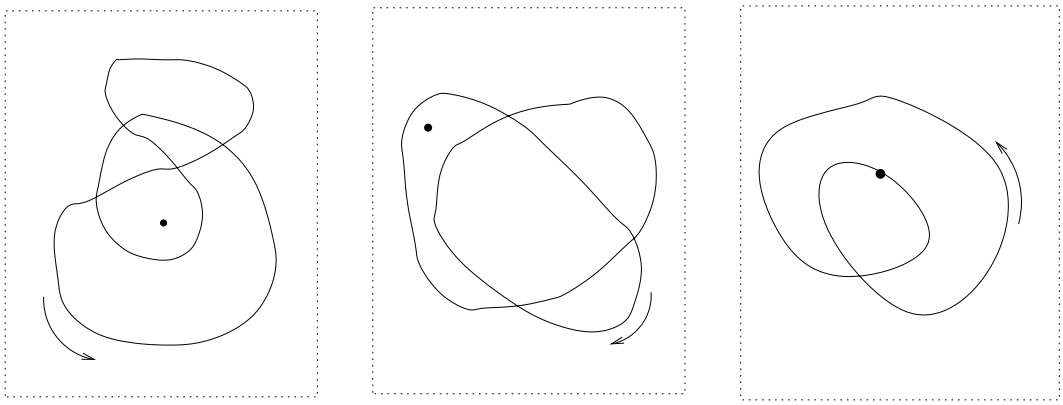
$$P_t(x) = x^n + t(a_{n-1}x^{n-1} + \cdots + a_1 x + a_0)$$

defines a family of polynomials, one for each value of t. We think of t as varying from 0 to 1 in $\mathbb{R}$. When $t = 0$, we have the polynomial x^n, and when $t = 1$ we have the polynomial P we started with.

The polynomial $P_0(x)$ is just x^n, so it certainly has a root, at 0. The idea of the proof is to find a way of making sure that this root does not fly away and vanish as t varies from 0 to 1. We will in fact find a real number R such that each P_t has a root somewhere in the disc D_R of centre 0 and radius R. To do this, we look at what P_t does on the boundary of the disc D_R, namely the circle C_R of centre 0 and radius R.

Each P_t defines a "map" from $\mathbb{C}$ to $\mathbb{C}$, sending each point $x \in \mathbb{C}$ to $P(x) \in \mathbb{C}$. For each point x on C_R we get a point $P_t(x)$ in $\mathbb{C}$, and the collection of all these points, for all the $x \in C_R$, is called the *image* of C_R under P_t. Because P_t is "continuous". a property you will soon learn about in Analysis, the image of C_R under P_t is a closed curve, with no breaks. In the special case of P_0, the image is the circle of radius R^n.

As x goes round the circle C_R once, then $P_0(x)$ goes round the circle C_{R^n} n times. (Remember that the argument of the product of two complex numbers is the sum of their arguments, so the argument of x^2 is twice the argument of x, and by induction the argument of x^n is n times the argument of x.) That is, *as x goes round the circle C_R once, $P_0(x)$ winds round the origin n times*. We say: P_0 winds the circle C_R round the origin n times. For $t \neq 0$, the situation is more complicated. The image under P_t of the circle C_R might look like any one of the curves shown in the picture below.



In each picture I have added an arrow to indicate the direction $P_t(c)$ moves in as x moves round C_R in an anticlockwise direction, and have indicated the origin by a black dot. Although none of the three curves is a circle, for both the first and the second it still makes sense to speak of the *number of times P_t winds the circle C_R round the origin in an anticlockwise direction*. You could measure it as follows: imagine standing at the origin, with your eyes on the point $P_t(x)$. As x moves round the circle C_R in an anticlockwise direction, this point moves, and you have to twist round to keep your eyes on it. The number in question is the number of complete twists you make in the anticlockwise direction minus the number in the clockwise direction.

We call this the *winding number* for short. In the first curve it is 2, and in the second it is -1. But the third curve runs right over the origin, and we cannot assign a winding number. In fact if the origin were shifted upwards a tiny bit (or the curve were shifted down) then the winding number would be 1, and if the origin were shifted downwards a little, the winding number would be 2. What it is important to observe is that if, in one of the first two pictures, the curve moves in such a way that it never passes through the origin, *then the winding number does not change.* Although this is, I hope, reasonably clear from the diagram, it really requires proof. But here I am only giving a sketch of the argument, so I ask you to trust your visual intuition.

We've agreed that the winding number of P_0 is n. Now we show that if R is chosen big enough then the winding number of P_t is still n for each $t \in [0,1]$. The reason is that if we choose R big enough, we can be sure that the image under P_t of C_R never runs over the origin, for any $t \in [0,1]$. For if $|x| = R$ we have

$$|P_t(x)| = |x^n + t(a_{n-1}x^{n-1} + \cdots + a_0)| \geq |x^n| - t\Big(|a_{n-1}||x^{n-1}| + \cdots + |a_0|\Big)$$

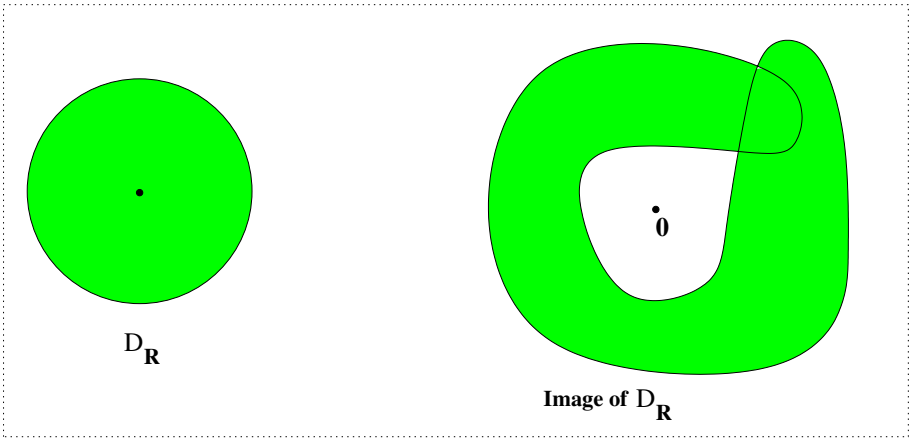
The last expression on the right hand side is equal to

$$= R^n\Big\{1 - t\Big(\frac{|a_{n-1}|}{R} + \frac{|a_{n-2}|}{R^2} + \cdots + \frac{|a_0|}{R^n}\Big)\Big\}$$

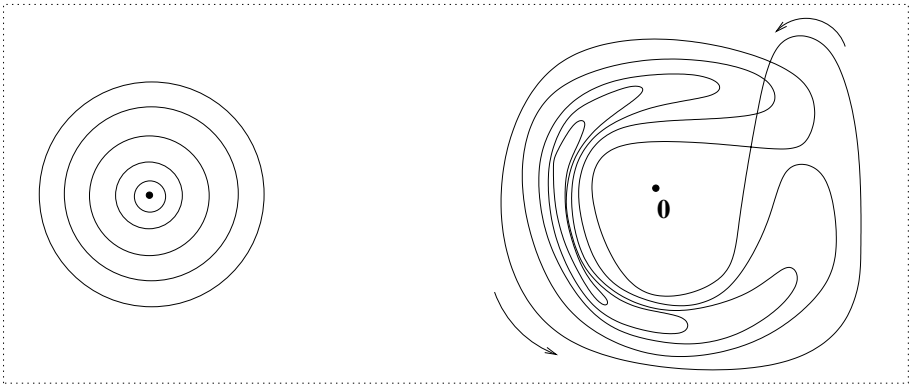
It's not hard to see that if R is big enough, then the expression in round brackets on the right is less than 1, so provided $t \in [0,1]$ and $|x| = R$, $P_t(x) \neq 0$.

So now, as P_0 morphs into P_t, the winding number does not change, because the curve never runs through the origin. In particular, P *itself winds* C_R *round the origin* n *times.*

Now for the last step in the proof. Because P winds C_R round the origin n times, P_R must have a root somewhere in the disc D_R with centre 0 and radius R. For suppose to the contrary that there is no root in D_R. In other words, the image of D_R does not contain the origin, as shown in the picture.



I claim that this implies that the winding number is zero. The argument is not hard to understand. We've agreed that if, as t varies, the curve $P_t(C_R)$ does not at any time pass through the origin, then the number of times P_t winds C_R round the origin does not change. We now apply the same idea to a different family of curves.



The disc D_R is made up of the concentric circles $C_{\lambda R}, \lambda \in [0,1]$, some of which are shown in the lower picture on the left in the diagram at the foot of the last page. The images of these circles lie in the image of D_R. If the image of D_R does not contain the origin, then none of the images of the circles $C_{\lambda R}$ passes through the origin. It follows that *the number of times P winds the circle $C_{\lambda R}$ around the origin does not change as λ varies from 0 to 1.*

When $\lambda = 0$, the circle $C_{\lambda R}$ is reduced to a point, and its image is also just a single point. When λ is very small, the image of $C_{\lambda R}$ is very close to this point, and clearly cannot wind around the origin any times at all. That is, for λ small, P winds the curve $C_{\lambda R}$ around the origin 0 times. The same must therefore be true when $\lambda = 1$. In other words, *if P does not have a root in D_R then P winds C_R round the origin 0 times.*

But we've shown that P winds C_R n times around the origin if R is big enough. Since we are assuming that $n > 0$, this means that a situation like that shown in the picture is impossible: the image of D_R under P must contain the origin. In other words, P must have a root somewhere in the disc D_R. □

7.4 Algebraic numbers

A complex number α is an *algebraic number* if it is a root of a nonzero polynomial $P \in \mathbb{Q}[x]$. For example, for any $n \in \mathbb{N}$, the n'th roots of any positive rational number q are algebraic numbers, being roots of the rational polynomial

$$x^n - q.$$

In particular the set of algebraic numbers contains $\mathbb{Q}$ (take $n = 1$).

The set of algebraic numbers is in fact a field. This is rather non-obvious: it is not obvious how to prove, in general, that the sum and product of algebraic numbers are algebraic (though see the exercises at the end of this section).

It is not hard to show (using Exercise 7.7) that if α is a root of both P and $Q \in \mathbb{Q}[x]$ then it is root of $\mathrm{hcf}(P,Q)$. It then follows that if we let P be the polynomial of *least degree* with α as a root, then every other polynomial with α as a root is a *multiple* of P. This P (scaled to be monic) is called the *minimal polynomial* of the algebraic number α. For example, $\alpha = \sqrt{5} + \sqrt{6}$ is algebraic and has minimal polynomial $x^4 - 22x^2 + 1$. (To check this, first show that $\alpha^2 = 11 + 2\sqrt{30}$.) The study of algebraic numbers is (not surprisingly) called Algebraic Number Theory (see the Third Year course MA3A6); it was developed by people trying to prove Fermat's Last Theorem, using Roots of Unity (which are algebraic, being roots of $x^n - 1$).

Complex numbers which are not algebraic are *transcendental*. It is not obvious that there are any transcendental numbers. In the next (and final) chapter we will develop methods which show that in fact almost all complex numbers are transcendental. Surprisingly, showing that any individual complex number is transcendental is much harder. Apostol's book on Calculus (see the Introduction) gives a straightforward, though long, proof that e is transcendental. A famous monograph of Ivan Niven, "Irrational numbers", (available from the library) contains a clear proof that π is transcendental. This has an interesting implication for the classical geometrical problem of "squaring the circle", since it is not hard to prove[28] that any length one can get by geometrical constructions with ruler and compass, starting from a fixed unit, is an algebraic number. For example, the length $x = \sqrt{2}$ in the diagram on page 28 is an algebraic number. Because π is transcendental (and therefore so is $\sqrt{\pi}$), there can be no construction which produces a square whose area is equal to that of an arbitrary given circle.

Exercise 7.10. *(i) Show that if $\alpha \in \mathbb{C}$, and for some positive integer n, α^n is algebraic, then α is algebraic too. Deduce that if $\alpha \in \mathbb{C}$ is transcendental, then so is $\alpha^{\frac{1}{n}}$ for any $n \in \mathbb{N}$.*

Exercise 7.11. *(i) Find a polynomial in $\mathbb{Q}[x]$ with $\sqrt{2}\sqrt{3}$ as a root. (ii) Ditto for $\sqrt{2} \times 3^{\frac{1}{3}}$. (iii) Ditto for $\sqrt{2} + \sqrt{3}$. Hint: by subtracting suitable multiples of even powers of $\sqrt{2} + \sqrt{3}$ from one another, you can eliminate the square roots. (iv)* Can you do it for $\sqrt{2} + 3^{\frac{1}{3}}$?*

As an application of our work on polynomials, and the factorisation theory of integers we can prove the following which is both a huge help in finding rational roots of integer polynomials, and also gives a way to prove that numbers are irrational.

Proposition 7.23. *Let $P(x) = a_d x^d + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ and let α be a root of P.*

1. *If $\alpha \in \mathbb{Z}$ then $\alpha \mid a_0$;*
2. *More generally, if $\alpha = m/n \in \mathbb{Q}$ with $\mathrm{hcf}(m, n) = 1$ then $m \mid a_0$ and $n \mid a_d$.*

Proof. (1) $a_0 = -a_1\alpha - a_2\alpha^2 - \cdots - a_d\alpha^d \in \alpha\mathbb{Z}$. (2) Substitute $\alpha = m/n$ in $P(\alpha) = 0$ and clear denominators to get

$$a_d m^d + a_{d-1} m^{d-1} n + \cdots + a_1 m n^{d-1} + a_0 n^d = 0.$$

So $m \mid a_0 n^d$; but $\mathrm{hcf}(m, n^d) = 1$, so $m \mid a_0$. Similarly, $n \mid a_d m^d \implies n \mid a_d$. □

Examples. We can use this to show that many algebraic numbers are irrational.

1. $\alpha = \sqrt{77}$ is a root of $x^2 - 77$. If $\alpha = m/n$ were rational it would have to be an integer since $n \mid 1$, but $8 < \alpha < 9$ so $\alpha \notin \mathbb{Z}$. hence α must be irrational!
2. $\alpha = \sqrt{2} + \sqrt{3}$ is a root of $x^4 - 10x^2 + 1$ (see previous exercise), so if $\alpha = m/n$ were rational then $m \mid 1$ and $n \mid 1$ which implies $\alpha = \pm 1$. This is ridiculous since $\alpha > 3$; so α is irrational.

[28] See, for instance, Ian Stewart, *Galois Theory*, Chapter 5

8 Counting: to infinity and beyond?

8.1 Different Infinities

We return to the question which we started to consider in section 6.3: what does it mean to count? We have answered this question in the case of finite sets: a set A is finite if there is a bijection $\{1, \ldots, n\} \to A$, and in this case[29] the number of elements in A is n, and write $|A| = n$. If there is no bijection $\{1, \ldots, n\} \to A$ for any $n \in \mathbb{N}$, we say A is infinite. Is that the end of the story? Do all infinite sets have the same number of elements? More precisely, given any two infinite sets, is there necessarily a bijection between them? The answer is no. In this section we will prove that $\mathbb{R}$ is *not* in bijection with $\mathbb{N}$. But we will begin with

Proposition 8.1. *If $B \subset \mathbb{N}$ is infinite then there is a bijection $c : \mathbb{N} \to B$.*

We will also prove

1. Many other infinite sets, such as $\mathbb{Q}$, are also in bijection with $\mathbb{N}$.
2. The set of algebraic numbers is in bijection with $\mathbb{N}$.
3. There are infinitely many different infinities.

Definition 8.2. *The set A is* **countable** *if there is a bijection between A and some subset of $\mathbb{N}$ (possibly $\mathbb{N}$ itself); A is* **countably infinite** *if it is countable but not finite.*

Proposition 8.1 implies

Corollary 8.3. *Every countably infinite set is in bijection with $\mathbb{N}$.*

Proof. Suppose A is a countably infinite set. Then there is a bijection $f : A \to B$, where B is some infinite subset of $\mathbb{N}$. By Proposition 8.1, there is a bijection $c : \mathbb{N} \to B$ whose inverse is a bijection $c^{-1} : B \to \mathbb{N}$. Therefore $c^{-1} \circ f$ is a bijection from A to $\mathbb{N}$. □

Proof. of Proposition 8.1 Define a bijection $c : \mathbb{N} \to B$ as follows: let b_0 be the least element of B (using WOP), and set $c(0) = b_0$. Let b_1 be the least element of $\mathbb{N} \setminus \{b_0\}$ (using WOP again), and set $c(1) = b_1$. Let c_2 be the least element of $B \setminus \{b_0, b_1\}$. Set $c(2) = b_2$. Etc.

Since B is assumed to be infinite, this procedure never terminates. That is, for every n, $B \setminus \{b_0, b_1, \ldots, b_n\}$ is always non-empty, so by the WOP has a least element, b_{n+1}, and we can define $c(n+1) = b_{n+1}$. Thus, by induction on $\mathbb{N}$, $c(n)$ is defined for all n. The map c is injective, for $b_{n+1} > b_n$ for all n, so if $m > n$ it follows that $c(m) > c(n)$. It is surjective, because if $b \in B$ then b is equal to one of $c(0), c(1), \ldots, c(b)$ since $n \leq c(n)$ for all n (remember that $B \subset \mathbb{N}$). Thus c is a bijection. □

Proposition 8.4. *The set of rational numbers is countably infinite.*

Proof. Define an mapping $g : \mathbb{Q} \to \mathbb{N}$, as follows:

- $g(0) = 0$

[29] As a special case, $|A| = 0$ if there is a bijection from the empty set $\{\}$ to A. A function with empty domain may seem strange to you, but it is certainly surjective since no element of A fails to be in its image!

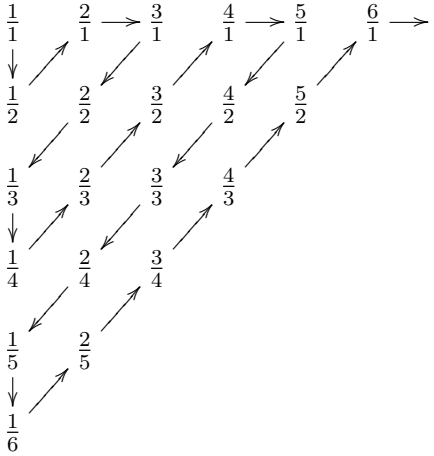
- if $q \in \mathbb{Q}$ is positive and written in lowest form as $\frac{m}{n}$ (with $m, n \in \mathbb{N}$) then $g(q) = 2^m \cdot 3^n$
- if $q \in \mathbb{Q}$ is negative and is written in lowest form as $q = -\frac{m}{n}$ with $m, n \in \mathbb{N}$ then $g(q) = 2^m \cdot 3^n \cdot 5$.

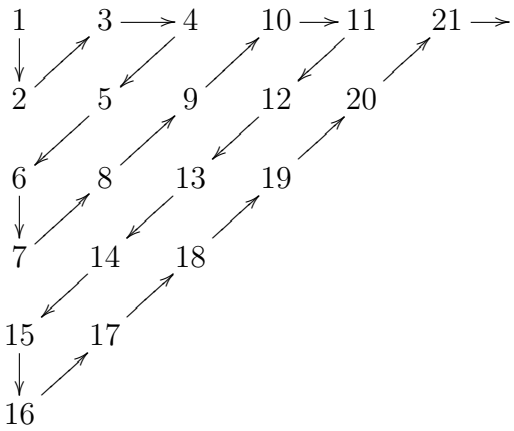
Uniqueness of factorisation into primes implies that g is an injection, and clearly its image is infinite. By definition this means that $\mathbb{Q}$ is countably infinite. □

Here is a graphic way of counting the positive rationals. The array

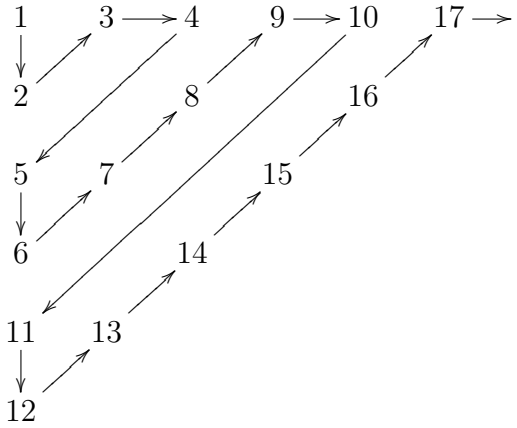
$$\begin{array}{ccccccc} \frac{1}{1} & \frac{2}{1} & \frac{3}{1} & \frac{4}{1} & \frac{5}{1} & \cdots \\ \frac{1}{2} & \frac{2}{2} & \frac{3}{2} & \frac{4}{2} & \frac{5}{2} & \cdots \\ \frac{1}{3} & \frac{2}{3} & \frac{3}{3} & \frac{4}{3} & \frac{5}{3} & \cdots \\ \frac{1}{4} & \frac{2}{4} & \frac{3}{4} & \frac{4}{4} & \frac{5}{4} & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \end{array}$$

contains every positive rational number (with repetitions such as $\frac{2}{2}$ or $\frac{2}{4}$). We count them as indicated by the following zigzag pattern:





This defines a surjection $\mathbb{N} \to \mathbb{Q}_{>0}$, but not an injection, as it takes no account of the repetitions. For example, it maps $1, 5, 13, \ldots$ all to $1 \in \mathbb{Q}$. But this is easily remedied by simply skipping each rational not in lowest form; the enumeration becomes



We have defined a bijection $\mathbb{N} \to \mathbb{Q}_{>0}$.

Exercise 8.1. *(i) Suppose that X_1 and X_2 are countably infinite. Show that $X_1 \times X_2$ is countably infinite. Hint: both proofs of the countability of $\mathbb{Q}$ can be adapted to this case. Go on to prove by induction that if $X_1, \ldots, X_n$ are all countably infinite then so is $X_1 \times \cdots \times X_n$. (ii) Suppose that each of the sets $X_1, X_2, \ldots, X_n \ldots$ is countably infinite. Show that their union $\cup_{n\in\mathbb{N}} X_n$ is countably infinite. Hint 1: make an array like the way we displayed the positive rationals in the previous paragraph. Define a map by a suitable zig-zag. Hint 2: do part (iii) and then find a surjection $\mathbb{N} \times \mathbb{N} \to \cup_{n\in\mathbb{N}} X_n$. (iii) Show that if A is a countable set and there is a surjection $g : A \to B$ then B is also countable. Hint: a surjection has a right inverse, which is an injection.*

Proposition 8.5. *The set A of algebraic numbers is countably infinite.*

Proof. The set of polynomials $\mathbb{Q}[x]_{\leq n}$ of degree $\leq n$, with rational coefficients, is countably infinite: there is a bijection $\mathbb{Q}[x]_{\leq n} \to \mathbb{Q}^{n+1}$, defined by mapping the polynomial $a_0 + a_1 x + \cdots + a_n x^n$ to $(a_0, a_1, \ldots, a_n) \in \mathbb{Q}^{n+1}$, and by Exercise 8.1(i), $\mathbb{Q}^{n+1}$ is countably infinite. It follows, again by Exercise 8.1(i), that $\mathbb{Q}[x]_{\leq n} \times \{1, \ldots, n\}$ is countably infinite.

Each non-zero polynomial in $\mathbb{Q}[x]_{\leq n}$ has at most n roots. If $P \in \mathbb{Q}[x]_{\leq n}$, order its roots in some (arbitrary) way, as $\alpha_1, \ldots, \alpha_k$. Define a surjection

$$f_n : \big(\mathbb{Q}[x]_{\leq n} \smallsetminus \{0\}\big) \times \{1, 2, \ldots, n\} \to A_n$$

by

$$f(P, j) = j\text{'th root of } P.$$

(if P has k roots and $k < n$, define $f_n(P, k+1) = \cdots = f_n(P, n) = \alpha_k$). As there is a surjection from a countable set to A_n, A_n itself is countable. It is clearly infinite.

Finally, the set A of algebraic numbers is the union $\cup_{n\in\mathbb{N}} A_n$, so by Exercise 8.1(ii), A is countably infinite. □

So far, we've only seen *one* infinity.

Proposition 8.6. *The set $\mathbb{R}$ of real numbers is not countable.*

Proof. If $\mathbb{R}$ is countable then so is the open interval $(0, 1)$. Suppose that $(0, 1)$ is countable. Then by Corollary 8.3 its members can be enumerated[30], as a_1, a_2, …, a_k, …, with decimal expansions

$$\begin{aligned} a_1 &= 0.\, a_{11}\, a_{12}\, a_{13} \ldots \\ a_2 &= 0.\, a_{21}\, a_{22}\, a_{23} \ldots \\ \ldots &= \ldots.\ldots \\ a_k &= 0.\, a_{k1}\, a_{k2}\, a_{k3} \ldots \\ \ldots &= \ldots.\ldots \end{aligned}$$

(to avoid repetition, we avoid decimal expansions ending in an infinite sequence of 9's.) To reach a contradiction, it is enough to produce just *one* real number in $(0, 1)$ which is not on this list. We construct such a number as follows: for each k, choose any digit b_k between 1 and 8 which is different from a_{kk}. Consider the number

$$b = 0\,.\, b_1\, b_2 \ldots b_k \ldots$$

[30]It is more convenient here to start counting at 1 and not 0.

Its decimal expansion differs from that of a_k at the k'th decimal place. Because we have chosen the b_k between 1 and 8 we can be sure that $b \in (0,1)$ and is not equal in value to any of the a_k. We conclude that *no enumeration can list all of the members of* $(0,1)$. That is, $(0,1)$ is not countable. □

This argument, found by Georg Cantor (1845-1918) in 1873, is known as Cantor's diagonalisation argument.

Corollary 8.7. *Transcendental numbers exist.*

Proof. If every real number were algebraic, then $\mathbb{R}$ would be countable. □

Exercise 8.2. *(i) Find a bijection* $(-1,1) \to \mathbb{R}$. *(ii) Suppose* a *and* b *are real numbers and* $a < b$. *Find a bijection* $(a,b) \to \mathbb{R}$.

The fact that the infinity of $\mathbb{R}$ is different from the infinity of $\mathbb{N}$ leads us to give them names, and begin a theory of transfinite numbers. We say that two sets have the *same cardinality* if there is a bijection between them. The cardinality of a set is the generalisation of the notion, defined only for finite sets, of the "number of elements it contains". The cardinality of $\mathbb{N}$ is denoted by $\aleph_0$; the fact that $\mathbb{Q}$ and $\mathbb{N}$ have the same cardinality is indicated by writing $|\mathbb{Q}| = \aleph_0$. The fact that $|\mathbb{R}| \neq \aleph_0$ means that there are infinite cardinals different from $\aleph_0$. Does the fact that $\mathbb{N} \subset \mathbb{R}$ mean that $\aleph_0 < |\mathbb{R}|$? And are there any other infinite cardinals in between? In fact, does it even make sense to speak of one infinite cardinal being bigger than another?

Suppose that there is a bijection $j : X_1 \to X_2$ and a bijection $k : Y_1 \to Y_2$. Then if there is an injection $X_1 \to Y_1$, there is also an injection $i_2 : X_2 \to Y_2$, $i_2 = k \circ i_1 \circ j^{-1}$, as indicated in the following diagram:

$$\begin{array}{ccc} X_2 & \overset{i_2}{\rightarrowtail} & Y_2 \\ {\scriptstyle j^{-1}}\downarrow & & \uparrow{\scriptstyle k} \\ X_1 & \underset{i_1}{\rightarrowtail} & Y_1 \end{array}$$

Similarly, if there is a surjection $X_1 \to Y_1$ then there is also a surjection $X_2 \to Y_2$.

This suggests the following definition.

Definition 8.8. *Given cardinals* $\aleph$ *and* $\aleph'$, *we say that* $\aleph \leq \aleph'$ *(and* $\aleph' \geq \aleph$*) if there are sets* X *and* Y *with* $|X| = \aleph$ *and* $|Y| = \aleph'$, *and an injection* $X \to Y$.

Note that By Proposition 6.16, $|X| \geq |Y|$ also if there is a surjection $X \to Y$.

This definition raises the natural question: is it true [31] that

$$|X| \leq |Y| \quad \text{and} \quad |Y| \leq |X| \quad \Longrightarrow \quad |X| = |Y|?$$

In other words, if there is an injection $X \to Y$ and an injection $Y \to X$ then is there a bijection $X \to Y$?

Theorem 8.9. Schroeder-Bernstein Theorem *If* X *and* Y *are sets and there are injections* $i : X \to Y$ *and* $j : Y \to X$ *then there is a bijection* $X \to Y$.

[31] The analogous statement is certainly true if we have integers or real numbers p, q in place of the cardinals $|X|, |Y|$.

Proof. Given $y_0 \in Y$, we trace its ancestry. Is there an $x_0 \in X$ such that $i(x_0) = y_0$? If there is, then is there a $y_1 \in Y$ such that $j(y_1) = x_0$? And if so, is there an $x_1 \in X$ such that $i(x_1) = y_1$? And so on. Points in Y fall into three classes:

1. those points for which the line of ancestry originates in Y
2. those points for which the line of ancestry originates in X.
3. those points for which the line of ancestry never terminates

Call these three classes Y_Y, Y_X and Y_∞. Clearly $Y = Y_Y \cup Y_X \cup Y_\infty$, and any two among Y_∞, Y_Y and Y_X have empty intersection.

Divide X into three parts in the same way:

1. X_X consists of those points for which the line of ancestry originates in X;
2. X_Y consists of those points for which the line of ancestry originates in Y
3. X_∞ consists of those points for which the line of ancestry never terminates.

Again, these three sets make up all of X, and have empty intersection with one another. Note that

1. i maps X_X to Y_X,
2. j maps Y_Y to X_Y,
3. i maps X_∞ to Y_∞.

Indeed,

1. i determines a bijection $X_X \to Y_X$
2. j determines a bijection $Y_Y \to X_Y$
3. i determines a bijection $X_\infty \to Y_\infty$.

Define a map $f : X \to Y$ by

$$f(x) = \begin{cases} i(x) & \text{if } x \in X_X \\ j^{-1}(x) & \text{if } x \in X_Y \\ i(x) & \text{if } x \in X_\infty \end{cases}$$

Then f is the required bijection. □

The Schroeder Bernstein Theorem could be used, for example, to prove Proposition 8.4, that $|\mathbb{Q}| = \aleph_0$, as follows: as in the first proof of Proposition 8.4 we construct an injection $\mathbb{Q} \to \mathbb{Z}$ (sending $\pm\frac{m}{n}$ to $\pm 2^m 3^n$), and then an injection $\mathbb{Z} \to \mathbb{N}$ (say, sending a non-negative integer n to $2n$ and a negative integer $-n$ to $2n-1$). Composing the two give us an injection $\mathbb{Q} \to \mathbb{N}$. As there is also an injection $\mathbb{N} \to \mathbb{Q}$ (the usual inclusion), Schroeder-Bernstein applies, and says that there must exist a bijection.

Exercise 8.3. *Use the Schroeder-Bernstein Theorem to give another proof of Proposition 8.1. Hint: saying that a set X is infinite means precisely that when you try to count it, you never finish; in other words, you get an injection $\mathbb{N} \to X$.*

Let X and Y be sets. We say that $|X| < |Y|$ if $|X| \leq |Y|$ but $|X| \neq |Y|$. In other words, $|X| < |Y|$ if there is an injection $X \to Y$ but there is no bijection $X \to Y$.

Definition 8.10. *Let X be a set. Its* **power set** $\mathscr{P}(X)$ *is the set of all the subsets of X.*

If $X = \{1, 2, 3\}$ then X has eight distinct subsets:

$$\emptyset, \{1\},\ \{2\},\ \{3\},\ \{2, 3\},\ \{1, 3\},\ \{1, 2\},\ \{1, 2, 3\}$$

so $\mathscr{P}(X)$ has these eight members. It is convenient to count $\emptyset$ among the subsets of X, partly because this gives the nice formula proved in the following proposition, but also, of course, that it is true (vacuously) that every element in $\emptyset$ does indeed belong to X.

Proposition 8.11. *If $|X| = n$ then $|\mathscr{P}(X)| = 2^n$.*

Proof. Order the elements of X, as $x_1, \ldots, x_n$. Each subset Y of X can be represented by an n-tuple of 0's and 1's: there is a 1 in the i'th place if $x_i \in Y$, and a 0 in the i'th place if $x_i \notin Y$. For example, $\emptyset$ is represented by $(0, 0, \ldots, 0)$, and X itself by $(1, 1, \ldots, 1)$. We have determined in this way a bijection

$$\mathscr{P}(X) \to \underbrace{\{0, 1\} \times \cdots \times \{0, 1\}}_{n \text{ times}} = \{0, 1\}^n.$$

The number of distinct subsets is therefore equal to the number of elements of $\{0, 1\}^n$, 2^n. □

So if X is a finite set, $|X| < |\mathscr{P}(X)|$. The same is true for infinite sets.

Proposition 8.12. *If X is a set, there can be no surjection $X \to \mathscr{P}(X)$.*

Proof. Suppose that $p : X \to \mathscr{P}(X)$ is a map. We will show that p cannot be surjective by finding some $P \in \mathscr{P}(X)$ such that $p(x) \neq P$ for any $x \in X$. To find such a P, note that since for each x, $p(x)$ is a subset of X, it makes sense to ask: does x belong to $p(x)$? Define

$$P = \{x \in X : x \notin p(x)\}.$$

Claim: for no x in X can we have $p(x) = P$. For suppose that $p(x) = P$. If $x \in P$, then $x \in p(x)$, so by definition of P, $x \notin P$. If $x \notin P$, then $x \notin p(x)$, so by definition of P, $x \in P$. That is, the supposition that $p(x) = P$ leads us to a contradiction. Hence we cannot have $p(x) = P$ for any $x \in X$, and so p is not surjective. □

The set P in the proof is not itself paradoxical: in the case of the map

$$p : \{1, 2, 3\} \to \mathscr{P}(\{1, 2, 3\})$$

defined by

$$p(1) = \{1, 2\},\ p(2) = \{1, 2, 3\},\ p(3) = \emptyset,$$

P is the set $\{3\}$, since only 3 does not belong to $p(3)$. And indeed, no element of $\{1, 2, 3\}$ is mapped to $\{3\}$. If $p : \{1, 2, 3\} \to \mathscr{P}(\{1, 2, 3\})$ is defined by

$$p(1) = \{1\},\ p(2) = \{2\},\ p(3) = \{3\}$$

then $P = \emptyset$; again, for no $x \in \{1, 2, 3\}$ is $p(x)$ equal to P.

Corollary 8.13. *For every set X, $|X| < |\mathscr{P}(X)|$.*

Proof. There is an injection $X \to \mathscr{P}(X)$: for example, we can define $i : X \to \mathscr{P}(X)$ by $i(x) = \{x\}$. Hence, $|X| \leq |\mathscr{P}(X)|$. Since there can be no surjection $X \to \mathscr{P}(X)$, there can be no bijection, so $|X| \neq |\mathscr{P}(X)|$. □

Corollary 8.14. *There are infinitely many different infinite cardinals.*

Proof.

$$\aleph_0 = |\mathbb{N}| < |\mathscr{P}(\mathbb{N})| < |\mathscr{P}(\mathscr{P}(\mathbb{N}))| < |\mathscr{P}(\mathscr{P}(\mathscr{P}(\mathbb{N})))| < \cdots.$$

□

8.2 Concluding Remarks

Questions

1. What is the next cardinal after $\aleph_0$?
2. Is there a cardinal between $\aleph_0$ and $|\mathbb{R}|$?
3. Does question 1 make sense? In other words, does the Well-Ordering Principle hold among infinite cardinals?
4. Given any two cardinals, $\aleph$ and $\aleph'$, is it always the case that either $\aleph \leq \aleph'$ or $\aleph' \leq \aleph$? In other words, given any two sets X and Y, is it always the case that there exists an injection $X \to Y$ or an injection $Y \to X$ (or both)?

None of these questions has an absolutely straightforward answer. To answer them with any clarity it is necessary to introduce an axiomatisation of set theory; that is, a list of statements whose truth we accept, and which form the starting point for all further deductions. Axioms for set theory were developed in the early part of the twentieth century in response to the discovery of paradoxes, like Russell's paradox, described on page 54 of these lecture notes, which arose from the uncritical assumption of the "existence" of any set one cared to define — for example, Russell's "set of all sets which are not members of themselves". The standard axiomatisation is the Zermelo-Fraenkel axiomatisation ZF. There is no time in this course to pursue this topic. The final chapter of Stewart and Tall's book *The Foundations of Mathematics* lists the von Neumann-Gödel-Bernays axioms, a mild extension of ZF. A more sophisticated account, and an entertaining discussion of the place of axiomatic set theory in the education of a mathematician, can be found in Halmos's book *Naive Set Theory*. Surprisingly, quite a lot is available on the internet.

Of the questions above, Question 4 is the easiest to deal with. The answer is that if we accept the Axiom of Choice, then Yes, every two cardinals can be compared. In fact, the comparability of any two cardinals is equivalent to the Axiom of Choice.

The Axiom of Choice says the following: if $X_\alpha, \alpha \in A$ is a collection of non-empty sets indexed by the set A — that is, for each element α in A there is a set X_α in the collection — then there is a map from the index set A to $\cup_\alpha X_\alpha$ such that $f(\alpha) \in X_\alpha$ for each $\alpha \in A$. The statement seems unexceptionable, and if the index set A is finite then one can construct such a map easily enough, without the need for a special axiom. However, since the Axiom of Choice involves the completion of a possibly infinite process, it is not accepted by all mathematicians to the same extent as the other axioms of set theory. It was shown to be independent of the Zermelo-Fraenkel axioms for set theory by Paul Cohen in 1963.

Remark 8.15. We have tacitly used the Axiom of Choice in our proof of Proposition 6.16, that if $p : X \to Y$ is a surjection then there is an injection $i : Y \to X$ which is a right inverse to p. Here is how a formal proof, using the Axiom of Choice, goes: Given a surjection p, for each $y \in Y$ define

$$X_y = \{x \in X : p(x) = y\}$$

(this is what we called $f^{-1}(y)$ at the end of Section 6.4 on page 63). The collection of sets X_y is, indeed, indexed by Y. Clearly

$$\bigcup_{y \in Y} X_y = X,$$

and now the Axiom of Choice asserts that there is a map i from the index set Y to X, such that for each $y \in Y$, $i(y) \in X_y$. This means that i is a right inverse to p, and an injection, as required.

Almost without exception, the Axiom of Choice and the Zermelo-Fraenkel axioms are accepted and used by every mathematician whose primary research interest is not set theory and the logical foundations of mathematics. However, you will rarely find Axiom of Choice used explicitly in any of the courses in a Mathematics degree. Nevertheless, a statement equivalent to the Axiom of Choice, *Zorn's Lemma*, is used, for example to prove that every vector space has a basis[32], and that every field has an algebraic closure. The comparability of any two cardinals is also an easy deduction from Zorn's Lemma. Unfortunately it would take some time to develop the ideas and definitions needed to state it, so we do not say more about it here. Again, Halmos's book contains a good discussion.

There is a remarkable amount of information about the Axiom of Choice on the Internet. A Google search returns more than 1.5 million results. Some of it is very good, in particular the entries in *Wikipedia* and in *Mathworld*, and worth looking at to learn about the current status of the axiom. One interesting development is that although very few mathematicians oppose its unrestricted use, there is an increasing group of computer scientists who reject it.

The *Continuum Hypothesis* is the assertion that the answer to Question 2 is No, that there is no cardinal intermediate between $|\mathbb{N}|$ and $|\mathbb{R}|$. Another way of stating it is to say that if X is an infinite subset of $\mathbb{R}$ then either $|X| = \aleph_0$ or $|X| = |\mathbb{R}|$. For many years after it was proposed by Cantor in 1877, its truth was was an open question. It was one of the list of 23 important unsolved problems listed by David Hilbert at the International Congress of Mathematicians in 1900. In 1940 Kurt Gödel showed that no contradiction would arise if the Continuum Hypothesis were added to the ZF axioms for set theory, together with the Axiom of Choice. The set theory based on the Zermelo Fraenkel axioms together with the Axiom of Choice is known as ZFC set theory. Gödel's result here is summarised by saying that the Continuum Hypothesis is *consistent* with ZFC set theory. It is far short of the statement that the Continuum Hypothesis *follows from* ZFC, however. Indeed, in 1963 Cohen showed that no contradiction would arise either, if the *negation* of the Continuum Hypothesis were assumed. So both its truth and its falsity are consistent with ZFC set theory, and neither can be proved from ZFC.

[32]Zorn's lemma is not needed here to prove the result for finite dimensional vector spaces