Introduction to University Mathematics

Richard Earl

Michaelmas 2019

SYNOPSIS

- The natural numbers and their ordering. Induction as a method of proof, including a proof of the binomial theorem with non-negative integral coefficients. [1.5]
- Sets. Examples including $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and intervals in $\mathbb{R}$. Inclusion, union, intersection, power set, ordered pairs and Cartesian product of sets. Truth tables, equivalent logical results, quantifiers. Relations. Definition of an equivalence relation. Examples. [2.5]
- Functions: composition, restriction; injective (one-to-one), surjective (onto) and invertible functions; images and preimages. [2]
- Writing mathematics and addressing quantifiers. Formulation of mathematical statements with examples.
- Proofs and refutations: standard techniques for constructing proofs; counter-examples. Example of proof by contradiction and more on proof by induction.
- Problem-solving in mathematics: experimentation, conjecture, confirmation, followed by explaining the solution precisely. [2]

RECOMMENDED READING

- C.J.K.Batty, *How do Undergraduates do Mathematics?,* (Mathematical Institute Study Guide, 1994)
- K.Houston, *How to Think Like a Mathematician,* (CUP, 2009)
- L.Alcock, *How to Study for a Mathematics Degree,* (OUP, 2012)
- R.B.J.T.Allenby, *Numbers and Proofs*, (Butterworth-Heinemann, London, 1997)
- R.A.Earl, *Towards Higher Mathematics* (CUP, 2017) – Chapter 2 on induction

SET THEORETIC AND LOGICAL NOTATION

IMPORTANT SETS

$\mathbb{N}$ – the set of *natural* numbers $\{0, 1, 2, \ldots\}$. (Another common convention begins with 1.)
$\mathbb{Z}$ – the set of *integers* $\{0, \pm 1, \pm 2, \ldots\}$.
$\mathbb{Q}$ – the set of *rational* numbers.
$\mathbb{R}$ – the set of *real* numbers.
$\mathbb{C}$ – the set of *complex* numbers.
$\mathbb{Z}_n$ – the *integers, modulo* $n \geqslant 2$.
$\mathbb{R}^n$ – *n-dimensional real space* – the set of all real n-tuples $(x_1, x_2, \ldots, x_n)$.
$\mathbb{R}[x]$ – the set of *polynomials* in x with real coefficients.
$\varnothing$ – the empty set

For $a, b \in \mathbb{R}$ with $a < b$ we define
$(a, b) = \{x \in \mathbb{R} : a < x < b\}$.
$(a, b] = \{x \in \mathbb{R} : a < x \leqslant b\}$.
$[a, b) = \{x \in \mathbb{R} : a \leqslant x < b\}$.
$[a, b] = \{x \in \mathbb{R} : a \leqslant x \leqslant b\}$.

SET THEORETIC NOTATION

$X \cup Y$ – the *union* of X and Y – $\{s : s \in X \text{ or } s \in Y\}$.
$X \cap Y$ – the *intersection* of X and Y – $\{s : s \in X \text{ and } s \in Y\}$.
$X \times Y$ – the *Cartesian product* of X and Y – $\{(x, y) : x \in X \text{ and } y \in Y\}$.
$X - Y$ or $X \backslash Y$ – the *complement* of Y in X – $\{s : s \in X \text{ and } s \notin Y\}$.
$\mathcal{P}(X)$ – the *power set* of a set X, that is the set of subsets of X.
$\in$ – is an *element* of, e.g. $\sqrt{2} \in \mathbb{R}$ and $\pi \notin \mathbb{Q}$.
$\subset, \subseteq$ – is a *subset* of, e.g. $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.
$f \colon X \to Y$ – f is a *function*, map, mapping from a set X (the domain) to a set Y (the codomain).
$f(X)$ – the *image* or *range* of the function f – i.e. the set $\{f(x) : x \in X\}$.
$g \circ f$ – the *composition* of the maps g and f – do f first then g.
$|X|$ – the *cardinality* (size) of the set X

LOGICAL NOTATION

$\forall$	for all	$\Rightarrow$	implies, is sufficient for, only if
$\exists$	there exists	$\Leftarrow$	is implied by, is necessary for, if
$\exists!$	there exists unique	$\Leftrightarrow$	if and only if, is logically equivalent to
$\neg$	negation, not	: or | or s.t.	such that
$\vee$	or	$\square$ or QED	found at the end of a proof
$\wedge$	and		

The Greek Alphabet

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

1. THE NATURAL NUMBERS AND INDUCTION

1.1 The Natural Numbers

We already know intuitively what the natural numbers are. Here is a definition – this first description does not define them in terms of anything more basic but just says they are what you think they are.

Definition 1 *A **natural number** is a non-negative whole number. That is it is a member of the sequence* $0, 1, 2, 3, \ldots$ *obtained by starting from 0 and adding 1 successively. We write* $\mathbb{N}$ *for the set* $\{0, 1, 2, 3, \ldots\}$ *of all natural numbers.*

When discussing foundational material it is convenient to include 0 as a natural number. In the rest of mathematics though, and life more generally, one starts counting at 1, so you will also see $\mathbb{N}$ defined as the set $\{1, 2, 3, \ldots\}$. Observe here we are using curly brackets or braces to gather together objects into a set. We will discuss sets in more detail in the next chapter.

Beyond the set $\mathbb{N}$ of natural numbers, there are operations and relations associated with $\mathbb{N}$. Given natural numbers x, y then we can associate their **sum** $x + y$ in $\mathbb{N}$ and their **product** $x \times y$ in $\mathbb{N}$. This is to say that $+$ and $\times$ are *binary operations* on $\mathbb{N}$. The natural numbers 0 and 1 have special roles in that

$$x + 0 = x \text{ for all } x \text{ in } \mathbb{N}; \qquad x \times 1 = x \text{ for all } x \text{ in } \mathbb{N}.$$

Definition 2 *A **binary operation** $*$ on a set S associates an element $x * y$ in S with each ordered pair (x, y) where x, y are in S. (Binary operations will be studied in further detail in the Groups and Group Actions course next term.)*

Further the set $\mathbb{N}$ has a natural ordering $\leqslant$. (As a mathematical object, $\leqslant$ is a *binary relation* on $\mathbb{N}$. Binary relations will be discussed in detail in the next chapter.)

Definition 3 *Let x, y be natural numbers. We write $x \leqslant y$ if there exists a natural number z such that $x + z = y$.*

Proposition 4 *Let x, y, z be natural numbers. Then*

(a) $x \leqslant x$.

(b) if $x \leqslant y$ and $y \leqslant x$ then $x = y$.

(c) if $x \leqslant y$ and $y \leqslant z$ then $x \leqslant z$.

(d) either $x \leqslant y$ or $y \leqslant x$ holds true.

Proof (a) This follows as 0 is a natural number and $x + 0 = x$.

(b) As $x \leqslant y$ then $x + a = y$ for some natural number a and similarly $y \leqslant x$ implies $y + b = x$ for some b. Then

$$x + (a + b) = (x + a) + b = y + b = x$$

and hence $a + b = 0$. This is only possible for natural numbers if $a = b = 0$ and so $x = y$.

(c) As $x \leqslant y$ and $y \leqslant z$ then $x + a = y$ and $y + b = z$ for some a, b. Then

$$z = y + b = (x + a) + b = x + (a + b)$$

and so $x \leqslant z$ as $a + b$ is a natural number.

(d) If $x \leqslant y$ then $y = x + z$ for a natural number z and we see that $z = y - x$ is a natural number. If it is not the case that $x \leqslant y$ then $y - x$ is consequently an integer but not a natural number. So $y - x$ is a negative integer. Then

$$-(y - x) = x - y$$

is a natural number (positive in fact) and

$$x = y + (x - y)$$

showing that $y \leqslant x$. $\square$

Remark 5 It's worth taking a moment to note what algebraic laws have been necessary in the proof of the above. We have certainly used the *associativity* of $+$, that is the rule that $x+(y+z) = (x+y+z)$. Is this something we need to assume as an *axiom*, or something we should be able to prove?

Below is a somewhat more rigorous definition of the natural numbers than Definition 1 and which leads more naturally to proofs. It is possible to examine in finer detail models for the natural numbers and those interested should consider taking Part B Set Theory in the third year.

For now we shall work with:

Definition 6 $\mathbb{N}$ *is the smallest set such that*

(i) $0 \in \mathbb{N}$

(ii) if $n \in \mathbb{N}$ *then* $n + 1 \in \mathbb{N}$.

This definition of the natural numbers ties in very readily with proofs by *induction.*

1.2 Induction

Mathematical statements can come in the form of a single proposition such as

$$3 < \pi \qquad \text{or} \qquad 0 < x < y \implies x^2 < y^2,$$

but often they come in a family of statements such as

A $\quad 2^x > 0$ for all real numbers x;

B $\quad n$ lines in the plane,no two parallel, no three concurrent,
divide the plane into $n(n+1)/2 + 1$ regions for $n = 1, 2, 3, \ldots$;

C $\quad \displaystyle\int_0^{\pi} \sin^{2n}\theta \, \mathrm{d}\theta = \frac{(2n)!}{(n!)^2}\frac{\pi}{2^{2n}}$ for $n = 0, 1, 2, 3, \ldots$;

D $\quad 2n$ can be written as the sum of two primes for all $n = 2, 3, 4, \ldots$.

Induction (or more precisely *mathematical induction*) is a particularly useful method of proof for dealing with families of statements, such as the last three statements above, which are indexed by the natural numbers, the integers or some subset of them. We shall prove statement B using induction (Example 7). Statements B and C can be approached with induction because, in each case, knowing that the nth statement is true helps enormously in showing that the $(n + 1)$th statement is true –

this is the crucial idea behind induction. Statement D, on the other hand, is a famous open problem known as *Goldbach's Conjecture.* If we let $D(n)$ be the statement that $2n$ can be written as the sum of two primes, then it is currently known that $D(n)$ is true for $n \leqslant 4 \times 10^{18}$. What makes statement D different from B and C, and more intractable to induction, is that in trying to verify $D(n+1)$ we can't generally make much use of knowledge of $D(n)$ and so we can't build towards a proof. For example, we can verify $D(19)$ and $D(20)$ by noting that

$$38 = 7 + 31 = 19 + 19 \quad \text{and} \quad 40 = 3 + 37 = 11 + 29 = 17 + 23.$$

Here, knowing that 38 can be written as a sum of two primes is no great help in verifying that 40 can be, as none of the primes we might use for the latter was previously used in splitting 38.

By way of an example, we shall prove statement B by induction before giving a formal definition of just what induction is.

Example 7 *Show that n lines in the plane, no two of which are parallel and no three meeting in a point, divide the plane into $n(n+1)/2+1$ regions.*

Solution

Proving $B(0)$: When we have no lines in the plane then clearly we have just one region, as expected from putting $n = 0$ into the formula $n(n+1)/2+1$.

Assuming $B(n)$ and proving $B(n+1)$: Suppose now that we have n such lines dividing the plane into $n(n+1)/2+1$ regions and we add an $(n+1)$th line. This extra line meets each of the previous n lines because, by assumption, it is parallel with none of them. Also, it meets each of these n lines in a distinct point, as we have assumed that no three lines are concurrent. These n points of intersection divide the new line into $n+1$ segments.

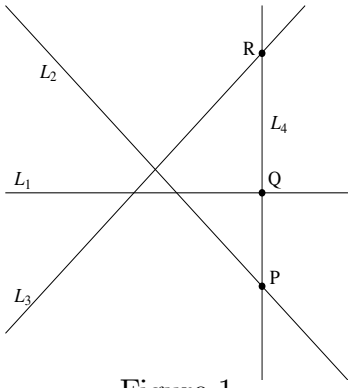


Figure 1

For each of these $n+1$ segments there are now two regions, one on either side of the segment, where previously there had been only one region. So by adding this $(n+1)$th line we have created $n+1$ new regions. For example, in the diagram on the right, the four segments, 'below P', PQ, QR and 'above R' on the fourth line L_4, divide what were four regions previously into eight new ones. In total, then, the number of regions we now have is

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

So the given formula is correct for the number of regions with $n+1$ lines; the result follows by induction. □

Definition 8 *The first statement to be proved ($B(0)$ in the above example) is known as the **initial case** or **initial step.** Showing the $(n+1)$th statement follows from the nth statement is called the **inductive step**, and the assumption that the nth statement is true is called the **inductive hypothesis**.*

Be sure that you understand Example 7: it contains the important steps common to any proof by induction.

- In particular, note in the final step that we have retrieved our original formula of $n(n+1)/2+1$, but with $n+1$ now replacing n everywhere; *this was the expression that we always had to be working towards!*

By induction we now know that B is true, i.e. that $B(n)$ is true for any $n \geqslant 1$. How does this work? Well, suppose we wanted to be sure $B(3)$ is correct – above we have just verified (amongst other things) the following three statements:

$$B(0) \text{ is true;} \qquad \text{if } B(0) \text{ is true then } B(1) \text{ is true;}$$
$$\text{if } B(1) \text{ is true then } B(2) \text{ is true;} \qquad \text{if } B(2) \text{ is true then } B(3) \text{ is true;}$$

and so putting the four statements together, we see that $B(3)$ is true. The first statement tells us that $B(0)$ is true and the next three are stepping stones, first to the truth about $B(1)$, on to $B(2)$ and then on to $B(3)$. A similar chain of logic can be made to show that any $B(n)$ is true.

Formally, then, the principle of induction is as follows:

Theorem 9 *(**The Principle of Induction**) Let $P(n)$ be a family of statements indexed by the natural numbers $n = 0, 1, 2, \ldots$. Suppose that*

- *(Initial Step) $P(0)$ is true;*
- *(Inductive Step) for any $n \geqslant 0$, if $P(n)$ is true then $P(n+1)$ is also true.*

Then $P(n)$ is true for all $n \geqslant 0$.

Proof Let S be the set of natural numbers such that $P(n)$ is true. Then $0 \in S$ as we know $P(0)$ is true. Further if $n \in S$ then $P(n)$ is true, so that $P(n+1)$ is true or equivalently $n+1 \in S$.

Thus S has the properties that (i) $0 \in S$ and (ii) if $n \in S$ then $n+1 \in S$. As $\mathbb{N}$ is the smallest such subset with these properties then $\mathbb{N}$ is contained in S. Hence $S = \mathbb{N}$. $\square$

It is not hard to see how we might amend the hypotheses of the theorem above to show:

Corollary 10 *Let N be an integer and let $P(n)$ be a family of statements for $n \geqslant N$. Suppose that*

- *(Initial Step) $P(N)$ is true;*
- *(Inductive Step) for any $n \geqslant N$, if $P(n)$ is true then $P(n+1)$ is also true.*

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

Proof The corollary follows by applying Theorem 9 to the statements $Q(n) = P(n+N)$, $n \geqslant 0$. $\square$

Here is another version of induction, which is usually referred to as the *strong form of induction*. In some problems, the inductive step might depend on some earlier case but not necessarily the immediately preceding case – such a case is Example 17.

Theorem 11 *(**Strong Form of Induction**) Let $P(n)$ be a family of statements for $n \geqslant 0$. Suppose that*

- *(Initial Step) $P(0)$ is true;*
- *(Inductive Step) for any $n \geqslant 0$, if $P(0), P(1), \ldots, P(n)$ are all true then so is $P(n+1)$.*

Then $P(n)$ is true for all $n \geqslant 0$.

Proof For $n \geqslant 0$, let $Q(n)$ be the statement '$P(k)$ is true for $0 \leqslant k \leqslant n$'. The assumptions of the above theorem are equivalent to: (i) $Q(0)$ (which is the same as $P(0)$) is true and (ii) if $Q(n)$ is true then $Q(n+1)$ is true. By induction (as stated in Theorem 9) we know that $Q(n)$ is true for all n. As $P(n)$ is a consequence of $Q(n)$, then $P(n)$ is true for all n. □

As a consequence of induction we can now show:

Proposition 12 *Every non-empty subset of the natural numbers has a minimal element.*

Proof Suppose, for a contradiction, that S is a subset of $\mathbb{N}$ with no minimal element and define

$$S^* = \{\text{natural numbers } n \text{ such that none of } 0, 1, \ldots, n \text{ is in } S\}.$$

We shall show that $S^* = \mathbb{N}$ and conclude that S is empty, a contradiction.

Note that 0 is in S^*. If not then 0 is in S and S has a minimal element (namely 0). Now suppose that n is in S^*. This means that none of $0, 1, \ldots, n$ is in S. It follows that $n+1$ is not in S, or else it would be the minimal element of S. Hence none of $0, 1, \ldots, n, n+1$ are in S or equivalently $n+1$ is in S^*. By induction $S^* = \mathbb{N}$ and so S is empty. □

Corollary 13 *A strictly decreasing sequence of natural numbers $x_1, x_2, x_3, \ldots$ is finite.*

Proof Consider the subset $\{x_1, x_2, x_3, \ldots\}$ of $\mathbb{N}$. This has a minimal element, say x_n. If x_n were not the last in the sequence then we have $x_n > x_{n+1}$, contradicting x_n being minimal. Hence the sequence is finite as it terminates with x_n. □

1.3 Examples

Our inductive definition of $\mathbb{N}$ allows us to define addition of natural numbers inductively.

Definition 14 *We define addition on $\mathbb{N}$ by*

(i) $x + 0 := x$ for all $x \in \mathbb{N}$.

(ii) $x + (n+1) := (x+n) + 1$.

Proposition 15 ***(Associativity)*** *$x + (y + z) = (x + y) + z$ for all $x, y, z \in \mathbb{N}$.*

Proof We shall prove this first for $z = 0$. In the case when $z = 0$, treating x and y as arbitrary natural numbers, we have

$$\text{LHS} = x + (y + 0) = x + y = (x + y) + 0 = \text{RHS},$$

from the previous definition. So if we assume the proposition is true for $z = n$ and all $x, y \in \mathbb{N}$ then

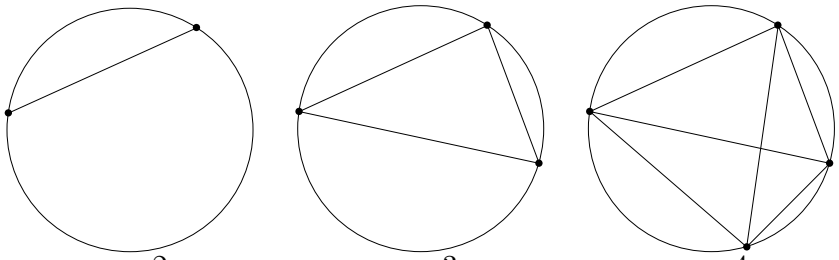
$$\begin{aligned} x + (y + (n+1)) &= x + ((y+n) + 1) && \text{[by definition]} \\ &= (x + (y+n)) + 1 && \text{[by definition]} \\ &= ((x+y) + n) + 1 && \text{[by hypothesis]} \\ &= (x+y) + (n+1) && \text{[by definition]} \end{aligned}$$

The result then follows by induction □

Proposition 16 ***(Commutativity)*** *$x + y = y + x$ for all $x, y \in \mathbb{N}$.*

Proof This is left as Sheet 1, Exercise 2.

To reinforce the need for proof, and to show how patterns can at first glance deceive us, consider the following example. Take two points on the circumference of a circle and take a line joining them; this line then divides the circle's interior into two regions. If we take three points on the perimeter then the lines joining them will divide the disc into four regions. Four points can result in a maximum of eight regions. Surely, then, we can confidently predict that n points will maximally result in 2^{n-1} regions.



$n = 2$ $n = 3$ $n = 4$

Further investigation shows our conjecture to be true for $n = 5$ but, to our surprise, when we take six points on the circle, the maximum number of regions attained is 31, no matter how we choose the points. Indeed the maximum number of regions attained from n points on the perimeter is given by the formula

$$\frac{1}{24}(n^4 - 6n^3 + 23n^2 - 18n + 24).$$

Our original guess was way out! This is known as *Moser's circle problem.*

Example 17 *Show that every integer $n \geqslant 1$ can be written as $n = 2^k l$ where k, l are natural numbers and l is odd.*

Solution We shall use the strong form of induction. Certainly $1 = 2^0 \times 1$ can be written in this way. Now say that $n \geqslant 2$ and every m in the range $1 \leqslant m < n$ can be written in the desired way. If n is odd then we may write $n = 2^0 \times n$ in the required format. If n is even then $n/2$ is a natural number in the range $1 \leqslant n/2 < n$ and so, by hypothesis, we may write $n/2 = 2^k l$ in the required format. Then $n = 2^{k+1} l$ is also expressed in the desired format. The result follows. □

Example 18 *Show for $n, k \geqslant 1$, that*

$$\sum_{r=1}^{n} r(r+1)(r+2)\cdots(r+k-1) = \frac{n(n+1)(n+2)\cdots(n+k)}{k+1}. \tag{1.1}$$

Remark 19 This problem differs from our earlier examples in that our family of statements now involves two variables n and k, rather than just the one variable. If we write $P(n, k)$ for the statement in equation (1.1) then we can use induction to prove all of the statements $P(n, k)$ in various ways:

- we could prove $P(1, 1)$ and show how $P(n + 1, k)$ and $P(n, k + 1)$ both follow from $P(n, k)$ for $n, k \geqslant 1$;
- we could prove $P(1, k)$ *for all* $k \geqslant 1$ and show knowing $P(n, k)$ *for all* k leads to the truth of $P(n + 1, k)$ *for all* k – this reduces the problem to one application of induction in n, but to a family of statements at a time;

- we could prove $P(n,1)$ *for all* $n \geqslant 1$ and show how knowing $P(n,k)$ *for all* n leads to proving $P(n,k+1)$ *for all* n – in a similar fashion to the previous method, now inducting through k and treating n as arbitrary.

What these different approaches rely on is that all the possible pairs (n,k) are somehow linked to our initial pair (or pairs). Let

$$S = \{(n,k) \colon n,k \geqslant 1\}$$

be the set of all possible pairs (n,k). The first method of proof uses the fact that the only subset T of S satisfying the properties

$$(1,1) \text{ is in } T, \qquad \text{if } (n,k) \text{ is in } T \text{ then } (n,k+1) \text{ is in } T, \qquad \text{if } (n,k) \text{ is in } T \text{ then } (n+1,k) \text{ is in } T,$$

is S itself. The second and third bullet points above rely on the fact that the whole of S is the only subset having similar properties. □

Solution (of Example 18) In this case the second method of proof seems easiest, that is we will prove that $P(1,k)$ holds for all $k \geqslant 1$ and show that assuming the statements $P(N,k)$, for a particular N and all k, is sufficient to prove the statements $P(N+1,k)$ for all k. Firstly we note

$$\text{LHS of } P(1,k) = 1 \times 2 \times \cdots \times k \qquad \text{and} \qquad \text{RHS of } P(1,k) = \frac{1 \times 2 \times \cdots \times (k+1)}{k+1} = 1 \times 2 \times \cdots \times k$$

are equal, proving $P(1,k)$ for all $k \geqslant 1$. Now if $P(N,k)$ holds true, for particular N and all $k \geqslant 1$, we have

$$\begin{aligned}
\text{LHS of } P(N+1,k) &= \sum_{r=1}^{N+1} r(r+1)(r+2)\cdots(r+k-1) \\
&= \frac{N(N+1)\ldots(N+k)}{k+1} + (N+1)(N+2)\cdots(N+k) \qquad \text{[by hypothesis]} \\
&= (N+1)(N+2)\cdots(N+k)\left(\frac{N}{k+1}+1\right) \\
&= \frac{(N+1)(N+2)\cdots(N+k)(N+k+1)}{k+1} \\
&= \text{RHS of } P(N+1,k),
\end{aligned}$$

proving $P(N+1,k)$ simultaneously for each k. This verifies all that is required for the second method. □

1.4 The Binomial Theorem

All of you will have met the identity

$$(x+y)^2 = x^2 + 2xy + y^2$$

and may have met identities like

$$(x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3.$$

It may even have been pointed out to you that these coefficients $1, 2, 1$ and $1, 3, 3, 1$ are simply the numbers that appear in **Pascal's triangle** and that more generally the nth row (counting from $n = 0$) contains the coefficients in the expansion of $(x+y)^n$. Pascal's triangle is the infinite triangle of numbers that has 1s down both edges and a number internal to some row of the triangle is calculated by adding the two numbers above it in the previous row. So the triangle grows as follows:

$$\begin{array}{lccccccccccc}
n=0 & & & & & & 1 & & & & & \\
n=1 & & & & & 1 & & 1 & & & & \\
n=2 & & & & 1 & & 2 & & 1 & & & \\
n=3 & & & 1 & & 3 & & 3 & & 1 & & \\
n=4 & & 1 & & 4 & & 6 & & 4 & & 1 & \\
n=5 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 \\
n=6 & 1 & & 6 & & 15 & & 20 & & 15 & & 6 \quad 1
\end{array}$$

From the triangle we could, say, read off the identity

$$(x+y)^6 = x^6 + 6x^5y + 15x^4y^2 + 20x^3y^3 + 15x^2y^4 + 6xy^5 + y^6.$$

Of course we haven't *proved* this identity yet! These identities, for general n, are the subject of the *binomial theorem*. We introduce now the binomial coefficients; their connection with Pascal's triangle will become clear soon.

Definition 20 *The (n,k)th **binomial coefficient** is the number*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \qquad \textit{where} \qquad 0 \leqslant k \leqslant n.$$

*$\binom{n}{k}$ is read as 'n **choose** k' and in some books is denoted as ${}^nC_k$. By convention $\binom{n}{k} = 0$ if $k > n \geqslant 0$ or $n \geqslant 0 > k$.*

- Note some basic identities concerning the binomial coefficients:

$$\binom{n}{k} = \binom{n}{n-k}; \qquad \binom{n}{0} = \binom{n}{n} = 1; \qquad \binom{n}{1} = \binom{n}{n-1} = n. \tag{1.2}$$

  The first identity reflects the fact that Pascal's triangle is left-right symmetrical, the second that the left and right edges are all 1s and the third that the next diagonals in from the edges progress $1, 2, 3, \ldots$.

The following lemma demonstrates that the binomial coefficients are precisely the numbers from Pascal's triangle.

Lemma 21 *Let $1 \leqslant k \leqslant n$. Then*

$$\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}.$$

Proof Putting the LHS over a common denominator we obtain

$$\begin{aligned}\frac{n!}{(k-1)!(n-k+1)!}+\frac{n!}{k!(n-k)!} &= \frac{n!\,\{k+(n-k+1)\}}{k!(n-k+1)!}\\ &= \frac{n!\times(n+1)}{k!(n-k+1)!}=\frac{(n+1)!}{k!(n+1-k)!}=\binom{n+1}{k}.\end{aligned}$$ □

Corollary 22 *The kth number in the nth row of Pascal's triangle is $\binom{n}{k}$ (remembering to count from $n=0$ and $k=0$). In particular, the binomial coefficients are whole numbers.*

Proof We shall prove this by induction. Note that $\binom{0}{0}=1$ gives the 1 at the apex of Pascal's triangle, proving the initial step. Suppose now that the numbers $\binom{n}{k}$, where $0\leqslant k\leqslant n$, are the numbers that appear in the nth row of Pascal's triangle. The first and last entries of the $(n+1)$th row (associated with $k=0$ and $k=n+1$) are

$$1=\binom{n+1}{0}\quad\text{and}\quad 1=\binom{n+1}{n+1}$$

as required. For $1\leqslant k\leqslant n$, then the kth entry on the $(n+1)$th row is formed by adding the $(k-1)$th and kth entries from the nth row. By the inductive hypothesis and Lemma 21 their sum is

$$\binom{n}{k-1}+\binom{n}{k}=\binom{n+1}{k},$$

verifying that the $(n+1)$th row also consists of the correct binomial coefficients. The result follows by induction. □

Finally, we come to the binomial theorem.

Theorem 23 ***(Binomial Theorem)*** *Let n be a natural number and x, y be real numbers. Then*

$$(x+y)^n=\sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k}.$$

Proof Let's check the binomial theorem first for $n=0$. We can verify this by noting

$$\text{LHS}=(x+y)^0=1;\qquad\qquad \text{RHS}=\binom{0}{0}x^0y^0=1.$$

For induction, we aim to show the theorem holds in the $(n+1)$th case assuming the nth case to be true. We have

$$\text{LHS}=(x+y)^{n+1}=(x+y)(x+y)^n=(x+y)\left(\sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k}\right)$$

writing in our assumed expression for $(x+y)^n$. Expanding the brackets gives

$$\sum_{k=0}^{n}\binom{n}{k}x^{k+1}y^{n-k}+\sum_{k=0}^{n}\binom{n}{k}x^k y^{n+1-k}=x^{n+1}+\sum_{k=0}^{n-1}\binom{n}{k}x^{k+1}y^{n-k}+\sum_{k=1}^{n}\binom{n}{k}x^k y^{n+1-k}+y^{n+1},$$

by taking out the last term from the first sum and the first term from the second sum. In the first sum we now make a change of variable; we set $k = l - 1$, noting that as k ranges over $0, 1, ..., n-1$ then l ranges over $1, 2, ..., n$. So the above equals

$$\begin{aligned} & x^{n+1} + \sum_{l=1}^{n} \binom{n}{l-1} x^l y^{n+1-l} + \sum_{k=1}^{n} \binom{n}{k} x^k y^{n+1-k} + y^{n+1} \\ = \; & x^{n+1} + \sum_{k=1}^{n} \left\{ \binom{n}{k-1} + \binom{n}{k} \right\} x^k y^{n+1-k} + y^{n+1} \\ = \; & x^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} x^k y^{n+1-k} + y^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} x^k y^{n+1-k} \end{aligned}$$

by Lemma 21. The final expression is the RHS of the binomial theorem in the $(n+1)$th case as required. □

Example 24 *Let n be a natural number. Show that*

$$\begin{aligned} &(a) \qquad \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n; \qquad (1.3) \\ &(b) \qquad \binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots = 2^{n-1}; \\ &(c) \qquad \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \cdots = 2^{n-1}. \end{aligned}$$

Note that the sums in (b) and (c) are not infinite as the binomial coefficients $\binom{n}{k}$ eventually become zero once $k > n$.

Solution From the binomial theorem we have

$$(1+x)^n = \binom{n}{0} + \binom{n}{1} x + \binom{n}{2} x^2 + \cdots + \binom{n}{n} x^n.$$

If we set $x = 1$ we demonstrate (1.3). If we set $x = -1$ then we have

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^n \binom{n}{n} = (1-1)^n = 0. \qquad (1.4)$$

Equation $\frac{1}{2}(1.3) + \frac{1}{2}(1.4)$ gives (b) and equation $\frac{1}{2}(1.3) - \frac{1}{2}(1.4)$ gives (c). □

Optional Further Exercises

(for possible tutorial discussion)

Exercise 1 *Prove **Bernoulli's inequality**: $(1+x)^n \geqslant 1 + nx$ for real $x \geqslant -1$ and integers $n \geqslant 1$.*

Exercise 2 *What is wrong with the following 'proof' that all people are of the same height?*

'Let $P(n)$ be the statement that n persons must be of the same height. Clearly $P(1)$ is true as a person is the same height as him/herself. Suppose now that $P(k)$ is true for some natural number k and we shall prove that $P(k+1)$ is also true. If we have $k+1$ people then we can invite one person to briefly leave so that k remain – as $P(k)$ is true we know that these people must all be equally tall. If we invite back the missing person and someone else leaves, then these k persons are also of the same height. Hence the $k+1$ persons were all of equal height and so $P(k+1)$ follows. By induction everyone is of the same height.'

Exercise 3 *Prove for $n \geqslant 1$ that*

$$\underbrace{\sqrt{2+\sqrt{2+\sqrt{2+\cdots+\sqrt{2}}}}}_{n \text{ root signs}} = 2\cos\frac{\pi}{2^{n+1}}.$$

Exercise 4 *Show, for $n \geqslant 1$, that*

$$\sum_{r=1}^{n}\frac{1}{r^2} \leqslant 2 - \frac{1}{n}.$$

Exercise 5 ***(AM-GM inequality)*** *Given n positive real numbers, $x_1, \ldots, x_n$ their* ***arithmetic mean*** *A and geometric mean G are defined by*

$$A = \frac{x_1 + x_2 + \cdots + x_n}{n}, \qquad G = \sqrt[n]{x_1 x_2 \cdots x_n}.$$

(i) Show directly for $n = 2$ that $A \geqslant G$ with equality if and only if $x_1 = x_2$.
(ii) Let $x_1, \ldots, x_{n+1}$ be $n+1$ positive numbers with arithmetic mean μ and assume that $x_n < \mu < x_{n+1}$. Set

$$X_1 = x_n + x_{n+1} - \mu, \qquad X_2 = \mu.$$

Show that $X_1 X_2 > x_n x_{n+1}$ and that the numbers $x_1, x_2, \ldots, x_{n-1}, X_1$ have arithmetic mean μ. Deduce that $A_n \geqslant G_n$ for all n with equality if and only if all the x_i are equal.

Exercise 6 *Use the identity $(1+x)^{2n} = (1+x)^n(1+x)^n$ to show that $\sum_{k=0}^{n}\binom{n}{k}^2 = \binom{2n}{n}$.*

Exercise 7 *Let n be a natural number. Show that*

$$\binom{n}{0} - \binom{n}{2} + \binom{n}{4} - \binom{n}{6} + \cdots = 2^{n/2}\cos\frac{n\pi}{4}.$$

What is the value of $\binom{n}{1} - \binom{n}{3} + \binom{n}{5} - \binom{n}{7} + \cdots$?

Exercise 8 *Let F_n denote the nth Fibonacci number. Use induction to prove Binet's formula*

$$F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}$$

where $\alpha = (1+\sqrt{5})/2$ and $\beta = (1-\sqrt{5})/2$. Deduce the value of

$$\sum_{n=0}^{\infty} F_n x^n,$$

where $x \in \mathbb{R}$. For what values of x does this series converge?

2. ELEMENTS OF SET THEORY AND LOGIC

2.1 Sets: Definitions and Notation

Sets are amongst the most primitive objects in mathematics, so primitive in fact that it is somewhat difficult to give a precise definition of what one means by a set – i.e a definition which uses words with entirely unambiguous meanings. For example, here is a description due to Cantor:

By an "aggregate" [set] we are to understand any collection into a whole M of definite and separate objects m of our intuition or our thought. These objects we call the "elements" of M.

One might now ask exactly what one means by a "collection" or by "objects", but the point is that we all know intuitively what Cantor is talking about. Cantor's "aggregate" is what we call a set.

Notation 25 (a) Let S be a set. We then write $x \in S$ to denote that x is an **element** of S. That is one of the "objects" in S. And we write $x \notin S$ to denote that x is not an element of S.

(b) Let S and T be sets. We write $T \subseteq S$ to denote that whenever $x \in T$ then $x \in S$. That is, every element of T is an element of S. In this case T is said to be a **subset** of S.

(c) The symbol $\subseteq$ is also read as "is contained in". Note that the symbol $\subset$ typically means the same and not "is contained in but not equal to", as you might suspect.

At the same time, too liberal an understanding of what a "collection" means can lead to famous paradoxes.

Remark 26 (**Russell's Paradox**) Let

$$H = \{\text{sets } S : S \notin S\}.$$

That is, H is the collection of sets S which are not elements of themselves. This, at first glance, is an odd choice of set to consider but also currently seems a perfectly valid set for our consideration. Most sets that we can think of seem to be in H. For example, $\mathbb{N}$ is in H, as the elements of $\mathbb{N}$ are single natural numbers, and no element is the set $\mathbb{N}$ itself. The problem arises when we ask the question: is $H \in H$?

There are two possibilities: either $H \in H$ or $H \notin H$. On the one hand, if $H \notin H$ then H meets the precise criterion for being in H and so $H \in H$. On the other hand, if $H \in H$ then $H \notin H$ is false, and so H does not meet the criterion for being in H and hence $H \notin H$. $\square$

So we have a contradiction either way. A modern take on Russell's Paradox is that the set H is inherently self-contradictory. It would be akin to starting a proof with "let x be the smallest positive real number" or "let n be that largest natural number". There are no such numbers, so it is not surprising that contradictory or nonsensical proofs might result from such a beginning. A more modern take on sets are the **ZF axioms**, so-named after the mathematicians Zermelo and Fraenkel, who gave a set of axioms for how a set might be constructed – for example by taking unions or

intersections of axiomatically assumed sets. Russell's set is not constructible via the ZF axioms and so simply would not be considered a set. There is likewise no "set of all sets".

Full details of these axioms are given in the Part B Set Theory course. Constructing the natural numbers and showing all of their properties given only the most primitive notion of a set is itself interesting, but also quite laborious. Having understood what one means by sets and natural numbers, we can precisely define other basic objects in mathematics such as the integers, rational numbers and real numbers. For now we will continue with our somewhat naive (and unadventurous) approach of what a collection might be, and leave esoteric specifics to another day.

Example 27 *Let* $A = \{1, 2, 3\}$. *There are three elements of* A *namely* $1, 2$ *and* 3. *There are* 8 *subsets of* A *namely*

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

where the last symbol $\varnothing$ *denotes the* ***empty set****, the set with no elements. Note that the order in which a set's elements are listed is unimportant so that* $\{1, 2, 3\} = \{1, 3, 2\}$ *for example.*

Definition 28 *Give a set* A *its* ***power set****, denoted* $\mathcal{P}(A)$*, is the set of all subsets of* A.

Example 29 *With* $A = \{1, 2, 3\}$ *again then*

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

Note that $1 \in A$, *that* $1 \notin \mathcal{P}(A)$, *but that* $\{1\} \in \mathcal{P}(A)$, *the last being equivalent to writing* $\{1\} \subseteq A$. *That is* 1 *is an element of* A *but the* $\{1\}$ *is a subset of* A.

We have all already met certain important mathematical sets, though the following notation may well be new to you.

Definition 30 *(a) We denote the set of* ***natural numbers*** *as* $\mathbb{N}$. *That is the set of non-negative whole numbers*

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

(b) The set of ***integers****, that is the set of whole numbers, is denoted* $\mathbb{Z}$. *The letter zed arises from the German word "zahlen" for "numbers". So*

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

(c) The set of ***rational numbers*** *(or just simply* ***rationals****) is denoted* $\mathbb{Q}$. *This is the set comprising all fractions where the numerator and denominator are both integers. So*

$$\mathbb{Q} = \left\{\frac{m}{n} : m, n \in \mathbb{Z}, n > 0\right\}.$$

(d) The set of real numbers $\mathbb{R}$ *will be formally introduced in Analysis I. For now we simply state that the* ***real numbers*** *are those numbers with a decimal expansion. This includes the rational numbers but also includes irrational numbers such as* $\sqrt{2}$ *and* π.

(e) The set of ***complex numbers*** *is the set of numbers*

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

where $i = \sqrt{-1}$.

(f) Given real numbers a, b with $a < b$ then we define the following bounded ***intervals***

$$\begin{aligned}(a,b) &= \{x \in \mathbb{R} : a < x < b\}\,; \qquad (a,b] = \{x \in \mathbb{R} : a < x \leqslant b\}\,;\\ [a,b) &= \{x \in \mathbb{R} : a \leqslant x < b\}\,; \qquad [a,b] = \{x \in \mathbb{R} : a \leqslant x \leqslant b\}\,,\end{aligned}$$

and the unbounded intervals

$$\begin{aligned}(a,\infty) &= \{x \in \mathbb{R} : a < x\}\,; \qquad [a,\infty) = \{x \in \mathbb{R} : a \leqslant x\}\,;\\ (-\infty,a) &= \{x \in \mathbb{R} : x < a\}\,; \qquad (-\infty,a] = \{x \in \mathbb{R} : x \leqslant a\}\,.\end{aligned}$$

Example 31 *Note*

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}.$$

Definition 32 *Given subsets A and B of a set S then:*
(a) the ***union*** *$A \cup B$ of A and B is the subset consisting of those elements that are in A or B (or both), that is:*

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

(b) the ***intersection*** *$A \cap B$ of A and B is the subset consisting of those elements that are in both A and B, that is:*

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

(c) the ***complement*** *of B, written B^c or B', is the subset consisting of those elements that are not in A, that is:*

$$A^c = \{x \in S : x \notin A\}.$$

(d) the ***complement of*** *B* ***in*** *A, written $A\backslash B$, or sometimes $A - B$, is the subset consisting of those elements that are in A and not in B, that is:*

$$A\backslash B = \{x \in A : x \notin B\} = A \cap B^c.$$

Note that $B^c = S\backslash B$.
(e) A and B are said to be ***disjoint*** *if $A \cap B = \varnothing$, that is the two subsets have no element in common.*

Example 33 *Let $S = \mathbb{Z}$.*

(a) With $A = \{0, 1, 2, \ldots\}$ and $B = \{0, -1, -2, -3, \ldots\}$ we have

$$A \cup B = \mathbb{Z}; \qquad A \cap B = \{0\}; \qquad A^c = \{-1, -2, -3, \ldots\} = B\backslash A.$$

(b) With $A = \{$even integers$\}$ and $B = \{$odd integers$\}$ then

$$A \cup B = \mathbb{Z}; \qquad A \cap B = \varnothing; \qquad A^c = B = B\backslash A.$$

Definition 34 *Let S and T be sets. Their* ***Cartesian product*** *$S \times T$ is the set of all ordered pairs (s, t) where $s \in S$ and $t \in T$. Note that – as the name suggests – order matters in an ordered pair. So $(1, 2) \neq (2, 1)$ whilst $\{1, 2\} = \{2, 1\}$ as sets.*

Definition 35 *If $n \geqslant 1$ then we write S^n for all ordered n-tuples, that is vectors of the form $(s_1, s_2, \ldots, s_n)$ where $s_i \in S$ for all i.*

Example 36 *Let $A, B \subseteq S$ and $C, D \subseteq T$. Then*

$$(A \times C) \cap (B \times D) = (A \cap B) \times (C \cap D).$$

To appreciate this, (s,t) is in the LHS and RHS if the four conditions $s \in A$, $t \in C$, $s \in B$, $t \in D$ all need to apply.

Example 37 *Note that $(A \times B)^c \neq A^c \times B^c$ in general. For example if $S = \{0,1\} = T$ and $A = \{0\} = B$ then*

$$(A \times B)^c = \{(0,1),(1,0),(1,1)\}, \qquad A^c \times B^c = \{(1,1\}\}.$$

We can use Cartesian products to define the notion of *disjoint unions*. If we take the union $A \cup B$ of two sets A and B, then any element that is in both A and B appears just once in the union. We might wish to keep some sense of an element being in both sets and retain a sense in the union of the x that came from A that is distinct from the notion of the x that came from B.

Definition 38 ***(Disjoint Union)*** *Let A and B be sets. Their disjoint union $A \sqcup B$ is defined to be*

$$A \times \{0\} \cup B \times \{1\}.$$

The set A is now identified with $A \times \{0\}$ and B with $B \times \{1\}$ and any element x that is in both A and B appears twice in the disjoint union as $(x,0)$ and $(x,1)$.

2.2 Sets: Logic and Proof

We now need to introduce some logical notation and language to help with our proofs of set identities.

Notation 39 Let P and Q denote logical statements – such as '$x \geqslant y$' or 'for all $a \in \mathbb{R}$, $a^2 \geqslant 0$'.

(a) $P \Rightarrow Q$

This reads "P **implies** Q". This means that whenever the statement P is true then the statement Q is true. This implication may be strict, meaning that it may be possible for Q to be true and P false. For example $x \geqslant 4 \Rightarrow x \geqslant 2$ but $4 > 3 \geqslant 2$ shows that the implication is strict.

We say that P is **sufficient** for Q and the Q is **necessary** for P. The statement $P \Rightarrow Q$ may also be read as "if P then Q", "Q if P" and, occasionally, "P only if Q".

$P \Rightarrow Q$ can also be written as $Q \Leftarrow P$.

(b) $P \Leftrightarrow Q$

This reads as "P **if and only if** Q", which is sometimes contracted to "P **iff** Q". This means that whenever the statement P is true then the statement Q and vice versa. So P is true precisely when Q is true, or equally P is **necessary and sufficient** for Q.

Note that the context of the statement is an important part of its truth or falsity. So in $\mathbb{R}$ the statement $x > 2 \Leftrightarrow x^2 > 4$ is false – with $x = -3$ being a counter-example – but the statement is true in $\mathbb{N}$.

(c) We write $P \wedge Q$ for the statement "P **and** Q" which holds when both P and Q are true.

(d) We write $P \vee Q$ for the statement "P **or** Q" which holds when either P or Q (or both) is true. So note this is not an "exclusive or".

(e) We write $\neg P$ for "**not** P" or the "**negation** of P". This is the statement that is true precisely when P is false, and vice versa.

(f) The symbol $\forall$ denotes "for all". So for example $\forall x \in \mathbb{R} \quad x^2 \geqslant 0$ is true. This use of "for all" means that we have a family of statements, one for each $x \in \mathbb{R}$. It is good practice to make clear what set is being varied over – for example $\forall x \in \mathbb{C} \quad x^2 \geqslant 0$ is false, with $x = i$ being a counter-example.

(g) The symbol $\exists$ denotes "there exists". So for example $\exists x \in \mathbb{R} \quad x^2 < 0$ is false, because no such real x exists. But again $\exists x \in \mathbb{C} \quad x^2 < 0$ is true and noting $i^2 = -1 < 0$ is enough to prove it.

(h) The symbols $\forall$ and $\exists$ are called **quantifiers** and respectively are sometimes referred to as the **universal quantifier** and the **existential quantifier**.

We shall see later that there are important equivalences between set-theoretic and logical identities. For now note that inclusion $A \subseteq B$ can be rewritten as

$$x \in A \quad \Rightarrow \quad x \in B,$$

which plays an important part in the following.

Proposition 40 ***(Double Inclusion)*** *Let A and B be two subsets of a set S. Then $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.*

Proof A and B are equal if they contain precisely the same elements. Hence we have

$$\begin{array}{lll} A = B & \Leftrightarrow & \forall s \in S \quad (s \in A \Leftrightarrow s \in B) \\ & \Leftrightarrow & \forall s \in S \quad (s \in A \Rightarrow s \in B \quad \wedge \quad s \in B \Rightarrow s \in A) \\ & \Leftrightarrow & (\forall s \in S \quad s \in A \Rightarrow s \in B) \wedge (\forall s \in S \quad s \in B \Rightarrow s \in A) \\ & \Leftrightarrow & A \subseteq B \quad \wedge \quad B \subseteq A. \end{array}$$

□

Proposition 41 ***(Distributive Laws)*** *Let A, B, C be subsets of a set S. Then*

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

and

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

Proof Suppose $x \in A \cup (B \cap C)$. This means that $x \in A$ or $x \in B \cap C$. From the definition of union this leads to a case by case analysis. If x is in A then we have $x \in A \cup B$ *and* $x \in A \cup C$. So x is in the RHS.

Conversely suppose that $x \in (A \cup B) \cap (A \cup C)$. So $x \in A \cup B$ and $x \in (A \cup C)$. Now we have four cases:

(i) $x \in A$ and $x \in A$ which imply $x \in A \subseteq A \cup (B \cap C)$;

(ii) $x \in A$ and $x \in C$ which imply $x \in A \subseteq A \cup (B \cap C)$;

(iii) $x \in B$ and $x \in A$ which imply $x \in A \subseteq A \cup (B \cap C)$;

(iv) $x \in B$ and $x \in C$ which imply $x \in B \cap C \subseteq A \cup (B \cap C)$.

Thus we've shown LHS $\subseteq$ RHS and RHS $\subseteq$ LHS both and the sets are equal.

The second equation is left as Sheet 1, Exercise 4(i). □

Remark 42 (**Logical equivalents of set-theoretic identities**) In a very natural way 'union', 'intersection' and 'complement' for sets correspond to 'or', 'and' and 'not' for logical statements. To

any subset $P \subseteq S$ we can associate the logical statement $P(x)$ which is true precisely when $x \in P$. The logical statements equivalent to

$$P \cup Q, \qquad P \cap Q, \qquad P^c,$$

are

$$P(x) \vee Q(x), \qquad P(x) \cap Q(x), \qquad \neg P(x).$$

And the logical equivalent of the previous distributive laws are

$$\begin{aligned} P \vee (Q \wedge R) &= (P \vee Q) \wedge (P \vee R), \\ P \wedge (Q \vee R) &= (P \wedge Q) \vee (P \wedge R). \end{aligned}$$

Remark 43 The identity $a(b+c) = ab + ac$ for real numbers is called the distributive law, and we say that multiplication "distributes" across addition. On the other hand addition doesn't distribute across multiplication as the identity $a + bc = (a+b)(a+c)$ is untrue. Above we have shown that $\cap$ distributes across $\cup$ and $\cup$ distributes across $\cap$.

Example 44 *Let A, B, C be subsets of a set S. Show that*

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

Solution The previous distributive laws help here so that we don't need to make a double-inclusion argument

$$\begin{aligned} \text{RHS} &= [(A \cup B) \cap (B \cup C)] \cap (C \cup A) \\ &= [[(A \cup B) \cap B] \cup [(A \cup B) \cap C]] \cap (C \cup A) \quad \text{[second law]} \\ &= [B \cup [(A \cup B) \cap C]] \cap (C \cup A) \quad \text{[simplification]} \\ &= [B \cup (A \cap C) \cup (B \cap C)] \cap (C \cup A) \quad \text{[second law]} \\ &= [B \cup (A \cap C)] \cap (C \cup A) \quad \text{[simplification]} \\ &= [B \cap (C \cup A)] \cup [(A \cap C) \cap (C \cup A)] \quad \text{[second law]} \\ &= [(B \cap C) \cup (A \cap B)] \cup [(A \cap C)] \quad \text{[simplification]} \\ &= \text{LHS} \qquad \square \end{aligned}$$

Example 45 *Let A be a subset of a set S and B, C be subsets of a set T. Then*

$$\begin{aligned} A \times (B \cup C) &= (A \times B) \cup (A \times C)\,. \\ A \times (B \cap C) &= (A \times B) \cap (A \times C)\,. \end{aligned}$$

Solution To prove the first equality we note

$$\begin{aligned} (s,t) \in \text{LHS} \quad &\Leftrightarrow \quad s \in A \wedge (t \in B \cup C) \\ &\Leftrightarrow \quad s \in A \wedge (t \in B \vee t \in C) \\ &\Leftrightarrow \quad (s \in A \wedge t \in B) \vee (s \in A \wedge t \in C) \\ &\Leftrightarrow \quad ((s,t) \in A \times B) \vee ((s,t) \in A \times C) \\ &\Leftrightarrow \quad (s,t) \in (A \times B) \cup (A \times C) \\ &\Leftrightarrow \quad (s,t) \in \text{RHS}. \end{aligned}$$

The second equality follows similarly. $\square$

Example 46 ***(Order matters)*** 

$$\bigcup_{m=1}^{2}\bigcap_{n=1}^{2} A_{m,n} = \bigcup_{m=1}^{2}(A_{m,1}\cap A_{m,2}) = (A\cap B)\cup(C\cap D)$$
$$\bigcap_{n=1}^{2}\bigcup_{m=1}^{2} A_{m,n} = \bigcap_{n=1}^{2}(A_{1,n}\cup A_{2,n}) = (A\cup C)\cap(B\cup D)$$

For $1\leqslant m,n\leqslant 2$ *let*

$$A_{m,n} = \begin{cases} \{1,2\} & (m,n)=(1,1)\\ \{3,4\} & (m,n)=(1,2)\\ \{2,4\} & (m,n)=(2,1)\\ \{1,3\} & (m,n)=(2,2)\end{cases}$$

Then

$$\bigcup_{m=1}^{2}\bigcap_{n=1}^{2} A_{m,n} = \bigcup_{m=1}^{2}(A_{m,1}\cap A_{m,2}) = \varnothing\cup\varnothing = \varnothing;$$
$$\bigcap_{n=1}^{2}\bigcup_{m=1}^{2} A_{m,n} = \bigcap_{n=1}^{2}(A_{1,n}\cup A_{2,n}) = \{1,2,4\}\cap\{1,3,4\} = \{1,3\}$$

In general it's the case that

$$\bigcup_{m}\bigcap_{n} A_{m,n} \subseteq \bigcap_{n}\bigcup_{m} A_{m,n}$$

but equality will not generally hold. □

In a similar manner the order of quantifiers can make an enormous difference to seemingly similar statements. For example, with

$$\exists x \in S \quad \forall y\in T \quad P(x,y)$$
$$\forall y \in T \quad \exists x\in S \quad P(x,y)$$

the first statement is *much* stronger than the second. Take care! The following example is chosen to show how different such superficially similarly statements actually are.

Example 47 *Let* S *be the set of capital cities and* T *be the set of countries. Let* $P(x,y)$ *be the statement "*x *is the capital of* y*".*

The statement

$$\forall y\in T \quad \exists x\in S \quad P(x,y)$$

is then true – it says every country has a capital city (and it doesn't really matter that some countries have arguably more than one capital). Importantly here the x *is permitted to depend on the* y *as the quantifier comes second. So for* $y =$ *Denmark there exists* $x =$ *Copenhagen and for* $y =$ *Botswana there exists* $x =$ *Gaborone.*

However the statement

$$\exists x\in S \quad \forall y\in T \quad P(x,y)$$

is far from true. This time the existential quantifier comes first and this single capital city x *is required to be the capital of all countries – there is clearly no such city.*

2.3 Truth Tables

An alternative approach to proving set-theoretic and logical identities is via **truth tables**. These provide a systematic means of treating all the different cases that arise. There may be different numbers of cases to consider depending on the number of sets involved in an identity. So the truth table for the intersection of two sets involves four cases as an element may independently be in each of the two sets or not.

Below are listed the truth tables for $A \cap B$, $A \cup B$, A^c, $A \backslash B$ and $A \Delta B$, the last denoting symmetric difference – to be in $A \Delta B$ an element needs to be in precisely one of A or B.

A	B	$A \cap B$
F	F	F
F	T	F
T	F	F
T	T	T

A	B	$A \cup B$
F	F	F
F	T	T
T	F	T
T	T	T

A	A^c
F	T
T	F

A	B	$A \backslash B$
F	F	F
F	T	F
T	F	T
T	T	F

A	B	$A \Delta B$
F	F	F
F	T	T
T	F	T
T	T	F

An alternative approach to demonstrating the distributive law

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

can then be made via these truth tables using a case by case analysis. For example, if an element x is in A and C, but not in B, then we have enough information to determine whether x is in the LHS/RHS. In all there would be eight cases to check (three independent choices of whether an element is in each of A, B, C) and these are listed below. The case just described is the sixth case below. As the LHS column and RHS column read identically then we do indeed have proved the identity true in all cases.

A	B	C	$B \cap C$	LHS	$A \cup B$	$A \cup C$	RHS
N	N	N	N	N	N	N	N
N	N	Y	N	N	N	Y	N
N	Y	N	N	N	Y	N	N
N	Y	Y	Y	Y	Y	Y	Y
Y	N	N	N	Y	Y	Y	Y
Y	N	Y	N	Y	Y	Y	Y
Y	Y	N	N	Y	Y	Y	Y
Y	Y	Y	Y	Y	Y	Y	Y

There are similarly truth tables for logical statements. If P and Q are now logical statements then below are the truth tables for $P \wedge Q$, $P \vee Q$, $\neg P$ and $P \Rightarrow Q$.

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

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

P	$\neg P$
F	T
T	F

P	Q	$P \Rightarrow Q$
F	F	T
F	T	T
T	F	F
T	T	T

The last truth table for $P \Rightarrow Q$ may take a little getting used to. It's also not hard to see that this is the same truth table as $(\neg A) \vee B$ as it is false only when $\neg P$ and Q are both false.

To help us understand why this is the case, consider how we prove $P \Rightarrow Q$ using *proof by contradiction*. In this case we assume that Q is false, whilst still assuming the hypotheses P to be true, and arrive at a contradiction. That is we show $P \wedge (\neg Q)$ to be false – or more succinctly we prove

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

For $P \wedge (\neg Q)$ to be true then both P and $\neg Q$ must be true. So for $P \wedge (\neg Q)$ to be false, only one of P and $\neg Q$ need be false. That is.

$$\neg(P \wedge (\neg Q)) \quad \Leftrightarrow \quad (\neg P) \vee (\neg(\neg Q)) \quad \Leftrightarrow \quad (\neg P) \vee Q.$$

(We have just demonstrated one of De Morgan's rules. More on this in the next section.) We can also see that the following truth tables are the same: that of $P \Rightarrow Q$ and that of $\neg Q \Rightarrow \neg P$.

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
T	T	T
F	F	T

P	Q	$\neg Q \Rightarrow \neg P$
T	T	T
T	F	F
T	T	T
F	F	T

The statement $\neg Q \Rightarrow \neg P$ is known as the **contrapositive** of $P \Rightarrow Q$ and the two statements are equivalent.

2.4 De Morgan's Laws

Augustus De Morgan was the first president of the London Mathematical Society. Beyond this, he is mainly remembered for the following two set-theoretic laws (and their logical equivalents).

Theorem 48 *(**De Morgan's Laws** – **finite version**) Let $A_1, \ldots, A_n$ be a family of subsets of a set S. Then*

$$\left(\bigcap_{k=1}^{n} A_k\right)^c = \bigcup_{k=1}^{n} A_k^c$$

and

$$\left(\bigcup_{k=1}^{n} A_k\right)^c = \bigcap_{k=1}^{n} A_k^c.$$

Proof We will prove the first identity with $n = 2$ using a truth table.

A_1	A_2	$A_1 \cap A_2$	LHS	A_1^c	A_2^c	RHS
N	N	N	Y	Y	Y	Y
N	Y	N	Y	Y	N	Y
Y	N	N	Y	N	Y	Y
Y	Y	Y	N	N	N	N

We can then prove the general result by induction. Suppose that the first De Morgan law holds true for n subsets. Then

$$\left(\bigcap_{k=1}^{n+1} A_k\right)^c = \left(\bigcap_{k=1}^{n} A_k \cap A_{n+1}\right)^c = \left(\bigcap_{k=1}^{n} A_k\right)^c \cup A_{n+1}^c = \bigcup_{k=1}^{n+1} A_k^c.$$

So the result follows by induction.

To see the second inequality now we can use the first law and note

$$\bigcap_{k=1}^{n} A_k^c = \left(\bigcap_{k=1}^{n} A_k^c\right)^{cc} = \left(\bigcup_{k=1}^{n} A_k^{cc}\right)^c = \left(\bigcup_{k=1}^{n} A_k\right)^c. \qquad \square$$

As before De Morgan's Laws have logical equivalents. These are

$$\begin{aligned} \neg(P \wedge Q) &\Leftrightarrow (\neg P) \vee (\neg Q); \\ \neg(P \vee Q) &\Leftrightarrow (\neg P) \wedge (\neg Q). \end{aligned}$$

These may be more intuitive equivalents of De Morgan's law. The first says that 'P and Q' will be false if either P or Q is false or, put another way, it is sufficient to prove that P and Q aren't both true by showing that either one is false. In the second $P \vee Q$ is true is either of P, Q holds, so for this to fail then both P and Q must be false.

Example 49 *Let $A, B \subseteq S$ and $C, D \subseteq T$. Then*

$$(A \times B)^c = (A^c \times T) \cup (S^c \times B).$$

Solution

$$\begin{aligned} (s,t) \in (A \times B)^c &\Leftrightarrow \neg((s,t) \in A \times B) \\ &\Leftrightarrow \neg(s \in A \wedge t \in B) \\ &\Leftrightarrow \neg(s \in A) \vee \neg(t \in B) \\ &\Leftrightarrow s \in A^c \vee t \in B^c \\ &\Leftrightarrow (s,t) \in A^c \times B^c. \qquad \square \end{aligned}$$

More generally for *arbitrary* unions and intersections, the quantifiers $\forall$ and $\exists$ make explicit, logically, what it means for an element to be in such intersections and unions. Above we consider finite unions and intersections. It's not hard to imagine that we might have infinitely many sets $A_0, A_1, A_2, \ldots$ and wish to consider the intersection and union

$$\bigcap_{n=0}^{\infty} A_n, \qquad \bigcup_{n=0}^{\infty} A_n.$$

To be in the intersection requires being in *every* A_n and to be in the union means being in *some* A_n. In these examples the sets A_n and *indexed* using $n \in \mathbb{N}$ and $\mathbb{N}$ is called the **indexing set**. We might generalize this to the case where we have sets $\{A_i : i \in I\}$, with I now being the indexing set, where I could be yet "larger" sets than $\mathbb{N}$ such as $\mathbb{R}$.

Hence we define the arbitrary intersection and arbitrary union by

$$x \in \bigcap_{i \in I} A_i \quad \Leftrightarrow \quad \forall i \in I \quad x \in A_i;$$
$$x \in \bigcup_{n=0}^{\infty} A_n \quad \Leftrightarrow \quad \exists i \in I \quad x \in A_i.$$

So if we are to have versions of De Morgan's laws that apply to arbitrary intersections and unions we need to be able to negative statements involving these quantifiers. Note we have

Proposition 50 ***(De Morgan's Laws – logical version)*** *Let $P(x)$ be a family of statements, indexed by the elements x of some set S. Then*

$$\neg\,(\forall x \in S \quad P(x)) \quad \Leftrightarrow \quad \exists x \in S \quad \neg P(x);$$
$$\neg\,(\exists x \in S \quad P(x)) \quad \Leftrightarrow \quad \forall x \in S \quad \neg P(x).$$

Proof For $\forall x \in S \quad P(x)$ to be true it is the case that $P(x)$ is universally true on the set S. For this not to be the case means that only one counter-example $x \in S$ needs to be exist where $\neg P(x)$ holds.

The second law follows from the first. If we replace $P(x)$ with $\neg P(x)$ we have

$$\neg\,(\forall x \in S \quad \neg P(x)) \quad \Leftrightarrow \quad \exists x \in S \quad P(x),$$

and if we negative both sides we arrive at the second law. □

Remark 51 You should make sure you are comfortable with these logical versions of De Morgan's laws. One says that for $P(x)$ not to be universally true means there is some counter-example. The second says that for $P(x)$ to be nowhere true means that it is everywhere false.

So far that might seem reasonably clear and intuitive. But, as we will see, logical statements in mathematics can become quite complicated, with many important statements including four quantifiers. The careful negation of such statements – for example if you wish to prove a result by contradiction – needs due attention.

Remark 52 (**Vacuously true statements**) Whatever the statement $P(x)$, the statement

$$\exists x \in \varnothing \quad P(x)$$

is untrue as no such x exists. This means it's negation

$$\neg(\exists x \in \varnothing \quad P(x)) \quad \Leftrightarrow \quad \forall x \in \varnothing \quad \neg P(x)$$

is always true, no matter what P (or its negation) is. We say a statement of the form

$$\forall x \in \varnothing \quad P(x)$$

is **vacuously true**. Essentially as $\varnothing$ there is no x for which the statement needs verifying, and so the statement is true.

Corollary 53 ***(De Morgan's Laws – arbitrary set-theoretic version)*** *Let S be a set and for each $i \in I$ let $A_i \subseteq S$. Then*

$$\left(\bigcap_{i\in I} A_i\right)^c = \bigcup_{i\in I} A_i^c.$$
$$\left(\bigcup_{i\in I} A_i\right)^c = \bigcap_{i\in I} A_i^c.$$

Proof We have

$$\begin{aligned} x \in \left(\bigcap_{i\in I} A_i\right)^c \quad &\Leftrightarrow \quad \neg\left(x \in \bigcap_{i\in I} A_i\right) \\ &\Leftrightarrow \quad \neg\left(\forall i \in I \quad x \in A_i\right) \\ &\Leftrightarrow \quad \exists i \in I \quad \neg(x \in A_i) \\ &\Leftrightarrow \quad \exists i \in I \quad x \in A_i^c \\ &\Leftrightarrow \quad x \in \bigcup_{i\in I} A_i^c. \end{aligned}$$

We can prove the second law in a similar way or alternatively set $B_i = A_i^c$ so that

$$x \in \left(\bigcup_{i\in I} B_i\right)^c \quad \Leftrightarrow \quad \neg\left(x \in \bigcup_{i\in I} A_i^c\right) \quad \Leftrightarrow \quad x \in \left(\bigcap_{i\in I} A_i\right) \quad \Leftrightarrow \quad x \in \bigcap_{i\in I} B_i^c.$$

□

2.5 Binary Relations. Equivalence Relations

Binary relations, (which we'll usually just refer to them simply as *relations*), are common in mathematics and everyday life, and include the following examples.

- The relation $\leqslant$, meaning "less than or equal to", which compares pairs of real numbers.
- The relation $|$, meaning "divides" or "is a factor of", which compares pairs of positive integers.
- The relation $\subseteq$, meaning "is a subset of", which compares subsets of a set.
- The relation $\leqslant$, meaning "is less than or equal to at all points", which compares pairs of functions from $\mathbb{R}$ to $\mathbb{R}$.
- The relation "is at the same height above sea level", which compares points on the earth's surface.

Formally a binary relation is defined as:

Definition 54 *A **binary relation** (or simply **relation**) R on a set S is a subset of $S \times S$. If $(s,t) \in R$ (where $s,t \in S$) then we write sRt.*

You might reasonably consider that this definition is pretty abstract and also fails to tie in with how you have been thinking of $\leqslant$, for example, all these years. But then what is $\leqslant$ as a mathematical object or at least what does it do? It, like all binary relations, takes two input values from a set and compares them, giving them the nod or not — that is the output is True (T) or False (F). So $\leqslant$ looks at the inputs $(3,4)$ and as $3 \leqslant 4$ returns a favourable response T, but as $4 \leqslant 3$ is not true, $\leqslant$ returns F to the pair $(4,3)$; note the order of the inputs is crucial. So we might have defined a relation R on the set S as a map from the set of ordered inputs $S \times S$ to the set $\{T,F\}$. But this is equivalent to the above definition: those ordered pairs on which the relation R looks favourably, outputting T, go into the subset R and those that return the output F do not. The subset R, as given in the definition, is the subset $R^{-1}(T)$ of $S \times S$. For those pairs (s,t) in R we then write sRt along the same lines as we would write $3 \leqslant 4$.

Example 55 *(a) Let $S = \{1,2,3\}$ and let $\leqslant$ denote "less than or equal to" when comparing elements of S. Then*

$$\leqslant \text{ equals } \{(1,1),(1,2),(1,3),(2,2),(2,3),(3,3)\}.$$

(b) Let $S = \{1,2,3\}$ and let $|$ denote the relation on S given by "divides". Then

$$| \text{ equals } \{(1,1),(1,2),(1,3),(2,2),(3,3)\}.$$

(c) Let $S = \mathcal{P}(\{1,2\})$, the set of subsets of $\{1,2\}$ and $\subset$ denote the relation "is strictly contained in". Then

$$\subset \text{ equals } \{\{\varnothing,\{1\}\},\{\varnothing,\{2\}\},\{\varnothing,\{1,2\}\},\{\{1\},\{1,2\}\},\{\{2\},\{1,2\}\}\}.$$

Definition 56 *Let S be a set, R a relation on S and $s,t,u \in S$. We say that*
*(a) R is **reflexive** if sRs for all s in S.*
*(b) R is **symmetric** if whenever sRt then tRs.*
*(c) R is **anti-symmetric** if whenever sRt and tRs then $s = t$.*
*(d) R is **transitive** if whenever sRt and tRu then sRu.*

Example 57 *Define R on $\mathbb{N}$ by aRb if $b = a^k$ for some $k \geqslant 1$. Then R is reflexive, anti-symmetric, transitive but not symmetric.*

Solution Reflexivity: R is reflexive as $a = a^1$ for all $a \in \mathbb{N}$ and so aRa.
Anti-symmetry: Say now that aRb and bRa. Then $b = a^k$ and $a = b^l$ for $k,l \geqslant 1$. If $a = 0$ then $a = b = 0$ follows. If $a \neq 0$ then $a = (a^k)^l = a^{kl}$ and this implies $a^{kl-1} = 1$. Then $kl = 1$, giving $k = l = 1$ and implying $a = b$.
Transitivity: We see that R is transitive also – if aRb and bRc then $b = a^k$ and $c = b^l$ for some $k,l \geqslant 1$. Then $c = (a^k)^l = a^{kl}$ and so we see that aRc as $kl \geqslant 1$.
Symmetry: Finally R is not symmetric as $2R4$ is true but $4R2$ is false. $\square$

Example 58 *We define R on S, the set of $n \times n$ real matrices with $GL(n,\mathbb{R})$, with ARB if there exists an invertible matrix P such that $A = P^{-1}BP$. Then R is reflexive, symmetric and transitive but not anti-symmetric. The relation R is called **similarity**.*

Solution Reflexivity: we see that ARA for all A as $A = I^{-1}AI$.
Symmetry: if ARB then $A = P^{-1}BP$ for some $P$and so $B = PAP^{-1} = (P^{-1})^{-1}AP^{-1}$ showing BRA.

Transitivity: if ARB and BRC then $A = P^{-1}BP$ and $B = Q^{-1}CQ$ for invertible P, Q. Then $A = P^{-1}Q^{-1}CQP = (QP)^{-1}C(QP)$ showing that ARC as QP is invertible.
Anti-symmetry: we have already shown that R is symmetric. If R was also anti-symmetric then whenever ARB we'd have BRA by symmetry and $A = B$ by anti-symmetry. However

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

showing that ARB where $A = \text{diag}(1, -1)$ and $B = \text{diag}(-1, 1)$ but $A \neq B$. □

Example 59 *(a) $\leqslant$ on $\mathbb{N}$ is reflexive, anti-symmetric, transitive but is not symmetric.*
(b) $<$ on $\mathbb{Z}$ is anti-symmetric (vacuously so), transitive but is not reflexive nor symmetric.
(c) $=$ on $\mathbb{R}$ is reflexive, symmetric, anti-symmetric and transitive.
(d) If we define R on $\mathbb{Z}$ by mRn if $|m - n| \leqslant 1$, then R is reflexive, symmetric, but not transitive nor anti-symmetric.
(e) Given a set S with three or more elements, if we define R on $\mathcal{P}(S)$ by ARB if $A \cap B \neq \varnothing$, then R is symmetric, but not reflexive, anti-symmetric or transitive.

Solution Details are left as optional exercises.

Definition 60 *Let S be a set and R a relation on S.*
*(a) We say that R is a **partial order** on S if R is reflexive, anti-symmetric and transitive.*
*(b) A partial order is said to be a **total order** if for every $a, b \in S$ then aRb or bRa (or both).*
(c) Partial orders are often denoted with the symbol $\leqslant$.

Example 61 *Let S be a set and let $\mathcal{P}(S)$ denote the set of subsets of S. Then $\subseteq$ is a partial order on $\mathcal{P}(S)$.*

Solution By definition $A \subseteq A$ for any subset A of S.
To show anti-symmetry, suppose that $A \subseteq B$ and $B \subseteq A$. By double inclusion $A = B$.
Finally, say $A \subseteq B$ and $B \subseteq C$. If $a \in A$ then $a \in B$ as $A \subseteq B$. But then as $B \subseteq C$ we also have $a \in C$. So $A \subseteq C$ and $\subseteq$ is transitive. □

Example 62 *The following are all examples of partial orders.*
(a) Let X be a set and $S = \{f : X \to \mathbb{R}\}$. We define $f \leqslant g$ if $f(x) \leqslant g(x)$ for all $x \in S$. Note that this is not in general a total order. For example, with $X = \mathbb{R}$ then $\sin x$ and $\cos x$ are not comparable using $\leqslant$.
(b) With $S = \mathbb{C}$ then following is a partial order

$$z_1 \leqslant z_2 \quad \Leftrightarrow \quad z_1 = z_2 \quad \text{or} \quad \text{Re}z_1 < \text{Re}z_2,$$

as is

$$z_1 \leqslant z_2 \quad \Leftrightarrow \quad z_1 = z_2 \quad \text{or} \quad |z_1| < |z_2|.$$

(c) (Lexicographic Order) With $S = \mathbb{C}$ then following is a total order

$$z_1 \leqslant z_2 \quad \Leftrightarrow \quad \text{Im}z_1 < \text{Im}z_2 \quad \text{or} \quad (\text{Im}z_1 = \text{Im}z_2 \ \text{ and } \ \text{Re}z_1 \leqslant \text{Re}z_2),$$

(d) There is no total order on $\mathbb{C}$ with the following algebraic properties:

$$\text{if } \ 0 \leqslant z_1 \ \text{ and } \ 0 \leqslant z_2 \ \text{ then } \ 0 \leqslant z_1 + z_2 \ \text{ and } \ 0 \leqslant z_1 z_2.$$

(e) "Divides" on $\mathbb{N}$ is a partial order which is not a total order. e.g. $2 \nmid 3$ and $3 \nmid 2$.

Definition 63 *We say that a relation R on a set S is an **equivalence relation** if R is reflexive, symmetric and transitive.*

Example 64 *The following are all examples of equivalence relations.*
(a) $S = \mathbb{C}$ with $z \sim w$ if $|z| = |w|$;
(b) $S = \{$polygons in $\mathbb{R}^2\}$ and $\sim$ is congruence;
(c) $S = \mathbb{R}[x]$ with $f(x) \sim g(x)$ if $f'(x) = g'(x)$.
(d) Similarity of matrices, as defined in Example 58.
*(e) S is the set of $m \times n$ matrices, and $A \sim B$ if there is an invertible $m \times m$ matrix P and invertible $n \times n$ matrix Q such that $A = PBQ$. Here $\sim$ is known as **equivalence** of matrices.*

Example 65 *The following relations **aren't** equivalence relations:*
(a) $S = \mathbb{Z}$ with $m \sim n$ iff $m < n$ as $\sim$ isn't reflexive or symmetric;
(b) $S = \mathcal{P}(X)$ with $A \sim B$ if $A \subseteq B$ as $\sim$ isn't symmetric;
(c) $S = \mathbb{R}[x]$ with $p(x) \sim q(x)$ if $p(a) = q(a)$ for some $a \in \mathbb{R}$ as $\sim$ isn't transitive.

Proposition 66 *Let $S = \mathbb{Z}$ and $n \geqslant 2$ is an integer. If we set $a \sim b$ if $a - b$ is a multiple of n then $\sim$ is an equivalence relation.*

Proof (a) For any $a \in \mathbb{Z}$ we have $a \sim a$ as 0 is a multiple of n.
(b) If $a \sim b$ then $a - b = kn$ for some integer k. Then $b - a = -kn$ and hence $b \sim a$.
(c) If $a \sim b$ and $b \sim c$ then $a - b = kn$ and $b - c = ln$ for integers k, l. But then

$$a - c = (a - b) + (b - c) = (k + l)n$$

and hence $a \sim c$. $\square$

Definition 67 *Given an equivalence relation $\sim$ on a set S with $a \in S$, then the **equivalence class of** a, written $\bar{a}$ or $[a]$, is the subset*

$$\bar{a} = \{x \in S : x \sim a\}.$$

Example 68 *For Example 64(a), the equivalence classes are the circles centred at the origin with radius $r > 0$, and the origin by itself.*
For Example 64(c), the equivalence class of 0 is the set of constant functions.

Theorem 69 *Let $\sim$ be an equivalence relation on the set S. The equivalence classes of $\sim$ form a partition of S.*

Definition 70 *Let S be a set and Λ be an indexing set. We say that a collection of subsets A_λ of S (where $\lambda \in \Lambda$) is a **partition** of S if*
(i) $A_\lambda \neq \varnothing$ for each $\lambda \in \Lambda$;
(ii) $\bigcup_{\lambda \in \Lambda} A_\lambda = S$;
(iii) if $\lambda \neq \mu$ then $A_\lambda \cap A_\mu = \varnothing$, or equivalently: if $A_\lambda \cap A_\mu \neq \varnothing$ then $\lambda = \mu$.

Proof (Not on IUM syllabus – this result is proved in the HT *Groups and Group Actions* course – but it is included here for anyone interested) Recall that the equivalence class of $a \in S$ is

$$\bar{a} = \{s \in S : s \sim a\}.$$

In order to show that these partition S we need to show that equivalence classes are non-empty and that every element of S lies in one, and only one, equivalence class of S. Given $a \in S$ then $a \sim a$ by

reflexivity and so $a \in \bar{a}$. Hence every element lies in at least one equivalence class and such classes are non-empty.

We'll now show that two equivalence classes are either disjoint or equal. If two classes aren't disjoint and have an element in common, say $c \in \bar{a} \cap \bar{b}$ where $a, b, c \in S$, then

$$c \sim a \quad \text{and} \quad c \sim b.$$

By symmetry $a \sim c$ and, as $c \sim b$, from transitivity we have $a \sim b$.

Suppose now that $s \in \bar{a}$. Then $s \sim a$ and $a \sim b$ gives $s \sim b$ and so $s \in \bar{b}$. We've shown $\bar{a} \subseteq \bar{b}$. By symmetry $b \sim a$ and the same argument shows $\bar{b} \subseteq \bar{a}$. Hence $\bar{a} = \bar{b}$ completing the proof. □

Example 71 *Given the equivalence relation in Proposition 66 there are n equivalence classes namely $\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}$. We see that*

$$\bar{0} = n\mathbb{Z}; \qquad \bar{1} = 1 + n\mathbb{Z}; \qquad \ldots \qquad \overline{n-1} = (n-1) + n\mathbb{Z} = -1 + n\mathbb{Z}.$$

Theorem 72 *Let S be a set. Given a partition P of S and $a \in S$, we will write P_a for the unique set in P such that $a \in P_a$.*

(a) Given an equivalence relation $\sim$ on S then the equivalence classes of $\sim$ form a partition $P(\sim)$ of S (where $P(\sim)_a = \bar{a}$ for each $a \in S$).

(b) Given a partition P of S then the relation $\sim_P$ on S defined by

$$a \sim_P b \text{ if and only if } b \in P_a$$

is an equivalence relation on S.

(c) As given above, (a) and (b) are inverses of one another; that is

$$P(\sim_P) = P \qquad \text{and} \qquad \sim_{P(\sim)} = \sim .$$

In particular, there are as many equivalence relations on a set S as there are partitions of the set S.

Proof This result is not on the IUM syllabus. A proof of this will appear in the HT *Groups and Group Actions* course.

Optional Further Exercises
(for possible tutorial discussion)

Exercise 9 *Let $A, B \subseteq S$. Show that $(A^c)^c = A$. Show more generally that $A \backslash (A \backslash B)) = A \cap B$.*

Exercise 10 *Let $A, B, C \subseteq S$. The **symmetric difference** $A \Delta B$ is defined to be the subset consisting of those elements of S which are in A or are in B, but not both.*
(i) Show that

$$A \Delta B = (A \backslash B) \cup (B \backslash A).$$

(ii) Show further that

$$A \Delta \varnothing = A, \qquad A \Delta B = B \Delta A, \qquad A \Delta (B \Delta C) = (A \Delta B) \Delta C, \qquad A \Delta A = \varnothing.$$

Consequently $\mathcal{P}(S)$ is an Abelian group under Δ, with identity $\varnothing$ and every element its own inverse.
(iii) Show that

$$A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C).$$

Together with identities

$$(A \cap B) \cap C = A \cap (B \cap C), \qquad A \cap B = B \cap A, \qquad A \cap S = A,$$

this means that $\mathcal{P}(S)$ is a ***commutative ring*** *under Δ and $\cap$, with additive identity $\varnothing$ and multiplicative identity S.*

Exercise 11 *Give a sequence of non-empty sets $A_1 \supseteq A_2 \supseteq A_3 \supseteq \cdots$ such that their intersection*

$$\bigcap_{k=1}^{\infty} A_k$$

is non-empty. Repeat the exercise but where the intersection is empty.

Exercise 12 *Let R_1 and R_2 be two relations on a set S.*

(i) Show that if R_1 and R_2 are reflexive then $R_1 \cup R_2$ and $R_1 \cap R_2$ are both reflexive.

(ii) Show that if R_1 and R_2 are symmetric then $R_1 \cup R_2$ and $R_1 \cap R_2$ are both symmetric.

(iii) Show that if R_1 and R_2 are transitive then $R_1 \cap R_2$ is transitive.

[It follows from (i), (ii), (iii) that the intersection of two equivalence relations is an equivalence relation.]

(iv) Give an example to show that the union of two transitive relations need not be transitive.

Exercise 13 *Let S_1 and S_2 be sets with total orders $\leqslant_1$ and $\leqslant_2$ respectively. Show that* ***lexicographic order*** *$\leqslant$ on $S_1 \times S_2$ as defined by*

$$(s_1, s_2) \leqslant (t_1, t_2) \quad \Leftrightarrow \quad s_1 < t_1 \quad or \quad (s_1 = t_1 \quad and \quad s_2 \leqslant t_2)$$

is a total order.

Exercise 14 *A partially ordered set $(S, \leqslant)$ is said to be a* ***lattice*** *if for each $x, y \in S$ there is a least upper bound $x \vee y$ and a greatest lower bound $x \wedge y$. Show that the following partially ordered sets are lattices, describing $\vee$ and $\wedge$ in each case. m(We say that z is an upper bound for x and y is $x \leqslant z$ and $y \leqslant z$ and z is further a least upper bound if whenever $x \leqslant w$ and $y \leqslant w$ then $z \leqslant w$.)*

(i) $(\mathcal{P}(X), \subseteq)$ where X is a given set.

(ii) $(\mathbb{N}, |)$.

(iii) $(\mathbb{R}, \leqslant)$.

(iv) The space of bounded functions $f \colon \mathbb{R} \to \mathbb{R}$ with $f \leqslant g$ if $f(x) \leqslant g(x)$ for all real x.

3. FUNCTIONS

3.1 History and Basic Definitions

Functions now play a key role in mathematics, but first, fledgling concepts of functions first date only back to the 17th century, mainly down to the introduction of Cartesian co-ordinates and the development of calculus. Even by Euler's time, a century later, the working definition of a function was at best somewhat limited:

> A function of a variable quantity is an analytic expression composed *in any way whatsoever* of the variable quantity and numbers or constant quantities

and Euler also permitted functions to take multiple values. Fourier series in the nineteenth century led to the study of arbitrary real-valued functions of a real variable. The more general (naïve) definition of a function below could not have come about without Cantor's work on set theory in the late 19th century and a final rigorous definition of a function was not really in place until the twentieth century with the work of Zermelo, Fraenkel, Skolem, Von Neumann, Weyl.

Definition 73 *Let X and Y be sets. A **function** $f\colon X \to Y$ is an assignment of a value $f(x) \in Y$ for each $x \in X$. The set X is called the **domain** of f and the set Y is called the **codomain** of f. Functions are also referred to as **maps** and **mappings**.*

Remark 74 It is an important, if subtle, aspect to appreciate that a function is the "whole package" of assignment, domain and codomain. For example the following four functions are all different functions, despite the assignment looking the same, and are different in some crucial ways as we will later see.

$$\begin{aligned} f_1\colon \mathbb{R} &\to \mathbb{R} && \text{given by} && f_1(x) = x^2. \\ f_2\colon \mathbb{R} &\to [0,\infty) && \text{given by} && f_2(x) = x^2. \\ f_3\colon [0,\infty) &\to \mathbb{R} && \text{given by} && f_3(x) = x^2. \\ f_4\colon [0,\infty) &\to [0,\infty) && \text{given by} && f_4(x) = x^2. \end{aligned}$$

Definition 75 *Given a function $f\colon X \to Y$, the **image** or **range** of f is the set*

$$f(X) = \{f(x) : x \in X\} \subseteq Y.$$

Typically the image $f(X)$ is a proper subset of the codomain Y.

Example 76 *(a) The function $f\colon \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = |x|$ has image $\mathbb{N}$. Here the image is a proper subset of the codomain.*
(b) Let $X = \{1, 2, 3, \ldots n\}$ and $S = \mathcal{P}(X)\backslash\{\varnothing\}$ denote the set of non-empty subsets of X. Then the function

$$\max\colon S \to X \qquad \textit{defined by} \qquad \max(A) = \textit{the largest element of } A,$$

is a function with image X as $\max(\{k\}) = k$ for each $1 \leqslant k \leqslant n$.

(c) Let $T = \mathcal{P}(\mathbb{N})\backslash\{\varnothing\}$ denote the set of non-empty subsets of $\mathbb{N}$. The function

$$\max\colon T \to \mathbb{N} \qquad \textit{defined by} \qquad \max(A) = \textit{the largest element of } A,$$

*is **not** a well-defined function as some non-empty subsets of $\mathbb{N}$, such as $\mathbb{N}$ itself, do not have a largest element.*
*(d) The function $f\colon \mathbb{Q} \to \mathbb{Z}$ given by $f(m/n) = n$ is **not** a well-defined function as we would have*

$$f(2/3) = 3 \qquad \textit{and} \qquad f(4/6) = 6$$

yet $2/3 = 4/6$. A function cannot map the same point to more than one image point. We could amend our definition to give a well-defined function by insisting that m/n is the rational in simplest form with $n > 0$.
*(e) The function $f\colon \mathbb{N} \to \mathbb{Z}$ defined by $f(n) = n$ has image $\mathbb{N}$. The map f is called **inclusion**. Given a set B and a subset $A \subseteq B$ then the inclusion map $\iota\colon A \to B$ is defined by $\iota(a) = a$ for all $a \in A$.*
*(f) Given a set X, the **identity map** $\mathrm{id}\colon X \to X$ is defined by $\mathrm{id}(x) = x$ for all $x \in X$.*
*(g) Given a function $f\colon X \to Y$, and a subset $A \subseteq X$, the **restriction** of f to A is the map $f_{|A}\colon A \to Y$ defined by*

$$f_{|A}(x) = f(x).$$

So $f_{|A}$ is the same assignment as f but restricted only to the domain of A.

Remark 77 (Well-definedness) The phrase *well-defined* is common in mathematics – and it is commonly confusing to undergraduates as checking something is well-defined means checking different things in different scenario. "Well-defined" means just that – that a mathematical object has been *properly* defined; the definition means that there is no ambiguity nor omission in the definition of the mathematical object. But given the varying nature of such objects, what needs checking varies from situation to situation.

That said, it is common to need to check that a function is well-defined, and there are two main ways in which we might need to check a function is well-defined.

(a) The assignment needs to be defined for all elements of the domain with the output in the codomain. The functions below each fail to be well-defined for different reasons.

$$\begin{aligned} f_1\colon \mathbb{R} &\to \mathbb{R} \qquad x \mapsto \sqrt{x}; \\ f_2\colon \mathbb{C} &\to \mathbb{C} \qquad x \mapsto \sqrt{x}; \\ f_3\colon \mathcal{P}(\mathbb{N}) &\to \mathbb{N} \qquad A \mapsto |A|\,; \\ f_4\colon \mathbb{R} &\to \mathbb{R} \qquad x \mapsto \min\left\{y : y^3 + y > x\right\}; \\ f_4\colon \mathbb{R} &\to \mathbb{R} \qquad x \mapsto \min\left\{y : y^2 + y = x\right\}. \end{aligned}$$

- f_1 is not defined on the whole domain – it's not defined on the negative numbers. One way to resolve this would be to restrict the domain to $[0, \infty)$.
- f_2 is ambiguous. Every complex number has at least one square root, but the definition does not make clear how $f_2(-2i)$ is defined – would the answer be $1 - i$ or $-1 + i$. This problem could be resolved by finding a way to specify which square root is intended.
- f_3 is not defined on the whole domain – some subsets of $\mathbb{N}$ are infinite. This could be resolved by restricting the domain to finite sets or by extending the codomain to $\mathbb{N} \cup \{\infty\}$.

- f_4 is not well-defined as the set of such y does not in general have a minimum element. For example, when $x = 0$ then $y^3 + y > 0$ on the set $(0, \infty)$. That set has no minimum. Changing the strict inequality to a weak inequality would be a possible way of resolving this.

- f_5 is not defined on the whole domain. When $x = -1$ we see there are no real roots to the equation $y^2 + y = x$. One way to resolve this would be to restrict the domain to $x \in [-1/4, \infty)$ at which point we see f_5 is the function

$$f_5(x) = \frac{-1 - \sqrt{1 + 4x}}{2}.$$

(b) Functions need to be carefully defined on sets of equivalence classes. Many functions are defined in terms of representatives of equivalence classes, or in terms of language relating to equivalence classes. We already do this without thinking, for example you will have known for a long time that

the area of a triangle equals half base times height.

This formula does not relate to specific triangles with precisely known vertices – such a formula exists but is messy – but rather is defined on set of congruence classes of triangles.

In other examples a function is not well-defined when it does not "descend" to the set of equivalence classes. Here are two functions that are well-defined on T, the set of triangles in $\mathbb{R}^2$.

For $t \in T$, $f(t) =$ the length of the longest side of t.

For $t \in T$, $g(t) =$ the length of the largest angle of t.

Both these are well-defined notions for a particular triangle. Two different equivalence relations on T are $\sim_1$ which denotes congruence and $\sim_2$ which denotes similarity. Note that the function g still makes sense on both sets of equivalence classes $T/\sim_1$and $T/\sim_2$. However the function f only makes sense on $T/\sim_1$. We cannot refer to the longest side of a collection of triangles that are similar to one another, but it still makes sense to refer to their common largest angle.

Definition 78 *Let $f\colon X \to Y$ be a function.*
*(a) Given $A \subseteq X$, then the **image** of A, denoted $f(A)$, is the subset*

$$f(A) = \{f(x) : x \in A\} \subseteq Y.$$

*(b) Given $C \subseteq Y$, then the **pre-image** of C, written $f^{-1}(C)$, is the subset.*

$$f^{-1}(C) = \{x : f(x) \in C\} \subseteq X.$$

Example 79 *(a) Let $f\colon \mathbb{R} \to \mathbb{R}$ be the function $f(x) = x^2$, and $A = [0, \infty)$ and $B = (-\infty, 0]$. Then*

$$f(A) = A, \qquad f(B) = A, \qquad f^{-1}(A) = \mathbb{R}, \qquad f^{-1}(B) = \{0\}.$$

(b) Let $g\colon \mathbb{R} \to \mathbb{R}$ be the function $g(x) = e^x$, with A, B as in (a). Then

$$g(A) = [1, \infty), \qquad g(B) = (0, 1], \qquad g^{-1}(A) = \mathbb{R}, \qquad g^{-1}(B) = \varnothing.$$

(c) Let $h\colon \mathbb{R} \to \mathbb{R}$ be the function $h(x) = \cos x$, with A, B as in (a). Then

$$h(A) = h(B) = [-1, 1], \qquad h^{-1}(A) = \bigcup_{k \in \mathbb{Z}} [-\pi/2 + 2k\pi, \pi/2 + 2k\pi], \qquad h^{-1}(B) = \bigcup_{k \in \mathbb{Z}} [\pi/2 + 2k\pi, 3\pi/2 +$$

Example 80 *Let $f\colon \mathbb{R} \to \mathbb{R}$ be the function $f(x) = x^2$. Find all finite subsets A such that $f(A) = A$.*
Solution $A = \varnothing$ is such a set. A non-empty finite set A has an element x of largest magnitude. If $|x| > 1$ then $|x^2| > |x|$ and so $x^2 \notin f(A)$. So $A \subseteq [-1, 1]$. Again if A has a largest or smallest magnitude non-zero element with $|x| < 1$ we can arrive at the same contradiction as before. It follows that $A \subseteq \{-1, 0, 1\}$. As $\{-1, 0, 1\}$ has 8 subsets we can check that the only possibilities are

$$\varnothing, \quad \{0\}, \quad \{1\}, \quad \{0, 1\}, \quad \{-1, 1\}, \quad \{-1, 0, 1\}.$$

□

Proposition 81 *Let $f\colon X \to Y$ be a function.*
(a) For any $A \subseteq X$ we have $A \subseteq f^{-1}(f(A))$ but do not have equality in general.
(b) For any $C \subseteq Y$ we have $f(f^{-1}(C)) \subseteq C$ but do not have equality in general.
See also Proposition 89.

Proof (a) By definition $A \subseteq f^{-1}(f(A))$ as the elements of A map into $f(A)$. However other elements may also map into $f(A)$. If we consider the map $f(x) = x^2$ from $\mathbb{R}$ to $\mathbb{R}$ then we see for $A = \{1\}$ that

$$f^{-1}(f(A)) = f^{-1}(\{1\}) = \{-1, 1\} \neq \{1\} = A.$$

(b) We immediately have $f(f^{-1}(C)) \subseteq C$ as f maps the elements of $f^{-1}(C)$ into C by definition. However $f(f^{-1}(C))$ is a subset of the image of f and so need not equal C. For example with the same f as in (a) and $C = \{-1\}$ we see that

$$f(f^{-1}(C)) = f(\varnothing) = \varnothing \neq \{-1\} = C.$$

□

Definition 82 *Given two functions $f\colon X \to Y$ and $g\colon Y \to Z$ the **composition** $g \circ f\colon X \to Z$ is defined by*

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

Example 83 *For maps $f\colon X \to X$ and $g\colon X \to X$ in general we do not have $f \circ g \neq g \circ f$. For example, if we define $f(x) = x^2$ and $g(x) = x + 1$ as maps from $\mathbb{R}$ to $\mathbb{R}$ then*

$$(f \circ g)(x) = (x + 1)^2 \neq x^2 + 1 = (g \circ f)(x).$$

Proposition 84 ***(Composition is associative)*** *Let $f\colon W \to X$, $g\colon X \to Y$, $h\colon Y \to Z$ be three functions. Then*

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

Proof Let $w \in W$. Then, by the definition of composition, we have

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

□

3.2 Injections, Surjections, Bijections

Definition 85 *Let $f\colon X \to Y$ be a function between two sets.*

*(a) We say that f is **1–1** or **injective** if whenever $f(x_1) = f(x_2)$ for $x_1, x_2 \in X$ then $x_1 = x_2$.*

*(b) We say that f is **onto** or **surjective** if for each $y \in Y$ there exists $x \in X$ such that $f(x) = y$.*

*(c) We say that f is **bijective** if f is 1–1 and onto.*

Example 86 *Which of the following functions $f_i\colon \mathbb{R} \to \mathbb{R}$ are injective, which surjective?*

$$f_1(x) = x^2, \qquad f_2(x) = 2^x, \qquad f_3(x) = x^3 - x, \qquad f_4(x) = x^3 + x.$$

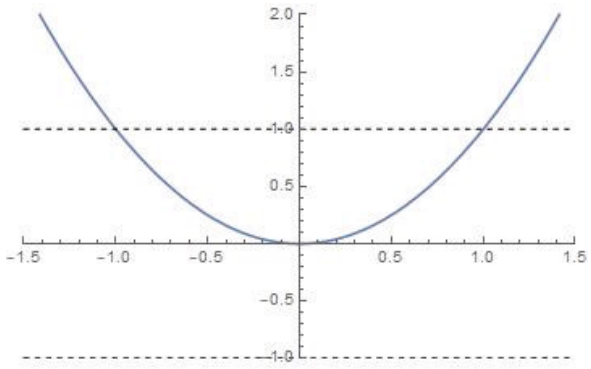


Figure 1: $y = f_1(x)$

Solution (a) f_1 is neither 1–1 nor onto. It is not 1–1 as $f_1(1) = 1 = f_1(-1)$ and is not onto as -1 is not in the image of f_1. the dashed lines in the graph of $y = f_1(x)$ highlight these facts.

(b) f_2 is 1–1. If $2^{x_1} = 2^{x_2}$ then $2^{x_1 - x_2} = 1$ and so $x_1 - x_2 = 0$. However f_2 is not onto as -1 is not in the image of the function.

(c) f_3 is not 1–1 as $f_3(1) = 0 = f_3(-1)$. It is onto, and this is best appreciated by a sketch of the graph $y = x^3 - x$ (Figure 1) or by knowing that every cubic has a real root. So the cubic equation $x^3 - x - y = 0$ has a real solution x for all values of y. Hence $y = f_3(x)$ is in the image of f_3 for all y or equivalently f_3 is onto.

(d) That $f_4'(x) = 3x^2 + 1 > 0$ means that f_4 is strictly increasing. So if $x_1 < x_2$ then $f_4(x_1) < f_4(x_2)$ and we see that f_4 never takes the same value at distinct inputs – that is f_4 is 1–1. Again sketching the graph $y = x^3 + x$ or knowing $x^3 + x - y = 0$ has a real solution x for all values of y, we see that f_4 is onto. □

Example 87 *If we return to the examples f_1, f_2, f_3, f_4 from Remark 74 we note the following*

$f_1\colon \mathbb{R} \to \mathbb{R}$	$f_1(x) = x^2$	*is neither 1–1 nor onto.*
$f_2\colon \mathbb{R} \to [0, \infty)$	$f_2(x) = x^2$	*is not 1–1 but is onto.*
$f_3\colon [0, \infty) \to \mathbb{R}$	$f_3(x) = x^2$	*is 1–1 but not onto.*
$f_4\colon [0, \infty) \to [0, \infty)$	$f_4(x) = x^2$	*is both 1–1 and onto.*

This reinforces the fact that a function is the whole package of assignment, domain and codomain. Note that f_1 and f_3 are not onto as -1 is not in the image, and f_1 and f_2 are not 1–1 as $(-1)^2 = 1^2$.

Proposition 88 *Let $f\colon R \to S$ and $g\colon S \to T$ be maps between sets R, S, T.*

(i) If f and g are onto then so is $g \circ f$. If $g \circ f$ is onto, then g is onto, but f need not be.

(ii) If f and g are 1–1 then so is $g \circ f$. If $g \circ f$ is 1–1, then f is 1–1, but g need not be.

Proof (i) Let $t \in T$. As g is onto then there exists $s \in S$ such that $g(s) = t$. Likewise as f is onto then there exists $r \in R$ such that $f(r) = s$. Hence

$$(g \circ f)(r) = g(f(r)) = g(s) = t,$$

thus showing that $g \circ f$ is onto. Again there is a partial converse, which is left to Sheet 2, Exercise 4(iii). But if $g \circ f$ is onto then f need not be onto as we can see by setting

$$\begin{aligned} R &= [0, \infty), \quad S = \mathbb{R}, \quad T = [0, \infty), \\ f\colon R &\to S \quad \text{given by} \quad x \mapsto \sqrt{x}, \\ g\colon S &\to T \quad \text{given by} \quad x \mapsto x^2. \end{aligned}$$

Here $(g \circ f)(x) = (\sqrt{x})^2 = x$ and so $g \circ f$ is certainly onto, but g is not onto as it does not take negative values.

(ii) This is Sheet 2, Exercise 4(i). There is a partial converse, namely that if $g \circ f$ is 1–1 then f is necessarily so, but g need not be. To show that f is 1–1, suppose that

$$f(r_1) = f(r_2).$$

Applying g to both sides of the equation, we have

$$(g \circ f)(r_1) = (g \circ f)(r_2)$$

and as $g \circ f$ is 1–1 then $r_1 = r_2$. However, g need not be 1–1 as shown using the same f, g, R, S, T as above. Here $(g \circ f)(x) = x$ and so $g \circ f$ is 1–1, but $g(1) = g(-1) = 1$ and so g is not 1–1. □

Proposition 89 *Let $f\colon X \to Y$ with $A \subseteq X$ and $B \subseteq Y$.*

(i) If f is 1–1 then $f^{-1}(f(A)) = A$.

(ii) If f is onto then $f(f^{-1}(B)) = B$.

(iii) In general, $f(f^{-1}(B)) = B \cap f(X)$.

(iv) If $f^{-1}(f(A)) = A$ for all $A \subseteq X$ then f is 1–1.

(v) If $f(f^{-1}(B)) = B$ for all $B \subseteq Y$ then f is onto.

Proof (i) We have already seen that $A \subseteq f^{-1}(f(A))$ so we need to show the reverse inclusion. Let $x \in f^{-1}(f(A))$. This means that $f(x) \in f(A)$ and so by definition there exists $a \in A$ such that $f(x) = f(a)$. Now as f is 1–1 then $x = a$ and so $x \in A$, thus showing the reverse inclusion.

(ii) We already have that $f(f^{-1}(B)) \subseteq B$ so we again need to show the reverse inclusion. Let $b \in B$. As f is onto then there exists $x \in X$ such that $b = f(x)$. Then $x \in f^{-1}(B)$ and $b = f(x) \in f(f^{-1}(B))$ and we've shown the reverse inclusion.

(iii) The logic of this proof is almost identical to (ii) and left as an optional exercise. Note that (iii) implies (ii), for if f is onto then $B \cap f(X) = B$.

(iv) Say that $f(x_1) = f(x_2)$ for $x_1, x_2 \in X$. Then $x_2 \in f^{-1}(f(\{x_1\})) = \{x_1\}$ and hence $x_2 = x_1$. This shows that f is 1–1.

(v) Let $y \in Y$ and then $f(f^{-1}(\{y\})) = \{y\}$. Consequently $f^{-1}(\{y\})$ is non-empty (as $f(\varnothing) = \varnothing$) and so there exists $x \in f^{-1}(\{y\})$ or equivalently $f(x) = y$. Hence f is onto. □

Definition 90 *Let $f\colon X \to Y$ be a function. We say that an **inverse** for f is a function $g\colon Y \to X$ such that*

$$g \circ f = id_X, \qquad f \circ g = id_Y.$$

*We say that f is **invertible** if it has an inverse.*

Proposition 91 *If $f\colon X \to Y$ is invertible then its inverse is unique. We write f^{-1} for the inverse.*

Proof Let g_1 and g_2 be two inverses for f. As composition is associative then

$$g_1 = g_1 \circ id_Y = g_1 \circ (f \circ g_2) = (g_1 \circ f) \circ g_2 = id_X \circ g_2 = g_2. \qquad \square$$

Notation 92 Let $f\colon X \to Y$ with $A \subseteq Y$. The earlier use of the notation $f^{-1}(A)$ for pre-images does not in any way imply that f is invertible. WHEN AND IF f is invertible, then the notation $f^{-1}(A)$ means the same both as the pre-image of A and also as the image of A under the function f^{-1}.

Example 93 *The function $x \mapsto \sin x$ from $\mathbb{R}$ to $\mathbb{R}$ is not invertible. It is not for example 1–1 as $\sin 0 = \sin \pi$. So when we consider the function $\sin^{-1}$ we are considering the inverse of the function $x \mapsto \sin x$ from $[-\pi/2, \pi/2]$ to $[-1, 1]$.*

Theorem 94 *A function $f\colon S \to T$ is bijective if and only if it is invertible.*

Proof Firstly we'll assume that f has an inverse $g\colon T \to S$ such that

$$f \circ g = id_T \text{ and } g \circ f = id_S. \tag{3.1}$$

To show f is 1–1, say $f(s_1) = f(s_2)$ for $s_1, s_2 \in S$. Then

$$s_1 = g(f(s_1)) = g(f(s_2)) = s_2$$

showing f is 1–1. To show that f is surjective, let $t \in T$ and note

$$f(g(t)) = t$$

showing that t is in the image of f and that f is onto.

Conversely, suppose that f is bijective. Our aim is to find a *well-defined* function $g\colon T \to S$ satisfying (3.1). For a function to be well-defined this means it needs to assign to every point of its domain a point in the codomain. Since f is onto, for $t \in T$, there exists $s \in S$ such that $f(s) = t$. As (3.1) requires that $f(g(t)) = t$ then a sensible definition for $g(t)$ would seem to be

$$g(t) = s.$$

A potential problem with this is that there may be many such s and a well-defined g can only assign one of these to t. But as f is 1–1 then we can show that there is in fact only one such s. If

$$f(s_1) = t = f(s_2)$$

then by injectivity $s_1 = s_2$. This means that the assignment

$$g(t) = s \text{ where } s \in S \text{ uniquely satisfies } f(s) = t \tag{3.2}$$

produces a well-defined map $g\colon T \to S$. Finally, for $s \in S$,

$$g\left(f\left(s\right)\right) = s$$

as s is the only element f maps to $f\left(s\right)$, and for $t \in T$,

$$f\left(g\left(t\right)\right) = t$$

straight from the definition of g in (3.2). $\square$

In fact, considered another way, injectivity and surjectivity can be rephrased as a function having a left-inverse or a right-inverse. We state, but do not prove, the following result.

Proposition 95 *Let $f\colon R \to S$ be a map between non-empty sets R and S.*
(a) f is 1–1 if and only if there is a map $g\colon S \to R$ such that $g \circ f = id_R$.
(b) f is onto if and only if there is a map $g\colon S \to R$ such that $f \circ g = id_S$.

3.3 Cardinality

Cardinality is a fancy word for size – given a set X we wish to rigorously define $|X|$, the cardinality of X, to be the number of distinct elements in the set X. For finite sets this will not throw up any surprises – more surprising results will emerge when infinite sets are encountered in the *Analysis I* course.

Definition 96 *Let $n \geqslant 1$ be a natural number and X be a set. We define the **cardinality** $|X|$ of X to be n if there is a bijection from X to the set $\{1, 2, \ldots, n\}$. The cardinality of the empty set is defined to be 0.*

Definition 97 *A set X is said to be **finite** if its cardinality is some natural number.*

Proposition 98 *Let $m, n \in \mathbb{N}$ with $m < n$. There is no bijection between $\{1, 2, \ldots, m\}$ and $\{1, 2, \ldots, n\}$. Consequently the cardinality of a finite set is well-defined.*

Proof Suppose, for a contradiction, there is some is a bijection between some $\{1, 2, \ldots, m\}$ and $\{1, 2, \ldots, n\}$ where $m < n$. And further we may assume m to be the smallest such integer for which there is a bijection

$$f\colon \{1, 2, \ldots, m\} \to \{1, 2, \ldots, n\}.$$

Then $1 \leqslant f(m) \leqslant n$ and we can restrict f to produce a bijection $\tilde{f}$ from $\{1, \ldots, m-1\}$ and $\{1, \ldots, n\} \setminus \{f(m)\}$ and then a bijection g from $\{1, \ldots, n\} \setminus \{f(m)\}$ to $\{1, \ldots, n-1\}$ by

$$g(k) = \begin{cases} k & 1 \leqslant k < f(m), \\ k-1 & f(m) < k \leqslant n. \end{cases}$$

Hence $g \circ \tilde{f}$ is a bijection from $\{1, \ldots, m-1\}$ to $\{1, \ldots, n-1\}$, contradicting the minimality of m. $\square$

Proposition 99 *Definition 96 agrees with the definition of cardinality given in Sheet 1, Exercise 5.*

Proof The definition given in Sheet 1, Exercise 5 is recursive, so the equivalence of these definitions can be verified using induction. The proof is left as an optional exercise.

Proposition 100 *Let n be a positive integer and $\varnothing \neq X \subseteq \{1, 2, \ldots, n\}$. There is an ordering*

$$x_1 < x_2 < \cdots < x_k$$

of the elements of X with $k \leqslant n$.

Proof The result holds for $n = 1$ as the only the only non-empty subset of $\{1\}$ is $\{1\}$. Assume now that the result is true for n and let $X \subseteq \{1, 2, \ldots, n+1\}$. If $X \subseteq \{1, 2, \ldots, n\}$ then we are done and if $n+1 \in X$ then, by hypothesis, there is an ordering $x_1, \ldots, x_k$ of $X \backslash \{n+1\}$ in which case $x_1, \ldots, x_k, n+1$ is an ordering of X. In the first case we have $k \leqslant n \leqslant n+1$ and in the second case as $k \leqslant n$ then $k+1 \leqslant n+1$. The result follows by induction. □

Proposition 101 ***(Pigeonhole Principle)*** *Let $m, n \in \mathbb{N}$ with $m > n \geqslant 1$ and let $f\colon \{1, 2, \ldots, m\} \to \{1, 2, \ldots, n\}$. Then there are distinct $1 \leqslant x_1 < x_2 \leqslant m$ with $f(x_1) = f(x_2)$. This means that there is no 1–1 map from $\{1, 2, \ldots, m\}$ to $\{1, 2, \ldots, n\}$. (The result gets its name from the analogy that if there are m letters that need to go into n pigeonholes, then at least one hole contains two or more letters.)*

Proof If the result is untrue, then there is a 1–1 map f from $\{1, \ldots, m\}$ to $\{1, \ldots, n\}$. This restricts to a bijection from $\{1, \ldots, m\}$ to the image of f. So the image of f contains m elements but is a subset of $\{1, \ldots, n\}$ so that $m \leqslant n$ by Proposition 100. This is the required contradiction. □

Proposition 102 *Let S and T be finite sets.*

(a) $|S| \leqslant |T|$ if and only if there is a 1–1 map from S to T.

(b) $|S| \geqslant |T|$ if and only if there is an onto map from S to T.

Proof (a) Say that $|S| = m$ and $|T| = n$ with $m \leqslant n$. Then we have bijections

$$f\colon S \to \{1, 2, \ldots, m\} \quad \text{and} \quad g\colon T \to \{1, 2, \ldots, n\}.$$

The map $h\colon \{1, 2, \ldots, m\} \to \{1, 2, \ldots, n\}$ given by $k \mapsto k$ is 1–1 and hence we have an injection $g^{-1} \circ h \circ f$ from S to T.

Conversely if there is a 1–1 map f from S to T, then this map is a bijection from S to its image $f(S) \subseteq T$. By Proposition 100 we then have $|S| = |f(S)| \leqslant |T|$ as required.

(b) Say that $|S| = m$ and $|T| = n$ with $m \geqslant n$. Then we have bijections

$$f\colon S \to \{1, 2, \ldots, m\} \quad \text{and} \quad g\colon T \to \{1, 2, \ldots, n\}.$$

The map $h\colon \{1, 2, \ldots, m\} \to \{1, 2, \ldots, n\}$ given by

$$h(k) = \begin{cases} k & 1 \leqslant k \leqslant n \\ n & n < k \leqslant m \end{cases}$$

is onto and hence we have a surjection $g^{-1} \circ h \circ f$ from S to T.

Conversely if there is a onto map f from S to T then, by Proposition 95, there a map $g\colon T \to S$ such that $f \circ g = id_T$. As id_T is 1–1 then g is 1–1 and hence $|T| \leqslant |S|$ as required. □

Proposition 103 *Let $n \geqslant 1$. There are $n!$ bijections from $\{1, 2, \ldots, n\}$ to $\{1, 2, \ldots, n\}$.*

Proof We could prove this by induction, but the proof is probably most transparent by considering how to construct such a bijection f. There are n choices for the value that $f(1)$ can take. However once $f(1)$ has been decided upon there are then $n-1$ choices for $f(2)$ as we must have $f(1) \neq f(2)$ for the map to be 1–1. Similarly, having decided on $f(2)$ there are then $n-2$ choices for $f(3)$ etc.. In all there are

$$n \times (n-1) \times (n-2) \times \cdots \times 2 \times 1 = n!$$

ways to construct a bijection. □

Example 104 *Let $A = \{1,2,3\}$ and $B = \{1,2\}$.How many maps are there from A to B? How many of these are 1–1, how many onto, how many bijective? Repeat this question for maps (b) $B \to A$, (c) $A \to A$, (d) $B \to B$.*

Solution (a) There are $2^3 = 8$ maps from A to B; to see this we note that each of $1,2,3$ can independently map to one of two values in B. None of these maps are 1–1 as we cannot find three distinct image points in B and so none of these maps are bijective. For a map $A \to B$ to be onto at least one element must map to each of 1 and 2. Say one element maps to 1 and two to 2; there are three such maps as the choice of what element maps to 1 entirely determines the map. There are similarly three maps where one element maps to 2. In all there are 6 onto maps from A to B.

(b) There are $3^2 = 9$ maps from B to A, none are onto, none are bijective and 6 are injective.

(c) There are $3^3 = 27$ maps from A to A. There are six maps that are 1–1, the same six being the onto maps and the bijections.

(d) There are $2^2 = 4$ maps from B to B. Two of these maps are 1–1 and as in (c) (and for the same reasons) these two maps are also the onto maps and the bijections. □

Example 105 *List the subsets of $\{1,2,3\}$.*

Solution There are eight subsets of $\{1,2,3\}$, each listed below.

$$\{1,2,3\}, \quad \{1,2\}, \quad \{1,3\}, \quad \{2,3\}, \quad \{1\}, \quad \{2\}, \quad \{3\}, \quad \varnothing.$$

Most of them will be natural enough though it may seem surprising that the **empty set**, $\varnothing$, the subset with no elements is a permitted subset.

Note that there are 2^3 subsets of $\{1,2,3\}$. This isn't that surprising if we note that each subset of $\{1,2,3\}$ is entirely determined by how it would 'respond' to the following 'questionnaire':

Is 1 an element of you? Is 2 an element of you? Is 3 an element of you?

Each element can be independently in a subset or not, irrespective of what else the subset may contain. Three independent binary (i.e. yes or no) decisions lead to 2^3 possible sets of responses. Respectively, the eight subsets above correspond to the series of questionnaire responses

$$YYY, \quad YYN, \quad YNY, \quad NYY, \quad YNN, \quad NYN, \quad NNY, \quad NNN. \quad \square$$

If we interpret the subsets of $\{1,2,\ldots,n\}$ as the possible responses to n yes-or-no questions then it is not surprising that there are 2^n subsets. Nonetheless we give a careful proof of this fact using induction.

Proposition 106 ***(Subsets of a finite set)*** *Show that there are 2^n subsets of the set $\{1,2,...,n\}$.*

Proof The subsets of $\{1\}$ are $\varnothing$ and $\{1\}$, thus verifying the proposition for $n = 1$. Suppose now that the proposition holds for a particular n and consider the subsets of $\{1, 2, \ldots, n, n+1\}$. Such subsets come in two, mutually exclusive, varieties: they either contain the new element $n+1$ or they don't.

The subsets of $\{1, 2, \ldots, n, n+1\}$ which *don't* include $n+1$ are precisely the subsets of $\{1, 2, ..., n\}$ and by hypothesis there are 2^n of these. The subsets of $\{1, 2, \ldots, n, n+1\}$ which *do* include $n+1$ are the previous 2^n subsets of $\{1, 2, ..., n\}$ together with the new element $n+1$ included in each of them; including $n+1$ in these 2^n distinct subsets still leads to 2^n distinct subsets. So in all we have $2^n + 2^n = 2^{n+1}$ subsets of $\{1, 2, \ldots, n, n+1\}$, completing the inductive step. □

Example 107 *Let X be a set with $|X| = n$.*

(a) How many binary relations are there on X?

(b) How many of these binary relations are reflexive?

(c) How many are symmetric?

(d) How many are reflexive and symmetric?

Solution (a) A binary relation on X is a subset of X^2. As $|X^2| = |X|^2 = n^2$ then there are 2^{n^2} relations on X.

(b) The decision to include (x_1, x_2) in a relation is one of n^2 independent binary choices. However for a reflexive relation, n of these decisions are already made as each (x, x) is in the relation. So $n^2 - n$ independent binary decisions remain and there are 2^{n^2-n} reflexive, binary relations on X.

(c) For symmetry if (x_1, x_2) is in the relation then so is (x_2, x_1). If we identify X with $\{1, 2, \ldots, n\}$ this means we only have to know whether (i, j) is in the relation where $i \leqslant j$. This leaves $\frac{1}{2}n(n+1)$ binary, independent decisions and so there are $2^{n(n+1)/2}$ symmetric, binary relations.

(d) For reflexivity and symmetry we still need to know whether (i, j) is in the relation where $i < j$. This leaves $\frac{1}{2}n(n-1)$ binary, independent decisions and so there are $2^{n(n-1)/2}$ reflexive, symmetric, binary relations.

Example 108 *Let A is a subset of $\{1, 2, 3, \ldots, 106\}$ of size 10.*

(a) As $|A| = 10$ then there are $2^{10} = 1024$ subsets of A.

(b) For each subset B of A, let s_B be the sum of the elements of B (with the convention that the empty set sums to zero). So the maximum possible value of s_B is achieved when B contains the ten largest elements of A in which case

$$s_B = 97 + 98 + \cdots + 106 = \frac{10}{2}(97 + 106) = 5 \times 203 = 1015.$$

(c) So we can consider s as a map from $\mathcal{P}(A)$ to $\{0, 1, \ldots, 1015\}$. As the first set has 1024 elements and the second set has 1016 then, by the pigeon-hole principle there exist (at least) two distinct subsets B, C of A such that $s_B = s_C$.

(d) The subsets found in part B and C are distinct, but need not be disjoint. For example, it might be the case that $\{1, 2, 3, 6, 9\}$ and $\{2, 5, 6, 8\}$ were the two distinct subsets of A; these are not disjoint as $2, 6$ are common elements. In this case we could produce disjoint sets, still with equal sums, by simply removing the common elements.

More generally, if B and C are distinct subsets such that $s_B = s_C$. Show that there are disjoint subsets B, C of A such that $s_B = s_C$ then $B \backslash C$ and $C \backslash B$ are disjoint subsets of A such that

$$s_{B\backslash C} = s_{C\backslash B}. \qquad \square$$

Recall, from Definition 20, that $\binom{n}{k} = n!/\{k!(n-k)!\}$ is read as 'n **choose** k'; as we shall see, the reason for this is that there are $\binom{n}{k}$ ways of choosing k elements without repetition from the set $\{1, 2, \ldots, n\}$, no interest being shown in the order that the k elements are chosen. By way of an example:

Example 109 *Determine* $\binom{5}{3}$ *and list the subsets corresponding to this number.*
Solution We have $\binom{5}{3} = \frac{5!}{3!2!} = \frac{120}{6\times 2} = 10$ and the corresponding subsets are

$$\{1,2,3\}, \quad \{1,2,4\}, \quad \{1,2,5\}, \quad \{1,3,4\}, \quad \{1,3,5\},$$
$$\{1,4,5\}, \quad \{2,3,4\}, \quad \{2,3,5\}, \quad \{2,4,5\}, \quad \{3,4,5\}.$$

Note that there are $6 = 3!$ orders of choosing the elements that lead to each subset. Any of the ordered choices

$$(1,2,3), \quad (1,3,2), \quad (2,1,3), \quad (2,3,1), \quad (3,1,2), \quad (3,2,1),$$

would have led to the same subset $\{1, 2, 3\}$. □

Proposition 110 *There are* $\binom{n}{k}$ *subsets of* $\{1, 2, \ldots, n\}$ *with* k *elements.*
Proof Let's think about how we might go about choosing k elements from n. For our 'first' element we can choose any of the n elements, but once this has been chosen it can't be put into the subset again. For our 'second' element, any of the remaining $n-1$ elements may be chosen, for our 'third' any of the $n-2$ that are left, and so on. So choosing a set of k elements from $\{1, 2, \ldots, n\}$ in a particular order can be done in

$$n \times (n-1) \times (n-2) \times \cdots \times (n-k+1) = \frac{n!}{(n-k)!} \text{ ways.}$$

But there are lots of different orders of choosing that would have produced the same subset. Given a set of k elements there are $k!$ ways of ordering them (Proposition 103) – that is to say, for each subset with k elements there are $k!$ different orders of choice that will each lead to that same subset. So the number $n!/(n-k)!$ is an 'overcount' by a factor of $k!$. Finally then, the number of subsets of size k equals $\binom{n}{k}$. □

Remark 111 In particular this means we can reinterpret the identity (1.3) as saying that the total number of subsets $\{1, 2, 3, \ldots, n\}$ equals 2^n (as demonstrated already in Proposition 106).

3.4 Infinite Sets

Cantor extended the ideas that we have seen introduced for the cardinality of finite sets to that of infinite cardinals. The smallest infinite cardinal is $\aleph_0$, pronounced *aleph-null*, the cardinality of the set of natural numbers $\mathbb{N}$. It's not hard to see that $\mathbb{Z}$ also has cardinality $\aleph_0$ but perhaps more surprising that $\mathbb{Q}$ also has cardinality $\aleph_0$. What may be even more surprising is that $\mathbb{R}$ has a larger cardinality – this is because Cantor showed there is no bijection from $\mathbb{R}$ to $\mathbb{N}$.

In our earlier results we saw that if A and B are two finite sets then:

- the disjoint union $A \sqcup B$ has cardinality $|A| + |B|$.
- the Cartesian product $A \times B$ has cardinality $|A|\,|B|$.
- the power set $\mathcal{P}(A)$ has cardinality $2^{|A|}$.
- there are $|B|^{|A|}$ maps from A to B.

Cantor extended these ideas to infinite sets, defining a way to add, multiply and take powers of infinite cardinals. We can also extend the idea of order to define the following:

- $|A| \leqslant |B|$ if there is a injection from A to B.
- $|A| \geqslant |B|$ if there is surjection from A to B.
- $|A| = |B|$ if there is a bijection from A to B.

A consequence of this is that we then need a theorem to prove that if $|A| \leqslant |B|$ and $|A| \geqslant |B|$ then $|A| = |B|$, the *Cantor-Bernstein-Schröder theorem.* Another significant theorem of Cantor's showed that any set A has more subsets than it does elements. That is $2^{|A|} > |A|$ and shows that there infinitely many different infinities! It turns out that

$$2^{\aleph_0} = |\mathcal{P}(\mathbb{N})| = |\mathbb{R}|\,,$$

but whether there is an infinity strictly between $|\mathbb{N}|$ and $|\mathbb{R}|$ turns out to be a very subtle question – the *continuum hypothesis* – which can not be decided using just the axioms of ZF set theory.

Some of these results are covered further in the *Analysis I* course this term.

Optional Further Exercises
(for possible tutorial discussion)

Throughout the following $f\colon X \to Y$ and $g\colon Y \to Z$ are functions, $A, B \subseteq X$, $C, D \subseteq Y$, $E \subseteq Z$.

Exercise 15 *Let $f\colon \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2$ with $A = [-1, 1]$. Find $f(\mathbb{R})$, $f^{-1}(\mathbb{R})$, $f(A)$, $f^{-1}(A)$.*

Exercise 16 *Let $f\colon \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = e^x$ with $A = [-1, 1]$. Find $f(\mathbb{R})$, $f^{-1}(\mathbb{R})$, $f(A)$, $f^{-1}(A)$.*

Exercise 17 *Let $f\colon \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2$. For each of the following cases, find a subset A such that*

(i) $f(f^{-1}(A)) = A$; (ii) $f(f^{-1}(A)) \neq A$; (iii) $f^{-1}(f(A)) = A$; (iv) $f^{-1}(f(A)) \neq A$.

Exercise 18 *Show that $f(A \cup B) = f(A) \cup f(B)$ but the corresponding identity is not true of intersections in general.*

Exercise 19 *Let $f\colon X \to Y$ and $g\colon Y \to Z$ with $A \subseteq X$, and $E \subseteq Z$.Show that*

$$(g \circ f)(A) = g(f(A)) \qquad \text{and} \qquad (g \circ f)^{-1}(E) = f^{-1}(g^{-1}(E)).$$

Exercise 20 *Let $f\colon \mathbb{N} \to \mathbb{N}$ be the map $f(n) = 2n$. Show that f is 1–1. Define a map $g\colon \mathbb{N} \to \mathbb{N}$ such that $(g \circ f)(n) = n$ for all n. Is there a map $h\colon \mathbb{N} \to \mathbb{N}$ such that $f(h(n)) = n$ for all n?*

Exercise 21 *How many differentiable functions $f(x)$ satisfy $f(x)^2 = x^2$ for all x? Show that there are infinitely many functions that satisfy $f(x)^2 = x^2$ for all x.*

Exercise 22 *Give an example of a bijection between the set $(0, 1)$ and each of the sets (i) $(0, \infty)$, (ii) $(-1, 1)$, (iii) $\mathbb{R}$, (iv) $[0, 1)$.*

Exercise 23 *Give an example of an injection from finite subsets of $\mathbb{N}$ and $\mathbb{N}$.*

Exercise 24 *Let S_1 and S_2 be sets with $\leqslant_1$ and $\leqslant_2$ be partial orders on S_1 and S_2. An **order isomorphism** between S_1 and S_2 is a bijection such that for all $x, y \in S$*

$$\phi(x) \leqslant_2 \phi(y) \quad \Leftrightarrow \quad x \leqslant_1 y.$$

(i) Show that $\leqslant$ is a partial order on $S_1 \sqcup S_2$ as defined by

$$x \leqslant y \quad \Leftrightarrow \quad \begin{cases} x \leqslant_1 y & \text{when } x, y \in S_1 \\ x \leqslant_2 y & \text{when } x, y \in S_2 \\ \text{true} & \text{when } x \in S_1 \text{ and } y \in S_2 \end{cases}$$

(ii) Show that, using the standard orders, that $\{0\} \sqcup \mathbb{N}$ is order isomorphic to $\mathbb{N}$ but not order isomorphic to $\mathbb{N} \sqcup \{0\}$.

4. WRITING MATHEMATICS, CONSTRUCTING PROOFS

4.1 Addressing Quantifiers. Analyzing Proofs.

Consider the two "proofs" below – one is correct, one false.

Proposition 112 *Let $f\colon R \to S$ and $g\colon S \to T$ be surjective. Then $g \circ f$ is surjective.*

Proof Let $t \in T$. As g is onto then there exists $s \in S$ such that $g(s) = t$. As f is onto then there exists $r \in R$ such that $f(r) = s$. Hence

$$(g \circ f)(r) = g(f(r)) = g(s) = t$$

and we see that $g \circ f$ is onto.

Proposition 113 *Let $f\colon R \to S$ and $g\colon S \to T$ be maps, such that $g \circ f$ is surjective. Then f is surjective.*

Proof Let $t \in T$ and write $t = g(s)$ where $s \in S$. As $g \circ f$ is onto then there exists r such that $g(f(r)) = t = g(s)$. Hence $f(r) = s$ and so f is onto.

The first proposition is true and its proof is correct and complete; the second proposition is false and so its "proof" is necessarily incorrect. Yet you may have found, reading these "proofs" for the first time, that both were plausible, especially if you didn't *actively* read the proof nor query its logic as you read. In both generating proofs yourself, and analyzing other – potentially incorrect or incomplete – proofs, it is important to know thoroughly the relevant definitions and how these definitions interweave. Most of that comes down to appreciating how to handle quantifiers and statements; to be confident in the veracity of a proof it's important to actively read and engage with each step of logic and again an intimate knowledge of the relevant definitions is important to that.

Looking to the first proposition, a formal statement of $g \circ f$ being surjective reads as

$$\forall t \in T \quad \exists r \in R \quad (g \circ f)(r) = t.$$

- Ask yourself, *really* ask yourself if you're comfortable with this line being correct. Is this what you would have written yourself? $g \circ f$ has T as its codomain and R as its domain, and being onto means *for every* element of the codomain *there exists* an element of the domain that maps to it. So yes this line is correct. If any of that was in doubt, then revisit your notes to make sure you have the definition right. *Don't try to start a proof with a fuzzy sense of what needs to be proved.*

When first meeting such dense language the new symbols may seem daunting, but the quantifiers $\forall$ and $\exists$ are in fact "road-signs" for the task at hand and, properly understood, will help construct a proof and indeed automatically fill in some of the lines of that proof.

Remark 114 Addressing quantifiers The first part of the statement reads $\forall t \in T$. Universal quantifiers, such as this, are relatively straightforward to address. Because of this quantifier our proof **must** begin

$$\text{Let } t \in T.$$

The only problem a universal quantifier presents is its generality. The statement requires something to be true for all t. We can address this by introducing an arbitrary but fixed t from T – then, in proving something to be true for this arbitrary t, we have proven it for all t. Consequently this t needs to be "untouched" during the proof. We cannot for convenience assume further specifics about this t (or else it would no longer be arbitrary) or if we wish to complete a proof by a case-by-case analysis then we need to be sure our cases are exhaustive. For example, we might prove something to be true of all real numbers x by showing it's true for all $x \geqslant 0$ and all $x < 0$.

The second quantifier reads $\exists r \in R$ and addressing these existential quantifiers is where all the work in a proof gets done. To do this we will need to look for help from the hypotheses.

Finally the statement ends with

$$(g \circ f)(r) = t.$$

So we now have the first and last lines of our proof. The proof must begin "Let $t \in T$" and must end "$(g \circ f)(r) = t$". Obviously at this moment we have no clear idea why such an $r \in R$ exists, and addressing this is our main task in completing the middle of the proof.

Note then that constructing a proof often begins by framing its extremes based on a clear, watertight sense of what needs proving, and then appreciating how the hypotheses help us fill in the middle, connecting logic.

Remark 115 Hypotheses Almost all propositions in mathematics take the form "if P then Q" (or "P if and only if Q" which is essentially two such statements combined). The facts given in P are the hypotheses and they are the connective tissue of a proof, taking us from the first scene-setting lines of a proof that frame and limit the proposition, to its concluding verification. Typically the result will be untrue without these hypotheses, so we should expect to use all the hypotheses along the way (possibly more than once), and only by knowing our formal definitions will it become clear when to deploy the hypotheses.

Here we need to get from "Let $t \in T$" to "$(g \circ f)(r) = t$". Our two hypotheses are

- $f\colon R \to S$ is onto: formally this means $\forall s \in S \quad \exists r \in R \quad f(r) = s$.
- $g\colon S \to T$ is onto: formally this means $\forall t \in T \quad \exists s \in S \quad g(s) = t$.

One hypothesis takes us forward (or at least gives us more information) when we are presented with an $s \in S$ and the other is helpful when we are presented with a $t \in T$. Returning to the task at hand, we see that the first line of our draft proof is "Let $t \in T$". Only one of our two hypotheses can "connect" to that information, the hypothesis that tells us g is onto. Thus we might expect the second line of our proof should read

$$\text{As } g \text{ is onto then there exists } s \in S \text{ such that } g(s) = t.$$

For a general map $g\colon S \to T$ it would not generally be the case that there exists such an $s \in S$, so it's important to include the hypothesis here to make clear the "why" of this intermediate conclusion.

And now we have introduced an $s \in S$ to which the first hypothesis neatly connects. Our third line now reads

$$\text{As } f \text{ is onto then there exists } r \in R \text{ such that } f(r) = s.$$

Again it's important to include the hypothesis that is being used as the conclusion "there exists $r \in R$ such that $f(r) = s$" is simply not true for general $f\colon R \to S$.

At this point we have used both hypotheses, so it might be timely to see how close we are to the desired conclusion. We need $r \in R$ such that $(g \circ f)(r) = t$. We haven't quite written that line down yet, but combining what we do know, from the second and third lines, we can see that

$$g(f(r)) = g(s) = t.$$

So our final line is only a notational redraft of where we have so far argued.

$$\text{Hence } (g \circ f)(r) = g(f(r)) = g(s) = t.$$

And the proof is now done.

Remark 116 Introducing notation The statement of the first proposition introduces the sets R, S, T and the maps f, g and so there is no further need to clarify that notation during the subsequent proof. However the elements r, s, t need to be carefully introduced and, where appropriate, carefully justified. So while we might introduce t as an arbitrary element of T the existence of s and r, together with the specific properties they have (e.g. $g(s) = t$) need to be carefully qualified by the hypotheses.

It is also helpful to introduce notation that is unambiguous, and where possible, easy to remember. So it makes sense to have elements r, s, t in sets R, S, T rather than say x, y, z.

During a more complicated proof it may of course be the case that several elements from the same set are discussed. In this case it will likely be important to make clear their differences – for example calling them s_1, s_2, s_3 or s, s', s''.

Remark 117 What a proof isn't Having learnt the requisite definitions thoroughly, a proof is certainly not a list of these definitions one after another in the hope that the reader will do the thinking and legwork for you. In a like manner eggs, cheese and cooking facilities are not per se an omelette, but all the necessary elements are there. Some appreciation of the final objective is necessary, and likewise how the ingredients work together. As with omelettes there are several ways to get a good end result (according to taste) and many ways to produce a result that technically might pass for an omelette, but only if you seek a generous friend's opinion.

Remark 118 Appreciating the roles and purposes of variables and hypotheses Initially proofs may seem like a sea of Greek notation and weirder symbols like $\forall$ and $\exists$. Whilst the rigour of these definitions helps keep a new proof-writer on the straight-and-narrow in generating a proof, some intuition will be very helpful in

- appreciating the role and need of a particular variable in the logic;
- appreciating where the help is coming from, and where the problems lie;
- appreciating, at a level beyond simple logic, how a particular proof works.

To return to the first (correct) proof, the desired result is

$$\forall t \in T \quad \exists r \in R \quad (g \circ f)(r) = t.$$

Here both quantifiers are problematic in the sense that the universal quantifier sets out the general scope of the task, and the existential quantifier assigns a task for each case within the given scope.

However in the first hypothesis

$$\forall t \in T \quad \exists s \in S \quad g(s) = t,$$

the universal quantifier is helpful as we know a certain result holds within a particular scope.

So you need to be able to separate task from help in a useful way. This might seem obvious in the sense that to prove "if P then Q" it is clearly going to be "P" that is helpful, but once all the dense logic starts appearing on the page it can become difficult to separate the help from the task.

Finally mathematical thinking is a lot more than laying logical cable as this may seem. It is important to build intuition of what definitions mean, and this will only become increasingly important as you meet more advanced ideas. You might, for example, begin to appreciate that a function $f\colon X \to Y$ being 1–1 is akin to there being no loss of information in the process of applying f – all of X is in some sense still present and retrievable in $f(X)$. So it might seem natural that the composition of two injective functions is injective as no information is lost overall. In itself there is no harm having/developing that intuition, but at the same time it is important to recognize how far from a satisfactory proof "no information is lost overall" is.

Remark 119 Analyzing proofs Let's return to the incorrect proof of the false statement:

Statement:Let $f\colon R \to S$ and $g\colon S \to T$ be maps, such that $g \circ f$ is surjective. Then f is surjective.

Proof: Let $t \in T$ and write $t = g(s)$ where $s \in S$. As $g \circ f$ is onto then there exists r such that $g(f(r)) = t = g(s)$. Hence $f(r) = s$ and so f is onto.

There is little chance of redeeming this proof, as the proposition itself is wrong. But it's worth flagging what errors are there and what irrelevances.

- One first tip-off is that the proof begins wrong. We are trying to prove that f is onto and so, necessarily, the proof has to begin by introducing $s \in S$, as S is the codomain of f. The false proof doesn't begin that way.
- We then write $t = g(s)$ for some s and there is no hypothesis that allows us to do this. To be able to guarantee the existence of such an s we would need to know that g is onto as a given hypothesis.
- A third error is to conclude from $g(f(r)) = g(s)$ that $f(r) = s$. This is something that we would know if g is 1–1, but again we haven't been told this.

Highlighted here these errors may now seem obvious, but passively read they would have seemed innocuous, and might easily have snuck by unnoticed.

4.2 Generating Proofs – Examples

The necessary guidance for how to construct and analyze proofs is largely given in the previous section. Here we apply that guidance to some further examples. The following definitions are not on the IUM syllabus, but you will meet them soon in the Analysis I course. They are introduced here to highlight how helpful careful definitions can be in generating a proof, even without any intuition having developed yet.

Definition 120 *(a) A (real)* ***sequence*** (x_n) *is a function* $x\colon \mathbb{N} \to \mathbb{R}$ *and we write* x_n *to denote* $x(n)$.
(b) A sequence (x_n) ***converges*** *if*

$$\exists L \in \mathbb{R} \quad \forall \varepsilon > 0 \quad \exists N \in \mathbb{N} \quad \forall n \geqslant N \quad |x_n - L| < \varepsilon.$$

Example 121 *Show that the sequence* $\left(\frac{1}{n+1}\right)$ *converges.*
Solution Thoughts: Looking at the definition of convergence, it begins with an existential quantifier $\exists L \in \mathbb{R}$. As opposed to universal quantifiers, some work and thinking has to be done in addressing this quantifier. This L is the **limit** to which the terms become arbitrarily close (within any ε). The sequence progresses as

$$1, \quad \frac{1}{2}, \quad \frac{1}{3}, \quad \frac{1}{4}, \quad \frac{1}{5}, \ldots,$$

remaining positive but becoming smaller and smaller. The only possible limit seems to be 0.

So we suspect $L = 0$ and the next quantifier is a universal one – here we just need a line "let $\varepsilon > 0$" introduced into the proof. But then we meet a second existential quantifier and need

$$\exists N \in \mathbb{N} \quad \forall n \geqslant N \quad |x_n - L| < \varepsilon.$$

Substituting in the expressions for $x_n = 1/(n+1)$ and L this means

$$\exists N \in \mathbb{N} \quad \forall n \geqslant N \quad \frac{1}{n+1} < \varepsilon.$$

We can rearrange the final equality to

$$\frac{1}{\varepsilon} - 1 < n.$$

So provided that $N \geqslant \varepsilon^{-1} - 1$ then we have found a suitable N and to address the third quantifier we need only include the phrase "let $n \geqslant N$".

Our proof might then look like:

Proof: Let $L = 0$ and take $\varepsilon > 0$. Take a natural number $N \geqslant \varepsilon^{-1} - 1$. For $n \geqslant N$ we have

$$|x_n - L| = \frac{1}{n+1} \leqslant \frac{1}{(\varepsilon^{-1} - 1) + 1} = \varepsilon.$$

Hence x_n converges.

Review: Note how much of this proof follows from the definition, the framing of the proof especially with the first and last lines necessarily having their form. Notice also how the proof addresses the quantifiers in the given order.

Example 122 *Show that the sequence* $((-1)^n)$ *does not converge.*

Remark 123 Negating statements Recall the logical forms of De Morgan's laws:

$$\begin{aligned}\neg(\forall x \in X \quad P(x)) &\Leftrightarrow \exists x \in X \quad \neg P(x);\\ \neg(\exists x \in X \quad P(x)) &\Leftrightarrow \forall x \in X \quad \neg P(x).\end{aligned}$$

The definition of convergence is

$$\exists L \in \mathbb{R} \quad \forall \varepsilon > 0 \quad \exists N \in \mathbb{N} \quad \forall n \geqslant N \quad |x_n - L| < \varepsilon.$$

By De Morgan's laws divergence (or non-convergence) is equivalent to

$$\begin{aligned}&\neg\left(\exists L \in \mathbb{R} \quad \forall \varepsilon > 0 \quad \exists N \in \mathbb{N} \quad \forall n \geqslant N \quad |x_n - L| < \varepsilon\right)\\ \Leftrightarrow\ &\forall L \in \mathbb{R} \quad \neg(\forall \varepsilon > 0 \quad \exists N \in \mathbb{N} \quad \forall n \geqslant N \quad |x_n - L| < \varepsilon)\\ \Leftrightarrow\ &\forall L \in \mathbb{R} \quad \exists \varepsilon > 0 \quad \neg\left(\exists N \in \mathbb{N} \quad \forall n \geqslant N \quad |x_n - L| < \varepsilon\right)\\ \Leftrightarrow\ &\forall L \in \mathbb{R} \quad \exists \varepsilon > 0 \quad \forall N \in \mathbb{N} \quad \neg\left(\forall n \geqslant N \quad |x_n - L| < \varepsilon\right)\\ \Leftrightarrow\ &\forall L \in \mathbb{R} \quad \exists \varepsilon > 0 \quad \forall N \in \mathbb{N} \quad \exists n \geqslant N \quad \neg\left(|x_n - L| < \varepsilon\right)\\ \Leftrightarrow\ &\forall L \in \mathbb{R} \quad \exists \varepsilon > 0 \quad \forall N \in \mathbb{N} \quad \exists n \geqslant N \quad |x_n - L| \geqslant \varepsilon\end{aligned}$$

So to negate a statement we need to reverse all the quantifiers (swap $\forall$s for $\exists$s and vice versa) and then negate the final statement.

Solution Thoughts: Looking at the definition

$$\forall L \in \mathbb{R} \quad \exists \varepsilon > 0 \quad \forall N \in \mathbb{N} \quad \exists n \geqslant N \quad \neg\,|x_n - L| \geqslant \varepsilon,$$

we begin with a universal quantifier $\forall L \in \mathbb{R}$. The remainder of the task is to show that this particular, but arbitrary L is not a limit. Let's try to understand just what is involved:

$$\exists \varepsilon > 0 \quad \forall N \in \mathbb{N} \quad \exists n \geqslant N \quad |x_n - L| \geqslant \varepsilon.$$

We need to find some $\varepsilon > 0$ such that

$$\forall N \in \mathbb{N} \quad \exists n \geqslant N \quad |x_n - L| \geqslant \varepsilon.$$

Note that $\forall N \in \mathbb{N} \quad \exists n \geqslant N$ means that however far we progress down into the natural numbers, there will be n beyond that point where a certain thing is true. So $\forall N \in \mathbb{N} \quad \exists n \geqslant N$ is equivalent to saying "there are infinitely many n". And for those n we need that $|x_n - L| \geqslant \varepsilon$ – that is we need x_n to be more than ε away from L.

Here is where a diagram helps visualize things. Quite generally it can be a good idea to capture a problem with a well-drawn, well-labelled diagram.

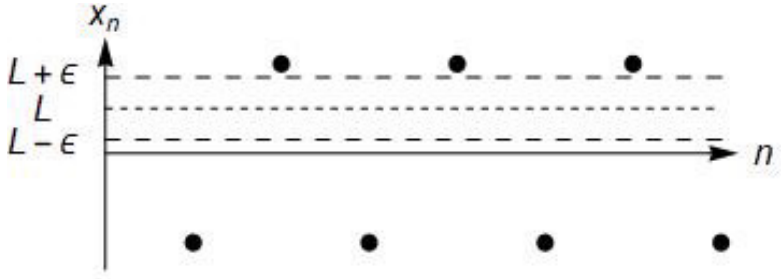


Figure 2: the sequence $-1, 1, -1, 1, -1, ...$

For each possible L we need to show there are infinitely many x_n at some distance (ε or more) away from L. Looking at the diagram it seems to make sense that when $L > 0$ to focus on the infinitely many values where $x_n = -1$ and when $L < 0$ to focus on the infinitely many values where $x_n = 1$. We will also need to include $L = 0$ in our case-by-case analysis.

This is an example where we have made further assumptions about our arbitrary L, but importantly the two cases we consider are exhaustive so we still are treating "all L". All this thinking has brought us to a point we might write down a formal proof.

Proof: Let $L \in \mathbb{R}$.

If $L > 0$ then set $\varepsilon = L$. Let $N \in \mathbb{N}$ and choose odd n such that $n \geqslant N$. Then

$$|x_n - L| = |-1 - L| = L + 1 \geqslant L = \varepsilon.$$

If $L < 0$ then set $\varepsilon = -L$. Let $N \in \mathbb{N}$ and choose even n such that $n \geqslant N$. Then

$$|x_n - L| = |1 - L| = 1 - L \geqslant -L = \varepsilon.$$

If $L = 0$ then set $\varepsilon = 1/2$. Let $N \in \mathbb{N}$ and choose any n such that $n \geqslant N$. Then

$$|x_n - L| = |x_n| = 1 \geqslant \frac{1}{2} = \varepsilon.$$

Example 124 *Let α be the unique real root that solves $\alpha^3 + \alpha = 1$. Show that α is irrational.*

Solution Suppose for a contradiction that $\alpha = m/n$ where m and n are coprime, positive integers. We then have that

$$\frac{m^3}{n^3} + \frac{m}{n} = 1 \qquad \Rightarrow \qquad m^3 + mn^2 = n^3.$$

Let p be a prime factor of m. We then see that p divides the LHS and so also divides n^3. As p is prime then p necessarily divides n. This is the required contradiction as we assumed m and n to be coprime.

Review: To what extent did the proof have to look like this? One approach would be to solve the cubic, find an explicit expression for α and then show that number to be irrational. But if we don't know how to solve the equation then contradiction seems the only alternative.

Once we have taken that approach, then we necessarily get to the equation $m^3 + mn^2 = n^3$ and our problem is how to get a contradiction from this – knowing the numbers involved are integers we might look to show that the two sides have different factors. We might note that m divides the LHS and so divides the RHS. However we can't in general quote that m then has to divide n just because it divides n^3. This is though true if m is prime, so now we can revisit the earlier step and instead focus on prime factors of m. It is not at all unusual, when constructing a proof, to have to go back and tighten an earlier assumption so that the direction of the proof can continue several steps later. Don't expect a first attempt at a proof to be as slick as the one above or those that appear in books.

4.3 Problem-solving. Producing counter-examples.

Here is a somewhat harder problem.

Example 125 *Let $f\colon \mathbb{N} \to \mathbb{N}$ be an onto function. Construct a function $g\colon \mathbb{N} \to \mathbb{N}$ which is a right inverse of f, i.e.$f(g(n)) = n$ for all n.*

Solution Thoughts: This is quite a general question – we are told nothing more about the function f except that it is onto. We could try finding examples of such g for certain specific f, but if we can only think of very specific onto functions then these examples aren't likely to offer much insight into the general picture.

So let's try a general approach and try to unpick just what g needs to do. We need that $f(g(n)) = n$ or written another way we need that $g(n) \in f^{-1}(\{n\})$. The set $f^{-1}(\{n\})$ is non-empty and so we just need a recipe for selecting our choice of $g(n)$. As non-empty subsets of the natural numbers, we can set

$$g(n) = \min\{k \in \mathbb{N} : f(k) = n\}.$$

A proof now just has to explain in a sensible order our previous thinking.

Example 126 ***Solution Proof**: Define*

$$g(n) = \min\{k \in \mathbb{N} : f(k) = n\}.$$

Note that the set $\{k \in \mathbb{N} : f(k) = n\} = f^{-1}(\{n\})$ is non-empty as f is onto, and non-empty subsets of $\mathbb{N}$ have minimal elements meaning g is well-defined. Finally as

$$g(n) \in \{k \in \mathbb{N} : f(k) = n\}$$

then $f(g(n)) = n$ as required.

Example 127 *Find all the 2×2 matrices A that satisfy $A^5 = I$ and $A^7 = I$.*

Solution Thoughts: If you have not seen an example like this before then the only way forward is to play around with what we've been given and see what we can deduce. We can conclude that $A^{12} = A^5A^7 = I$ and might ask what powers of A must equal the identity.

As $A^5 = I$ then A must be invertible (are we sure of this?) so that $I = I^{-1} = (A^5)^{-1} = A^{-5}$. We then have that $I = A^7A^{-5} = A^2$ and so $I = A^5(A^{-2})^2 = A$ and we have our result.

In fact having done all this thinking we might have the slicker proof:

Solution As $A^5 = I$ then $1 = \det A^5 = (\det A)^5$ and hence $\det A \neq 0$ and A is invertible. We then have

$$I = (A^5)^3(A^7)^{-2} = A^{15-14} = A$$

and $A = I$ is the only solution.

When it comes to producing counter-examples, or deciding on the truth or falsity of a statement, the approach is often much the same as trying to prove a statement. If no obvious counter-example is apparent, seeking to prove the statement may well be a best approach; even if the statement is false, then a counter-example can commonly be found where the logic of the proof just fails to follow.

Example 128 *True or false? Let $A, B \subseteq S$ and $f\colon S \to T$. Then $f(A \cap B) = f(A) \cap f(B)$.*

Solution Thoughts: For such questions, unless we can see the statement to be obviously true, I think most people try to find a counter-example, largely on the basis that a quick counter-example resolves the problem much quicker than a proof would. And it's a good instinct to go looking for counter-examples in the awkward places – potential special cases or where there hypotheses hold, but in some sense only just.

Such a case here might be when A and B are disjoint. There is no reason then that $f(A)$ and $f(B)$ need be disjoint – after all f might be constant – so it seems clear that the statement is false.

Importantly we still need to write down and explain a concrete counter-example.

Counter-example: Let $f\colon \mathbb{R} \to \mathbb{R}$ be the function $f(x) = 0$ for all $x \in \mathbb{R}$. Let $A = (-\infty, 0)$ and $B = (0, \infty)$ so that

$$\begin{aligned} \text{LHS} &= f(A \cap B) = f(\varnothing) = \varnothing; \\ \text{RHS} &= f(A) \cap f(B) = \{0\} \cap \{0\} = \{0\}. \end{aligned}$$

Hence the statement is false.

Further thoughts: But we might have not have so readily found a counter-example and tried proving the statement. Indeed this might have begun seemingly well.

Attempted proof: Let $t \in f(A \cap B)$. Then there exists $s \in A \cap B$ such that $f(s) = t$. As $s \in A \cap B \subseteq A$ then $t = f(s) \in f(A)$ and similarly $t \in f(B)$. Hence $t \in f(A) \cap f(B)$ and so $f(A \cap B) \subseteq f(A) \cap f(B)$.

Conversely let $t \in f(A) \cap f(B)$. As $t \in f(A)$ there exists $s_1 \in A$ such that $t = f(s_1)$; as $t \in f(B)$ there exists $s_2 \in B$ such that $t = f(s_2)$.

Further reflection: at this point we would like s_1 and s_2 to be the same point if we are to continue, but there seems to be no good reason why this is the case. It is also hear that we might find a counter-example. If "very different" s_1 and s_2 are being sent to the same point t then the statement is looking implausble – can we think of a function that does that?

Note also how close we might have been to "proving" this false statement. If we had been careless with our notation we might have concluded incorrectly that:

Conversely let $t \in f(A) \cap f(B)$. As $t \in f(A)$ there exists $s \in A$ such that $t = f(s)$; as $t \in f(B)$ there exists $s \in B$ such that $t = f(s)$. Then $s \in A \cap B$ and $t = f(s)$ showing $f(A) \cap f(B) \subseteq f(A \cap B)$.

It is very important that we make clear, with our choice of notation, that these two s are indeed distinct.

Example 129 *True or false? If the real sequences a_n and b_n converge, and $b_n \neq 0$ for all n, then the sequence a_n/b_n converges.*

Solution Thoughts: If we're going to find a counter-example here, it surely must be when b_n converges to 0. We might never be dividing by 0 when we make the quotient a_n/b_n but perhaps in some sense that becomes problematic in the limit. In any case, this seems a natural place to go looking for a counter-example.

At this point instinct might kick in and we realize if a_n stays away from 0 and b_n converges to 0 then a_n/b_n is going to be a large (positive or negative) value. So we need two sequences, with a_n and b_n converging with a_n at some remove from 0 and b_n converging to 0. When producing a counter-example, keep things simple.

Counter-example: Let $a_n = 1$ for all n and $b_n = 1/(n+1)$ for all n. Then $a_n \to 1$ and $b_n \to 0$ as $n \to \infty$, but

$$\frac{a_n}{b_n} = \frac{1}{1/(n+1)} = n + 1$$

does not converge.

Example 130 *True or false? The number* 100000003 *is a sum of two squares.*

Solution Thoughts: There has to be something property of the number 100000003 that is important here. We could program a computer to work this out, but this is clearly not our expected approach. Instead we might try to focus on what small numbers can be written as sums of squares, or investigate the nature of square numbers generally.

Beginning with small numbers we might create the table

$0 = 0^2 + 0^2$	$1 = 1^2 + 0^2$	$2 = 1^2 + 1^2$	3?	$4 = 0^2 + 2^2$	$5 = 1^2 + 2^2$
6?	7?	$8 = 2^2 + 2^2$	$9 = 0^2 + 3^2$	$10 = 1^2 + 3^2$	11?
12?	$13 = 2^2 + 3^2$	14?	15?	$16 = 0^2 + 4^2$	$17 = 1^2 + 4^2$

The list of numbers that cannot be expressed as a sum of two squares begins

$$3, 6, 7, 11, 12, 14, 15, \ldots$$

There doesn't seem to be than apparent a pattern here – and in any case by the time we have reached 100000003 we have a lot more square numbers to choose from.

What about the list of square numbers themselves

$$0, 1, 4, 9, 16, 25, 36, 49, 64, 81, \ldots$$

We can see that the even squares are divisible by 4 and this is not surprising as $(2k)^2 = 4k^2$. What about the odd squares? Well in this case

$$(2k+1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$$

is always 1 more than a multiple of 4.

So we can now see that the important fact about 100000003 is that it is 3 more than a multiple of 4. If square numbers are a multiple of 4 or one more than such a multiple, then a sum of two squares can be $0, 1$ or 2 more than a multiple of 4, but never 3 times such a multiple. The statement is false.

Solution Proof: Note that 100000003 is 3 more than a multiple of 4. As

$$(2k)^2 = 4k^2 \qquad \text{and} \qquad (2k+1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1,$$

then a square number is 0 or 1 more than a multiple of 4. So a sum of two squares can only be $0, 1$ or 2 more than a multiple of 4. It is therefore impossible that 100000003 can be written as a sum of two squares.

4.4 Appendix: Modular Arithmetic

Remark 131 Consider the following optional reading. Modular arithmetic is not expressly on the IUM syllabus, but some understanding of modular arithmetic helps during the first year, and highlights some of the topics that have arisen in the course, including equivalence relations and well-definedness.

Consider the odd and even integers. The product of two odd integers is an odd integer, no matter what odd integers we have in mind. Likewise we can see, for example, that

$$\text{Even} \times \text{Odd} = \text{Even}, \qquad \text{Odd} + \text{Odd} = \text{Even},$$

again irrespective of the even and odd numbers we have in mind. If we fill out the addition and multiplication tables for {Even, Odd} then we obtain

+	Even	Odd
Even	Even	Odd
Odd	Odd	Even

,

×	Even	Odd
Even	Even	Even
Odd	Even	Odd

.

More properly the above tables describe the arithmetic of the integers "modulo 2" or more simply "mod 2". **Modular arithmetic** is the study of remainders. If we divide an integer by 2 then there are two possible remainders 0 (when the integer is even) and 1 (when the integer is odd). We could instead rewrite the above addition and multiplication with 0 replacing Even and 1 replacing Odd. The tables would then look like:

+	0	1
0	0	1
1	1	0

,

×	0	1
0	0	0
1	0	1

.

Most of those calculations look fairly natural with the exception of $1+1=0$, but recall the equation is really conveying that an odd number added to an odd number makes an even number. From the point of view of remainders, adding the two remainders of 1 makes a whole new factor of 2; these two 1s add to *clock* back to 0.

In fact, modular arithmetic is sometimes also referred to as **clockwork arithmetic** and another everyday example of modular arithmetic is the 12-hour clock. It would not be at all surprising for me to say that 5 hours after 9 o'clock comes 2 o'clock or that 7 hours before 1 o'clock was 6 o'clock or that 7 three-hour shifts that started at 2 o'clock will end at 11 o'clock. In mod 12 arithmetic we would write these calculations as

$$5+9=2, \qquad 1-7=6, \qquad 2+7\times 3=11.$$

These facts are true irrespective of what day of the week we are discussing or whether 5 represents 5am or 5pm.(The only significant difference between mod 12 arithmetic and the 12-hour clock is that we write 0, instead of 12, for noon and midnight.)

More generally, we have:

Definition 132 *If we are doing arithmetic* mod n*, (where* $n \geqslant 2$*) then there are* n *possible remainders, namely*

$$0, 1, 2, 3, \ldots, n-1.$$

We define here rules for how to add, subtract and multiply these n *remainders in* mod n *arithmetic. Take* $a, b \in \{0, 1, 2, \ldots, n-1\}$*. It may well be the case that* $a+b, a-b$ *or* ab *aren't on this list, but the remainders of this sum, difference and product will be. We may define* mod n *addition, subtraction and multiplication by:*

$$\begin{aligned} a+b &= \textit{remainder when } a+b \textit{ is divided by } n; \\ a-b &= \textit{remainder when } a-b \textit{ is divided by } n; \\ ab &= \textit{remainder when } ab \textit{ is divided by } n. \end{aligned}$$

Notation 133 We write $\mathbb{Z}_n$ for the set of remainders $\{0, 1, 2, \ldots, n-1\}$ under the operations of $\bmod n$ arithmetic. Also we will write $\bmod n$ besides a sum, difference or product to denote that we are doing these operations in the context of $\bmod n$ arithmetic.

Example 134 *In* $\bmod 7$ *arithmetic we have*

$$\begin{aligned} 3+6 &= 2 \mod 7 \text{ as } 3+6=9 \text{ and } 9=1\times 7+2;\\ 3-5 &= 5 \mod 7 \text{ as } 3-5=-2 \text{ and } -2=(-1)\times 7+5;\\ 3\times 5 &= 1 \mod 7 \text{ as } 3\times 5=15 \text{ and } 15=2\times 7+1. \end{aligned}$$

We can more concisely write down all the rules of $\bmod 7$ *arithmetic with addition and multiplication tables:*

$+$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$\times$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Definition 132 has the advantage of being unambiguous (i.e. the operations $+, -, \times$ clearly deliver well-defined answers) but it also looks a little unnatural. For example, is it clear that the distributive law still applies? Alternatively, we can take a more formal view of what the arithmetic of $\mathbb{Z}_n$ is. In Proposition 66, we met the equivalence relation on $\mathbb{Z}$ given by $a \sim b$ if $a-b$ is a multiple of n. We can see now that this is the same as saying

$$a \sim b \text{ if and only if } a = b \mod n. \tag{4.1}$$

We saw in Example 71 that there are then n equivalence classes $\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}$. An alternative, more formal but also more natural, definition of the arithmetic of $\mathbb{Z}_n$ is then:

Definition 135 *Let* $\mathbb{Z}_n$ *denote the equivalence classes* $\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}$ *of* $\mathbb{Z}$ *under the equivalence relation (4.1). We define the operations* $+$ *and* $\times$ *on* $\mathbb{Z}_n$ *by*

$$\bar{a} + \bar{b} = \overline{a+b}, \qquad \bar{a} \times \bar{b} = \overline{a \times b}.$$

Proposition 136 *The operations* $+$ *and* $\times$ *are well-defined on* $\mathbb{Z}_n$*.*

Proof How might $+$ and $\times$ not be well-defined? Well, because the same equivalence class has many different representatives (e.g. $\bar{1} = \bar{7}$ in $\mathbb{Z}_6$) it's feasible that we might have $\bar{a} = \bar{\alpha}$ and $\bar{b} = \bar{\beta}$ yet $\overline{a+b} \neq \overline{\alpha+\beta}$. Adding the same two elements shouldn't be able to yield two different sums. So suppose that $\bar{a} = \bar{\alpha}$ and $\bar{b} = \bar{\beta}$, then

$$a - \alpha = kn \text{ and } b - \beta = ln$$

for $k, l \in \mathbb{Z}$. But then

$$(a+b) - (\alpha+\beta) = (a-\alpha) + (b-\beta) = (k+l)n$$

and

$$ab - \alpha\beta = (\alpha + kn)(\beta + ln) - \alpha\beta = (k\beta + l\alpha + kln)n$$

and hence $\overline{a+b} = \overline{\alpha+\beta}$ and $\overline{ab} = \overline{\alpha\beta}$ are both true so that $+$ and $\times$ are well-defined. $\square$

Proposition 137 *(a) + is associative and commutative.*

(b) Further × is associative, commutative and distributes over +.

Proof That + is associative and commutative, and the properties of × mentioned in (b) are all inherited from the same properties in $\mathbb{Z}$. For example, to see that the distributive law still holds, we simply have to note for $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$ that

$$\begin{aligned}
\bar{a}\left(\bar{b}+\bar{c}\right) &= \bar{a}(\overline{b+c}) && [\text{as } + \text{ is well-defined in } \mathbb{Z}_n] \\
&= \overline{a(b+c)} && [\text{as } \times \text{ is well-defined in } \mathbb{Z}_n] \\
&= \overline{ab+ac} && [\text{by the distributive law in } \mathbb{Z}] \\
&= \overline{ab}+\overline{ac} && [\text{as } + \text{ is well-defined in } \mathbb{Z}_n] \\
&= \bar{a}\,\bar{b}+\bar{a}\,\bar{c} && [\text{as } \times \text{ is well-defined in } \mathbb{Z}_n]. \qquad \square
\end{aligned}$$

We now note, for certain values of n, that modular arithmetic can have some unfortunate algebraic aspects such as

$$3 \times 5 = 0 \bmod 15, \qquad 4 \times 3 = 0 \bmod 6.$$

It follows that one cannot divide by 3 or 5 in $\mathbb{Z}_{15}$ nor divide by 3 or 4 in $\mathbb{Z}_6$. More generally we note:

Proposition 138 *Let $\bar{x} \in \mathbb{Z}_n$ with $x \neq 0$.*

$\bar{x}$ has a multiplicative inverse if and only if $\mathrm{hcf}(x, n) = 1$. *Hence if n is prime, then $\mathbb{Z}_n$ is in fact a field.*

Proof The proofs rely on theory from the Groups and Group Actions course and are omitteed here.