# Introductory Mathematics

Joseph Muscat 1999

1. What, in your opinion, is a number? Can you give a real-world example of a negative and a complex number? Are they just useful but "unreal" numbers?

2. Find the highest common factor of 182527 and 100939.

3. Both the rational and irrational numbers are "dense" in the sense that no matter how small an interval you consider, there are still plenty of them. Do you think there are more/less rationals than irrationals? Is this a meaningless question?

4. A Cretan once said "All Cretans are liars". Comment.

5. The ancient Chinese hypothesized that $n$ is a prime number when $n$ divides $2^n - 2$. In fact, 2 divides $2^2 - 2 = 2$, 3 divides $2^3 - 2 = 6$, 4 does not divide $2^4 - 2 = 14$, 5 divides $2^5 - 2 = 30$. Are you convinced it's true?

# 1 Logic

Logic is the language of mathematics. It tells us how to construct statements and how to deduce one statement from another.

## 1.1 Statements

**Definition** A **statement** is a meaningful sentence which is either **true** or **false**.

Ambiguous sentences, gibberish and sentences that cannot possibly be true or false, are not called statements.

There are many ways of constructing statements. The most common ones are the following:

- Given a statement $\phi$, we can form its **negation** or opposite NOT $\phi$. The statement NOT $\phi$ is true when $\phi$ is false and is false when $\phi$ is true.
- Given statements $\phi$ and $\psi$, we can form the **or** statement $\phi$ OR $\psi$, which is true when at least one of $\phi$ or $\psi$ is true.
- Given statements $\phi$ and $\psi$, we can form the **and** statement $\phi$ AND $\psi$, which is true when both $\phi$ and $\psi$ are true.
- The statement $\phi \Rightarrow \psi$ also written as IF $\phi$ THEN $\psi$, means that when $\phi$ is true, $\psi$ must also be true; when $\phi$ is false we cannot conclude anything about $\psi$ i.e. $\psi$ can be true or false.

  This **implication** statement is the most common one in mathematics, and has many equivalents in English eg $\phi$ *implies* $\psi$; $\psi$ *if* $\phi$; $\phi$ *is a sufficient condition for* $\psi$; $\psi$ *is a necessary condition for* $\phi$; $\psi$ *when* $\phi$. For example, "when the sun is up, it is daytime", "if $f(x)$ is a maximum then $f'(x) = 0$".
- We also have the **equivalence** statement $\phi \Leftrightarrow \psi$ which is the same as $\phi \Rightarrow \psi$ AND $\psi \Rightarrow \phi$. In this case $\phi$ is true exactly when $\psi$ is true, and therefore are essentially the same statement.

### 1.1.1 *Remarks*

$\phi \Rightarrow \psi$ and $\psi \Rightarrow \phi$ are two *different* statements. For example: Let us write "*If it is raining it must be wet outside*" in short as *raining* $\Rightarrow$ *wet*. The statement *wet* $\Rightarrow$ *raining* would then mean *if it is wet outside then it must be raining* which is false. Similarly $n$ even $\Rightarrow$ $2n$ even, but $2n$ even $\not\Leftarrow$ $n$ even!

However, $\phi \Rightarrow \psi$ and NOT $\psi \Rightarrow$ NOT $\phi$ have the same meaning. In the example above, the statement *if it is dry outside then it is not raining* is valid and has the same meaning as the original statement.

Note that NOT $\phi \Rightarrow$ NOT $\psi$ is the same as $\psi \Rightarrow \phi$.

One has to be very careful when taking opposites or negations. The opposite of *it is raining* is not *it is shining* but *it is not raining* (it could be slightly cloudy, very cloudy, drizzling etc.) Similarly the opposite of $n > 0$ is not $n < 0$ but $n \leqslant 0$.

Suppose that $\phi \Rightarrow \psi$. If $\phi$ is false it does not follow that $\psi$ is false. Statement $\psi$ could be true for other reasons. For example, $n$ is an odd prime $\Rightarrow$ $n^2$ is odd, is a true statement; yet $n^2$ may be odd even if $n$ is not an odd prime (eg $n = 9$).

## 1.2 For All, There Exists

Sometimes we wish to concatenate an infinite number of statements:

$$\phi_1 \text{ AND } \phi_2 \text{ AND } \phi_3 \text{ AND } \ldots.$$

We write this in short as,

$$\forall x \quad \phi_x$$

Note that $x$ does not have to be a number, as long as $\phi_x$ makes sense.

Similarly,

$$\exists x \quad \phi_x$$

means $\phi_1$ OR $\phi_2$ OR $\phi_3$ OR $\ldots$.

### 1.2.1 Example.

$$\forall x \quad (x+1)(x-1) = x^2 - 1$$

This is just shorthand for $(1+1)(1-1) = 1^2 - 1$ AND $(2+2)(2-2) = 2^2 - 1$ AND ....

$\exists n \quad n^2 = 4$ means that there is at least one $n$ (maybe there are many) which makes the statement true. In other words the following statement is true: $0^2 = 4$ OR $1^2 = 4$ OR $2^2 = 4$ OR $3^2 = 4$ OR .... The third part of this statement is true, making the whole statement true.

One can use more variables, and can mix the two ideas:

$$\forall x, y \quad \phi_{x,y},$$

$$\forall x \, \exists y \quad \phi_{x,y}.$$

Examples: $\forall x, y \quad (x+y)(x-y) = x^2 - y^2$; $\quad \forall x \, \exists y \quad x < y$.

Note, however, that $\forall x \, \exists y \quad \phi_{x,y}$ and $\exists y \, \forall x \quad \phi_{x,y}$ are very different statements — the *order* of placing the symbols $\forall$ and $\exists$ is very important.

Examples: Let $\phi_{x,y}$ be the statement *$x$ is a citizen of country $y$*. Then $\forall x \, \exists y \quad \phi_{x,y}$ would mean *every person is a citizen of some country*. On the other hand, $\exists y \, \forall x \quad \phi_{x,y}$ means *there is a country such that all persons are citizens of it*.

Similarly, $\forall x \, \exists y \quad x < y$ is very different from $\exists y \, \forall x \quad x < y$.

## 1.3 Opposites

For all the statements that we can create, we can form their opposites or negation. Following is a list of the basic ones. More complex statements can be negated step by step.

| *Statement* | *Opposite* |
|---|---|
| $\phi$ | NOT $\phi$ |
| $\phi$ AND $\psi$ | NOT $\phi$ OR NOT $\psi$ |
| $\phi$ OR $\psi$ | NOT $\phi$ AND NOT $\psi$ |
| $\phi \Rightarrow \psi$ | $\phi$ AND NOT $\psi$ |
| $\forall x \quad \phi_x$ | $\exists x \quad$ NOT $\phi_x$ |
| $\exists x \quad \phi_x$ | $\forall x \quad$ NOT $\phi_x$ |

### 1.3.1 Examples

The opposite of $\forall x > 0 \quad x^2 + x > 0$ is $\exists x > 0 \quad x^2 + x \leqslant 0$.

The opposite of $\forall \epsilon > 0 \; \exists \delta > 0 \; \forall x \quad |x| < \delta \;\Rightarrow\; x^2 < \epsilon$ is

$$\exists \epsilon > 0 \; \forall \delta > 0 \; \exists x \quad |x| < \delta \text{ AND } x^2 \geqslant \epsilon.$$

## 1.4 Proofs

Consider the statements:

(i) Every number is the sum of four squares.

$$\forall n \, \exists a, b, c, d \quad n = a^2 + b^2 + c^2 + d^2$$

(ii) Every odd number is the sum of a prime number and twice a square number.

$$\forall n \text{ odd} \, \exists a, p \quad p \textit{ is } \text{prime AND } n = p + 2a^2$$

(iii) Every even number is the sum of two primes.

$$\forall n \text{ even} \; \exists p_1, p_2 \text{ prime } n = p_1 + p_2$$

If one starts checking the three statements whether they are true or not, by substituting one number after another, then all three statements would appear true.

(i)

$$\begin{array}{lll} 1 = 1^2 & 2 = 1^2 + 1^2 & 3 = 1^2 + 1^2 + 1^2 \\ 4 = 2^2 & 5 = 2^2 + 1^2 & 6 = 2^2 + 1^2 + 1^2 \\ 7 = 2^2 + 1^2 + 1^2 & 8 = 2^2 + 2^2 & 9 = 3^2 \end{array}$$

(ii) if we check just the odd non-primes,

$$\begin{array}{lll} 9 = 7 + 2.1^2 & 15 = 7 + 2.2^2 & 21 = 19 + 2.1^2 \\ 25 = 23 = 2.1^2 & 27 = 19 + 2.2^2 & 33 = 31 + 2.1^2 \\ 35 = 17 + 2.3^2 & 39 = 37 + 2.1^2 & 41 = 23 + 2.3^2 \end{array}$$

(iii)

$$\begin{array}{lll} 4 = 2 + 2 & 6 = 3 + 3 & 8 = 2 + 5 \\ 10 = 3 + 7 & 12 = 5 + 7 & 14 = 7 + 7 \\ 16 = 3 + 13 & 18 = 5 + 13 & 20 = 3 + 17 \end{array}$$

They all *appear* true, but in fact only (i) is known to be true — it was proved by J. Lagrange in the 18th century; (ii) is a false statement: the odd number 5777 cannot be written as $p+2a^2$ with $p$ prime; (iii) is not currently (2004) known to be true or false — it is called "Goldbach's Conjecture" and although most mathematicians think it's true, one cannot be certain until someone actually shows it so, which is why it is called a conjecture rather than a proposition or theorem.

We accept a statement, which in mathematics is called a *proposition, theorem, corollary* etc., to be true if there is a **proof** for it. Three ways of proving a statement (but not the only ones) are the following:-

- **Deductive proof**

  To prove a statement $\omega$, start with a previously proven statement $\alpha$, and show step by step, that $\alpha \Rightarrow \beta$, then that $\beta \Rightarrow \gamma$, and so on until you prove $\omega$.

  $$\alpha \Rightarrow \beta \Rightarrow \gamma \Rightarrow \ldots \Rightarrow \omega$$

  To prove the statement $\alpha \Rightarrow \omega$, assume that statement $\alpha$ is true, and continue as above to prove that $\omega$ is true.

- **Contrapositive proof**

  To prove $\alpha \Rightarrow \beta$, suppose that $\beta$ is false and then show that $\alpha$ must also be false. This way gives a direct proof for the statement NOT $\beta \Rightarrow$ NOT $\alpha$ which is the same as $\alpha \Rightarrow \beta$.

- **Proof by Contradiction**

  To prove a statement $\alpha$, suppose that it is false and hence show that you end up with a false statement i.e. NOT $\alpha \Rightarrow$ FALSE. This cannot possibly be the case. Therefore $\alpha$ must be true.

  To prove $\alpha \Rightarrow \beta$, suppose that it is false i.e. suppose that $\alpha$ is true AND $\beta$ is false, then show that you get a contradiction.

### 1.4.1 Examples

*Proposition*

$$x^2 - 3x + 2 < 0 \Rightarrow x > 0$$

Proof by deduction:

$$\begin{aligned} x^2-3x+2<0 &\Rightarrow 3x>x^2+2 && \text{adding } 3x \text{ on both sides}\\ &\Rightarrow 3x>2 && \text{since } x^2 \text{ is positive}\\ &\Rightarrow x>2/3 && \text{dividing by 3}\\ &\Rightarrow x>0 \end{aligned}$$

Proof by contrapositive:

$$\begin{aligned} x\leqslant 0 &\Rightarrow x-1<0 \text{ AND } x-2<0\\ &\Rightarrow (x-1)(x-2)\geqslant 0\\ &\Rightarrow x^2-3x+2\geqslant 0. \end{aligned}$$

Proof by contradiction.
Suppose that $x^2-3x+2<0$ AND $x\leqslant 0$. Then,

$$\Rightarrow x^2<3x-2\leqslant -2$$

$$\Rightarrow x^2<0 \quad \sharp$$

*Proposition* $0<x<y \Rightarrow x^2<y^2$.
Proof by deduction:

$$\begin{aligned} 0<x<y &\Rightarrow (y-x)>0 \text{ AND } (y+x)>0\\ &\Rightarrow y^2-x^2=(y-x)(y+x)>0\\ &\Rightarrow y^2>x^2 \end{aligned}$$

Proof by contrapositive:

$$\begin{aligned} x^2\geqslant y^2 &\Rightarrow 0\leqslant x^2-y^2=(x+y)(x-y)\\ &\Rightarrow x-y\geqslant 0\\ &\Rightarrow x\geqslant y \end{aligned}$$

Proof by contradiction:

$$\begin{aligned} 0<x<y \text{ AND } x^2\geqslant y^2 &\Rightarrow x^2\geqslant y^2>xy\\ &\Rightarrow x(x-y)>0\\ &\Rightarrow 0<x<0 \quad \sharp \end{aligned}$$

## 1.5 Exercises

1. The opposite of the statement "all paper comes from rainforests" is (i) "some paper does not come from rainforests", (ii) "all paper does not come from rainforests" or (iii) "some paper comes from rainforests".

2. The converse of the statement "if you study you'll do well" is (i) "if you don't do well then you haven't studied", (ii) "if you do well then you have studied" or (iii) "if you don't study then you won't do well".

3. Show that for any statements $\phi$, $\psi$ and $\omega$:

   (a) $\phi$ OR NOT $\phi$ is always true.

   (b) $\phi$ AND NOT $\phi$ is always false.

   (c) NOT (NOT $\phi$) $\Leftrightarrow$ $\phi$.

   (d) $\phi$ AND $\psi$ $\Rightarrow$ $\phi$.

   (e) $\phi$ $\Rightarrow$ ($\psi$ $\Rightarrow$ $\phi$).

   (f) $\phi$ OR ($\psi$ AND $\omega$) $\Leftrightarrow$ ($\phi$ OR $\psi$) AND ($\phi$ OR $\omega$).

   (g) $\phi$ AND ($\psi$ OR $\omega$) $\Leftrightarrow$ ($\phi$ AND $\psi$) OR ($\phi$ AND $\omega$).

   (h) $\phi$ $\Rightarrow$ $\phi$ AND $\psi$ is the same as $\phi$ $\Rightarrow$ $\psi$.

   (i) $\phi$ OR ($\psi$ AND NOT $\phi$) is the same as $\phi$ OR $\psi$.

4. Give examples from everyday life where $\phi$ $\Rightarrow$ $\psi$ is true but $\psi$ $\Rightarrow$ $\phi$ is false. A common error in everyday conversation is to deduce from $\phi$ $\Rightarrow$ $\psi$ that NOT $\phi$ $\Rightarrow$ NOT $\psi$. Give examples from newspaper articles illustrating this error, and correct the mistakes.

5. Give your own examples of statements in which $\forall x\, \exists y \quad \phi_{x,y}$ is true but $\exists y\, \forall x \quad \phi_{x,y}$ is false. Can you find examples where $\exists y\, \forall x \quad \phi_{x,y}$ is true but $\forall x\, \exists y \quad \phi_{x,y}$ is false?

6. Show that the statement $\mathbf{u} \cdot \mathbf{v} = 0 \;\Rightarrow\; \mathbf{u} = 0$ OR $\mathbf{v} = 0$ is false by giving a counterexample.

7. Write a short computer program that gives a list of numbers $n$ which divide $2^n - 2$. Show that they are all prime numbers up to $n = 341$, which is not.

# 2 The Integers

## 2.1 The Natural Numbers

We first define the natural numbers, denoted by $\mathbb{N}$.

The natural number 0 is defined to be the empty set $\{\ \}$. The natural number 1 is defined to be a set with a single element. The number 2 is defined to be a set with two elements, and so on.

In order that we don't run out of symbols, we can define the natural numbers as follows: **Definition** The set of natural numbers consists of the elements (numbers):

$$\begin{aligned} \mathbf{0} &= \{\ \} \\ \mathbf{1} &= \{\, 0 \,\} \\ \mathbf{2} &= \{\, 0, 1 \,\} \\ \mathbf{3} &= \{\, 0, 1, 2 \,\} \\ &\dots \end{aligned}$$

Every natural number $n$ has a *successive* natural number $n^+ = \{\, 0, 1, \dots, n \,\}$. For example, $0^+ = 1$, $23^+ = 24$. It is assumed that each successor number is different from all the other previous natural numbers, so that the process never ends. Conversely, every natural number is a successor of the previous number, *except* 0.

Notice that these numbers have an order starting from 0, followed by 1, followed by 2 and so on. We denote this by using the symbol $\leqslant$. The statement $m \leqslant n$ means that the number $n$ occurs to the right of $m$ in this order.

### 2.1.1 Principle of Induction

$\mathbb{N}$ satisfies the following principle, called mathematical induction.

A statement $\phi_n$ about natural numbers, is true for all natural numbers $n$, if it can be shown that

(i) $\phi_0$ is true

(ii) $\phi_n \Rightarrow \phi_{n^+}$.

In other words, if one proves that when the statement is true for the number $n$ then it follows that it is also true for the successive number $n^+$, and if we can start the whole inductive process by proving the statement for $n = 0$, then $\phi$ would be true for all $n$.

As an application of mathematical induction, we shall prove the following useful theorem.

**Theorem** A

**Every nonempty set of natural numbers has a smallest element.**

$$A \neq \varnothing \quad \Rightarrow \quad \exists m \in A \; \forall n \in A \quad m \leqslant n$$

Proof. We shall prove the statement by proving its contrapositive.
Suppose that $A$ has no smallest element. This means

$$\forall m \in A \; \exists n \in A \quad m > n.$$

Now, suppose for a moment, that 0 is an element of $A$. We already know that 0 is the smallest natural number. If $0 \in A$ it would follow that 0 is the smallest element in $A$. But we are supposing that $A$ has no smallest element. Therefore, it cannot be that $0 \in A$. This shows that $0 \notin A$.

Now suppose that, by the induction principle, we have already shown $0, \ldots, n \notin A$. Can $n^+$ be an element of $A$? Suppose it were. We know that 0 up to $n$ are not in $A$. Therefore, the elements of $A$ are greater than $n$ i.e. $\forall m \in A \quad m \geqslant n^+$. So $n^+$ would be the smallest element. This contradicts our original assumption, therefore $n^+ \notin A$.

Combining our results and using the principle of induction, we get that $\forall n \quad n \notin A$. The set $A$ has no elements, it is the empty set. We have therefore shown that if a set of natural numbers has no smallest element then it must be empty. Equivalently if a set of natural numbers is nonempty it must have a smallest element.

□

## 2.2 The Integers

The set of integers consists of two copies of the set of natural numbers $\mathbb{N}$, one copy called the **positive** integers, and the other the **negative** integers. We distinguish between the two by placing the marks + or − in front of the numbers, although in practice we usually omit the + sign, taking it

for granted. Moreover we identify $-0$ with $+0$ so that it provides the link between the two sets.

**Definition** The set of **integers** is defined by

$$\mathbb{Z} = +\mathbb{N} \cup -\mathbb{N}$$
$$+0 = -0$$

Note that by this definition, every integer is automatically either positive or negative.

In order that we can assert any statements about integers, we need to be given some statements about $\mathbb{Z}$ that we take to be true. These initial statements are called **axioms**, in our case about the integers. Which statements we take to be our axioms is quite arbitrary, and they vary from author to author, but as a minimum they should capture enough information about the integers. The axioms that we will take can in fact be proved using even simpler axioms: the interested reader can be recommended the book *Naive Set Theory* by Halmos.

### 2.2.1 Axioms about the Integers

We shall assume the following axioms.

The set of integers $\mathbb{Z}$ have two operations of **addition** and **multiplication** which give an integer each time any two integers are added or multiplied. We denote the added integers by $m + n$ and the multiplied integers by $m.n$ (although the . or $\times$ is usually omitted when it isn't confusing).

There is also a statement called the **less than** statement which says when one integer is less than or equal to another integer. We denote such a statement by $m \leqslant n$.

Axioms about addition:

| | | |
|---|---|---|
| 1. Associativity | $\forall a, b, c \in \mathbb{Z}$ | $(a + b) + c = a + (b + c)$ |
| 2. Commutativity | $\forall a, b \in \mathbb{Z}$ | $a + b = b + a$ |
| 3. Identity (zero) | $\forall a \in \mathbb{Z}$ | $a + 0 = a$ |
| 4. Inverse (negative) | $\forall a \in \mathbb{Z}$ | $a + (-a) = 0$ |

Axioms about multiplication:

| | | |
|---|---|---|
| 5. Associativity | $\forall a, b, c \in \mathbb{Z}$ | $(ab)c = a(bc)$ |
| 6. Commutativity | $\forall a, b \in \mathbb{Z}$ | $ab = ba$ |
| 7. Identity (unity) | $\forall a \in \mathbb{Z}$ | $a.1 = a$ |
| 8. Distributivity | $\forall a, b, c \in \mathbb{Z}$ | $a.(b + c) = ab + ac$ |

Axioms about *less than*:

| | | |
|---|---|---|
| 9. Transitivity | $\forall a, b, c \in \mathbb{Z}$ | $a \leqslant b$ AND $b \leqslant c \Rightarrow a \leqslant c$ |
| 10. Linear Order | $\forall a, b \in \mathbb{Z}$ | $a < b$ OR $a = b$ OR $a > b$ |
| 11. | $\forall a, b, c \in \mathbb{Z}$ | $a \leqslant b \Rightarrow a + c \leqslant b + c$ |
| 12. | $\forall a, b \in \mathbb{Z} c > 0$ | $a \leqslant b \Rightarrow a.c \leqslant b.c$ |

From these axioms we can start deducing other properties about the integers. Following is a list of propositions, which we usually have assumed, but that we are now proving, using the axioms.

*Proposition* 2.2.1

**There is only one zero.**

Proof. Suppose that $N$ is an integer with the property that $\forall a \in \mathbb{Z} \quad a + N = a$. By using axiom 3, then axiom 2, and then the above property of $N$, we can say

$$N = N + 0 = 0 + N = 0$$

Therefore $N = 0$: 0 is the only integer which can act as zero in the sense of axiom 3.

□

*Proposition* 2.2.2

**Each integer $a$ has only one additive inverse, $-a$.**

Proof. Let $a$ be any integer. Suppose that $a'$ is another integer with the property $a + a' = 0$. We would like to show that $a' = -a$.

$$\begin{array}{lll} a' & = a' + 0 & \text{by axiom 3} \\ & = a' + (a + (-a)) & \text{by axiom 4} \\ & = (a' + a) + (-a) & \text{by associativity} \\ & = (a + a') + (-a) & \text{by commutativity} \\ & = 0 + (-a) & \text{by the assumed property of } a' \\ & = (-a) + 0 & \text{by commutativity} \\ & = -a & \text{by axiom 3} \end{array}$$

Therefore $a' = -a$ : every integer has only one additive inverse, its negative.

□

We shall not always prove things in such detail, each time quoting the relevant axiom, but it should be appreciated that for each step there must be a reason for making the assertion.

*Proposition* 2.2.3

$$a + c = b \quad \Rightarrow \quad a = b - c$$

Note that $b - c$ is just shorthand for $b + (-c)$.

Proof.

$$\begin{array}{rll} a + c & = b & \\ \text{Therefore, } (a + c) + x & = b + x & \text{using axiom 11 twice} \\ \text{In particular, } (a + c) + (-c) & = b - c & \\ a + (c - c) & = b - c & \text{associativity} \\ a + 0 & = b - c & \text{by axiom 4} \\ a & = b - c & \text{by axiom 3} \end{array}$$

□

Hence every integer equation $x + c = b$ has a solution $x = b - c$. This is one of the reasons that negatives are useful. There are no natural numbers that solve the equation $x + 1 = 0$, but there are integers that do, as this proposition asserts.

*Proposition* 2.2.4

$$a + c = b + c \;\Rightarrow\; a = b$$

"We can cancel an integer on both sides of the equation"

Proof.

$$\begin{aligned} a+c &= b+c \\ a &= (b+c)-c && \text{by the previous propostion} \\ &= b+(c-c) && \text{associativity} \\ &= b+0 && \text{by axiom 4} \\ &= b && \text{by axiom 3} \end{aligned}$$

□

*Proposition* 2.2.5

$$a.0 = 0$$

Proof.

$$\begin{aligned} a.0+a.b &= a.(0+b) && \text{by distributivity} \\ &= ab && \text{by axioms 3 and 2} \\ &= 0+ab && \text{by axiom 3 and 2 again} \\ \therefore\ a.0 &= 0 && \text{by cancelling the } ab \end{aligned}$$

□

*Proposition* 2.2.6

$$(-a).b = -(ab) = a(-b)$$

Proof.

$$\begin{aligned} ab+(-a)b &= (a-a)b && \text{by distributivity} \\ &= 0.b && \text{by axiom 4} \\ &= 0 && \text{by the previous proposition} \end{aligned}$$

Therefore, transferring $ab$ on the other side of the equation, which we can do by one of the propositions,

$$(-a)b = -(ab)$$

□

One can similarly prove that $a(-b) = -(ab)$. Try it!

*Proposition* 2.2.7

$$-(-a) = a$$

Proof.

| | | |
|---|---|---|
| $a - a$ | $= 0$ | by axiom 4 |
| | $= (-a) + -(-a)$ | again by axiom 4 |
| | $= -(-a) + (-a)$ | commutativity |

Therefore, cancelling the $-a$ on both sides,

$$a = -(-a)$$

□

*Proposition* 2.2.8

$$(-a).(-b) = ab$$

Proof.

| | | |
|---|---|---|
| $(-a).x$ | $= -(ax)$ | by proposition 2.9 |
| In particular, $(-a)(-b)$ | $= -(a(-b))$ | |
| | $= -(-(ab))$ | by proposition 2.9 |
| | $= ab$ | by proposition 2.10 |

□

*Proposition* 2.2.9

$$c \leqslant 0 \text{ AND } a \leqslant b \;\Rightarrow\; ac \geqslant bc$$

Proof.

$$\begin{aligned} c &\leqslant 0 \\ \text{Therefore, } 0 = c - c &\leqslant 0 - c && \text{by axioms 4 and 11} \\ 0 &\leqslant -c && \text{by axiom 3} \\ \therefore,\ a(-c) &\leqslant b(-c) && \text{by axiom 12} \\ -ac &\leqslant -bc && \text{by proposition 2.9} \\ bc &\leqslant ac && \text{by axiom 11,} \end{aligned}$$

adding $ac$ and $bc$ on both sides and simplifying.

□

Taking $c = -1$ shows that if $a \leqslant b$ then $-b \leqslant -a$. Hence the negative integers are ordered in reverse of the positive ones i.e.

$$\ldots -2 \quad -1 \quad 0 \quad 1 \quad 2 \ldots$$

*Proposition* 2.2.10

$$a^2 = a.a \geqslant 0$$

Proof. We know, by axiom 10, that either $a > 0$ or $a = 0$ or $a < 0$.
If $a = 0$ then $a^2 = 0.0 = 0$ by proposition 2.8
If $a > 0$ then $a.a \geqslant a.0 = 0$ by axiom 12.
If $a < 0$ then $a.a \geqslant a.0 = 0$ by propositions 2.8 and 2.12

□

**Definition** The **modulus** of an integer $a$ is defined to be

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

Check that the following are true:

$$\begin{aligned} &|a| \geqslant 0 \\ &|a|^2 = a^2 \\ &|a| = 0 \Leftrightarrow a = 0 \\ &|a + b| \leqslant |a| + |b| \end{aligned}$$

*Proposition* 2.2.11

$$ab = 0 \;\Rightarrow\quad a = 0 \quad \text{OR} \quad b = 0$$

Proof. Suppose that NOT ($a = 0$ OR $b = 0$). That is suppose that $a \neq 0$ AND $b \neq 0$. Therefore we have either $a > 0$ or $a < 0$ and similarly $b > 0$ or $b < 0$. In any case, $|a| > 0$ and $|b| > 0$. It follows that

$$|ab| = |a|.|b| > 0.|b| = 0.$$

Therefore, $|ab| > 0$, which means that either $ab > 0$ or $ab < 0$ but not $ab = 0$. The conclusion is that if $a \neq 0$ and $b \neq 0$ then $ab \neq 0$. This is in fact what we had to prove.

□

This proposition allows us to deduce from $(x-1)(x-2) = 0$ that $x = 1$ or $x = 2$.

*Proposition* 2.2.12

$$\textbf{If } c \neq 0 \textbf{ then } ca = cb \;\Rightarrow\; a = b\textbf{.}$$

Proof.

$$\begin{aligned} ca &= cb \\ \therefore\; ca - cb &= 0 \quad \text{by proposition 2.2.3} \\ c(a-b) &= 0 \quad \text{by distributivity} \end{aligned}$$

Therefore, either $c = 0$ or $a - b = 0$ by the previous proposition. But we know that $c \neq 0$. Therefore it must be the case that $a - b = 0$, from which follows that $a = b$.

□

## 2.3 Factors

**Definition** We say that $a$ is a **factor** of $b$, written as $a|b$, when

$$\exists c \in \mathbb{Z} \quad b = ac$$

The terms $a$ **divides** $b$, $a$ is a **divisor** of $b$, $b$ is a **multiple** of $a$ all mean the same as $a$ is a factor of $b$.

**Definition** An integer $a$ is **even** when $2|a$, otherwise it is called **odd** i.e. $2 \not| a$.

Every integer $b$ has a list of factors: in particular, 1 is always a factor because $b = b.1$.

*Proposition* 2.3.1

1. **If** $a|b$ **and** $b|c$ **then** $a|c$
2. **If** $a|b$ **and** $a|c$ **then** $a|(eb + fc)$

Proof. 1. $a|b$ means that $b = ax$ for some $x \in \mathbb{Z}$. Similarly $b|c$ means $c = by$ for some $y \in \mathbb{Z}$. Combining the two, we get that

$$c = by = (ax)y = a(xy)$$

Therefore, $a$ multiplied by some integer gives $c$, i.e. $a|c$ as required.

2. $a|b$ means that $b = ax$ for some $x$. $a|c$ means that $c = ay$ for some integer $y$. Therefore, for any integers $e$ and $f$,

$$eb + fc = e(ax) + f(ay) = a(ex + fy)$$

Again, $a$ multiplied by an integer gives $eb + fc$ i.e. $a|(ef + fc)$.

□

**Definition** $c$ is a **common factor** of $a$ and $b$ when $c|a$ and $c|b$.
$c$ is the **highest common factor** of $a$ and $b$, denoted by hcf($a$,$b$), when
(i) $c$ is a common factor i.e. $c|a$ and $c|b$,
(ii) every other common factor of $a$ and $b$ is a factor of $c$ i.e.

$$d|a \text{ AND } d|b \Rightarrow d|c$$

**Theorem** B

**The Division Algorithm.**
**For any integers $a$, $b$ with $b \neq 0$, there exist integers $q$ called the quotient and $r$ called the remainder, such that,**

$$a = qb + r \quad 0 \leqslant r < |b|$$

Proof. Let us consider first the case when both $a$ and $b$ are strictly positive.

Define the set $A = \{a - mb \geqslant 0\} = \{a, a - b, \dots\}$. $A$ is nonempty since at least it contains $a$. Therefore we can apply theorem 2.2, and assert that $A$ has a smallest element, $a - qb$ which we shall call $r$. Since $r$ is an element of $A$, it satisfies $r \geqslant 0$. Now consider the integer $a - (q+1)b$. It is smaller than $r$ since in fact it is equal to $r - b$ and $b > 0$. Since $r$ is the *smallest* element of $A$, this new integer cannot be an element of $A$. Therefore it is negative ie $r - b < 0$.

For the other cases concerning $a$ and $b$, we can make use of what we have proven up to now.

When $a > 0$ but $b < 0$, we get that $a = q|b| + r$ which we can rearrange as $a = (-q)b + r$ with $0 \leqslant r < |b|$.

When $a < 0$ but $b > 0$, we get $-a = |a| = qb + r$. If $r$ happens to be 0, then we get $a = (-q)b$; otherwise, multiplying by $-1$ gives us $a = (-q)b - r = (-q-1)b + (b - r)$ where the new remainder satisfies $0 < (b - r) < b$.

When $a < 0$ and $b < 0$, we get $-a = |a| = q|b| + r$, which implies that $a = qb - r = (q+1)b + (|b| - r)$ with $0 \leqslant |b| - r < |b|$.

□

The division algorithm is, in a sense, a generalization of the idea of factors: if $b$ is a factor of $a$ then it will have a zero remainder when $a$ is "divided" by $b$. If we can show that when $a$ is divided by $b$ it leaves a remainder of 0, then we would have shown that $a|b$. We will illustrate this in the following proposition about highest common factors.

*Proposition* 2.3.2

1. **any two integers have a highest common factor;**
2. **the h.c.f. of $a$, $b$ can be written as a combination of $a$ and $b$; i.e. $hcf(a,b) = sa + tb$ for some $s$, $t \in \mathbb{Z}$.**

Proof. Let $A = \{ma + nb > 0 : m, n \in \mathbb{Z}\}$.

Then $A \neq \varnothing$ since either $a$ or $-a$ is surely in $A$. Therefore $A$ is a nonempty subset of $\mathbb{N}$. Therefore, by theorem 2.2, it has a minimum which we shall call $c$.

That is, $c$ is the smallest element of $A$. But $A$ consists of positive combinations of $a$ and $b$. Therefore $c$ must be positive and is of the form $sa + tb$ for some integers $s, t$.

Claim: $c|a$, i.e. *$c$ is a factor of $a$*

since, applying the division algorithm to $a$, $c$, we get

$$\begin{aligned} a &= qc + r & 0 \leqslant r < c \\ &= q(sa + tb) + r \\ \text{hence, } \quad r &= (1 - qs)a - qtb \end{aligned}$$

We find that the remainder $r$ is also a combination of $a$ and $b$, and if it were strictly positive it would be an element of $A$. However, since it is strictly smaller than $c$, which is the smallest element of $A$, $r$ cannot possibly be in $A$. Therefore it is not strictly positive. But we know that $r \geqslant 0$. That leaves the only possibility of $r = 0$: there is no remainder, $a = qc$ i.e. $c|a$.

Similarly one can show that $c|b$ (try it by first dividing $b$ by $c$). Hence, $c$ is a common factor of $a$ and $b$.

Suppose $d$ is any other common factor: $d|a$ and $d|b$. Therefore, by 2.20(2), $d|(sa + tb)$ i.e. $d|c$.

We have shown that $c$ is the highest common factor of $a$ and $b$.

□

This last proposition assures us that the highest common factor of any two integers exists, it does not tell us how to find it.

### 2.3.1 Euclidean Algorithm

To find the h.c.f. of $a$ and $b$, apply the division algorithm repeatedly to $a$ and $b$ and the subsequent remainders until there are no more remainders. The last remainder is the h.c.f.

$$\begin{aligned}
a &= q_0 b + r_1 && \ldots(1) && \text{where } 0 \leqslant r_1 < |b| \\
b &= q_1 r_1 + r_2 && \ldots(2) && 0 \leqslant r_2 < r_1 \\
r_1 &= q_2 r_2 + r_3 && \ldots(3) && 0 \leqslant r_3 < r_2 \\
&\ldots \\
r_{n-2} &= q_{n-1} r_{n-1} + r_n && \ldots(n-1) && 0 \leqslant r_n < r_{n-1} \\
r_{n-1} &= q_n r_n && \ldots(n)
\end{aligned}$$

At some point, there *must* be a zero remainder because the $r_n$'s form a strictly decreasing sequence of natural numbers.

But why is $r_n$ the h.c.f. of $a$ and $b$? Let us show that indeed it is a common factor of both integers and that every other common factor must divide $r_n$.

From equation $n$, we have that $r_n | r_{n-1}$, and so $r_n | q_{n-1} r_{n-1}$. From equation $n-1$, we therefore deduce that $r_n | r_{n-2}$. Continuing with this line of reasoning we can use each equation in order, and deduce that $r_n | r_k$ for all $k$. In particular, $r_n | r_1$ and $r_n | r_2$, and therefore, from equation 2, $r_n | b$ and from equation 1, $r_n | a$.

Let $c$ be any other common factor of $a$ and $b$. Therefore $c | (a - q_0 b)$ (why?), but this means $c | r_1$ from equation 1. Similarly $c | (b - q_1 r_1)$ i.e. $c | r_2$. Continuing in this way, we find that $c | r_k$ for all $k$; in particular $c | r_n$.

Example: Find the h.c.f. of 182527 and 100939.

$$\begin{aligned}
182527 &= 1 \times 100939 + 81588 && \ldots(1) \\
100939 &= 1 \times 81588 + 19351 && \ldots(2) \\
81588 &= 4 \times 19351 + 4184 && \ldots(3) \\
19351 &= 4 \times 4184 + 2615 && \ldots(4) \\
4184 &= 1 \times 2615 + 1569 && \ldots(5) \\
2615 &= 1 \times 1569 + 1046 && \ldots(6) \\
1569 &= 1 \times 1046 + 523 && \ldots(7) \\
1046 &= 2 \times 523
\end{aligned}$$

$\therefore$ h.c.f.(182527,100939)=523.

This algorithm also allows us to write the h.c.f. in terms of $a$ and $b$. In

the example above, we start with the penultimate equation 7.

$$\begin{aligned}
523 &= 1569 - 1046 && \text{from 7}\\
&= 1569 - (2615 - 1569) && \text{from 6}\\
&= 2 \times 1569 - 2615 && \text{rearranging}\\
&= 2 \times (4184 - 2615) - 2615 && \text{from 5}\\
&= -3 \times 2615 + 2 \times 4184 && \text{rearranging}\\
&-3 \times (19351 - 4 \times 4184) + 2 \times 4184 && \text{from 4}\\
&= 14 \times 4184 - 3 \times 19351 && \text{rearranging}\\
&= 14 \times (81588 - 4 \times 19351) - 3 \times 19351 && \text{from 3}\\
&= -59 \times 19351 + 14 \times 81588 && \text{rearranging}\\
&= -59 \times (100939 - 81588) + 14 \times 81588 && \text{from 2}\\
&= 73 \times 81588 - 59 \times 100939 && \text{rearranging}\\
&= 73 \times (182527 - 100939) - 59 \times 100939 && \text{from 1}\\
&= 73 \times 182527 - 132 \times 100939
\end{aligned}$$

Exercises: Find the h.c.f. of 276 and 161.

Find the h.c.f. of 115 and 46, and write it as a combination of the two integers.

### 2.3.2 Solving integer equations

Finding the h.c.f. is important to solve equations of the form $ax + by = c$ where $a, b, c$ are integers and $x, y$ are required to be integers.

Let us investigate the equation first. Suppose $d$ is the h.c.f. of $a$ and $b$. Then $d|(xa + yb)$ since the right-hand side is a combination of $a$ and $b$. Therefore $d|c$ must be true, if there is a solution (i.e. if $x$ and $y$ exist).

The first thing to do, therefore, is to find the h.c.f. of $a$ and $b$ and check whether it divides $c$. If not, it cannot possibly have a solution. If it does divide it, we can hope for a solution. Using the Euclidean algorithm, write $d$ as a combination of $a$ and $b$, say, $d = sa + tb$. Now, $d|c$ i.e. $c = md = (ms)a + (mt)b$. We have thus found a solution $x = ms$ and $y = mt$. Note that this is just one solution, and there could be others.

Example: Solve $182527x + 100939y = 1046$ for $x, y$ integers.

Solution: Apply the Euclidean algorithm to find hcf(182527,100939). We have already done this, and found the hcf to be 523. Now, let us check whether 523|1046; this is in fact true as $1046 = 2 \times 523$. Therefore, the equation *does* have a solution. We have to write 523 as a combination of

the two integers. We have done this and found that $523 = 73 \times 182527 - 132 \times 100939$. Hence, $1046 = 2 \times 523 = 2 \times (73 \times 182527 - 132 \times 100939) = 146 \times 182527 - 264 \times 100939$. One solution is therefore, $x = 146, y = -264$.

## 2.4 Prime Numbers

**Definition** An integer $a$ is called **prime** (also called **irreducible**), when

1. it is not 0 or $\pm 1$;
2. its only factors are $\pm 1$ and $\pm a$ i.e.

$$b|a \;\Rightarrow\; b = \pm 1 \;\text{ OR }\; b = \pm a$$

An integer which is not prime is called **composite**.

The first few (positive) primes are 2, 3, 5, 7, 11 etc.

**Definition** Two integers are called **coprime** if their only common factors are $\pm 1$.

i.e. $a$, $b$ are coprime $\Leftrightarrow hcf(a, b) = 1$.

For example, 15 and 16 are coprime as they don't have common factors except $\pm 1$.

Note that if $p$ is a prime number and $p \not| a$ then $p$ and $a$ are coprime; since: the factors of the prime number $p$ are $\pm 1$ and $\pm p$, and $\pm p$ are not factors of $a$ (given), so the common factors can only be $\pm 1$.

*Proposition* 2.4.1

**Let $p$ be a prime number; then**

$$p|ab \;\Rightarrow\; p|a \text{ or } p|b.$$

Proof. For sure, $p|a$ or $p \not| a$. One of the two must be true.

If $p \not| a$, then $p$ and $a$ are coprime (by the note above) i.e. hcf($a$, $b$)= 1. Using Prop. 2.23 we can write 1 as a combination of $p$ and $a$, $1 = sp + ta$. Multiplying by $b$ gives $b = spb + tab = (sb)p + (t)ab$. But $p|ab$ (given), hence $p|b$ as $b$ is a combination of $p$ and $ab$.

Therefore, either $p|a$ or $p|b$.

□

**Theorem** C

**Fundamental Theorem of Arithmetic**
**Any integer $a$, except 0,$\pm 1$, is the unique product of positive primes and $\pm 1$ (depending on the sign of $a$):**

$$a = p_1 \dots p_r$$

**where $p_i$ are unique primes.**

Proof. We first show that $a$ is a product of primes. Note that we need only prove this for positive integers. Let us prove it by induction on $n$.

When $n = 2$, 2 is prime; the prime decomposition is trivial ie $2 = 1 \times 2$.

Suppose every positive integer up to $n$ has a prime decomposition, and we need to consider the integer $n + 1$.

$n + 1$ is either a prime number — its prime decomposition is just itself (like the case with 2);

or $n+1$ is composite; ie. $n+1 = ab$ where $a, b \neq 1$. Therefore $a, b < n+1$ (otherwise their product would be larger than $n + 1$); so both $a$ and $b$ have a prime decomposition by the induction assumption ie $a = p_1 \dots p_k$ and $b = q_1 \dots q_r$ where the $p_i$ and $q_j$ are prime numbers. Hence $n + 1 = ab = p_1 \dots p_k q_1 \dots q_r$, a product of primes.

In any case, $n + 1$ is a product of primes.

Let us show that when $a = p_1 \dots p_r$ the prime numbers $p_i$ are unique. Let $a = q_1 \dots q_s$ be another prime decomposition of $a$. We have $a = p_1 \dots p_r = q_1 \dots q_s$. It can happen that some of the primes are common in both decompositions, say, $p_1 = q_1$ up to $p_t = q_t$ (of course we must allow the case that none are common, $t = 0$). Cancel these primes from both lists to get $p_{t+1} \cdots p_r = q_{t+1} \cdots q_s$.

Suppose that not all the primes are common, so that either there remain some primes $p_i$ or $q_j$ on either side of the equation. Without loss of generality, let us assume that $q_s$ remains; we find that $q_s | (p_{t+1} \dots p_r)$. Notice it can't be the case that the right hand side $p_{t+1} \cdots p_r = 1$ since no prime can be a factor of 1. From the definition of a prime number, $q_s$ must divide one of the numbers $p_{t+1}, \dots, p_r$. By relabelling the $p_i$'s if necessary, we can assume that $q_s | p_r$. But $p_r$ is itself a prime: its only factors are $\pm 1$ and $\pm p_r$; in this case, since $q_s$ is a factor of $p_r$, it must equal it $q_s = p_r$. Hence we have found that

one of the primes in both lists are the same, when we have already eliminated all such common primes. This is a contradiction.

Hence the only possibility is that $r = s$ and the primes are exactly paired up: $p_1 = q_1$, $p_2 = q_2$, $\ldots$, $p_r = q_r$ ie the two prime decompositions are in fact the same.

□

**Theorem** D

**The number of primes is infinite.**

Proof. Suppose there are a finite number of primes $2, 3, \ldots, p_N$.

Let $a := 2 \times 3 \times \ldots \times p_N + 1$. By the fundamental theorem of arithmetic that we have just proved, we know that $a$ is the unique product of primes, say, $a = q_1 \ldots q_r$. The $q_i$'s are primes and therefore must be somewhere in the list $2, 3, \ldots, p_N$. For example, $q_1 = p_s$.

Now, $q_1$ is a factor of $a$ and also of $2 \times 3 \times \ldots \times p_N$; hence it is a factor of their difference $q_1 | (a - 2.3 \ldots p_N) = 1$. But it is impossible for the prime $q_1$ to divide 1.

Hence this contradiction implies that there must be an infinite number of primes.

□

## 2.5 Exercises

1. Show that $a$ is even $\Leftrightarrow$ $a^2$ is even.

   That is, show that

   (a) $a$ is even $\Rightarrow$ $a^2$ is even

   (b) $a$ is odd $\Rightarrow$ $a^2$ is odd.

2. Show that if the integer $a$ is of the form $3k+1$ for some integer $k$, then so is $a^2$.

3. Use induction to prove that for any natural numbers $m, n \in \mathbb{N}$, $m+n = n+m$. Deduce that for any integers $a, b \in \mathbb{Z}$, $a+b = b+a$. Similarly prove that $0+m = m$ and $1m = m$.

4. Prove carefully that for any integers $a, b \in \mathbb{Z}$, (i) $-(a-b) = b-a$, (ii) $(a-b)c = ac-bc$, (iii) $ab = 1 \;\Rightarrow\; a = b = 1$ OR $a = b = -1$.

5. Prove that if $a|b$ and $b|a$ then $a = \pm b$.

6. Prove or disprove: let $a, b \in \mathbb{Z}$; $3|(a^2+b^2) \;\Rightarrow\; 3|a$ AND $3|b$.

7. Prove by induction on $n$ that $a-b|a^n - b^n$.

8. Find the highest common factor of 582 and 2425; and write it down in the form $582s + 2425t$ for some $s, t \in Z$; repeat for 285 and 347.

9. Prove that for $a, b, c$ integers, if $a, b$ are coprime and $a|bc$ then $a|c$.

10. Show that the hcf of an integer is unique up to sign i.e. if $c$ and $d$ are both hcf's of $a, b$ then $c = \pm d$.

11. Solve for $x, y \in \mathbb{Z}$, $57x + 87y = 9$; show that the equation $9797m + 9991n = 2$ has no integer solutions; find the values of $d \in \mathbb{Z}$ for which $6557x + 7031y = d$ has integer solutions.

12. Using only the axioms for the integers, prove that

    (a) $ax = a$ and $a \neq 0 \;\Rightarrow\; x = 1$

    (b) $x^2 - y^2 = (x-y)(x+y)$

    (c) $x^2 = y^2 \;\Rightarrow\; x = y$ or $x = -y$

13. Show that if $x \neq 0$ then $x^2 > 0$. Deduce that $1 > 0$.

14. If $c|(a+b)$ and $a, b$ are coprime, show that $a, c$ are coprime.

15. Prove that if $a, b$ are coprime and $ab = c^2$ then $a, b$ must be squares themselves. Deduce that the product of two primes can never give a square.

16. Show that the hcf of $a = 7n+4$ and $b = 9n+5$ must be 1 (Hint: show that the hcf divides $9a - 7b$).

17. Find the prime decomposition of (i) 499200, (ii*) 499201.

18. * Suppose that $p$ has the property that if it is a factor of $ab$ then it must be a factor of $a$ or of $b$ (ie $p|ab \Rightarrow p|a$ OR $p|b$). Show that it is a prime number.

19. * Show that there are infinitely many primes of the form $4k+3$. (Hint: suppose that $p_1, p_2, \ldots, p_n$ are the only primes of this form. Let $N = 4p_1 \ldots p_n - 1$. $N$ has its prime decomposition $N = q_1 \ldots q_r$ for some primes $q_i$. Show that among the $q_i$'s there must be exactly one prime of type $4k+3$ and get a contradiction.)

20. In the Division Algorithm, where $a = qb + r \quad 0 \leqslant r < |b|$, show that, given $a$ and $b$, the quotient $q$ and the remainder $r$ are unique. i.e. show that if $a = q_1 b + r_1 = q_2 b + r_2$ with $0 \leqslant r_1, r_2 < |b|$, then $q_1 = q_2$ and $r_1 = r_2$.

21. Define $\binom{n}{m} = \dfrac{n!}{m!(n-m)!}$. Prove by induction on $n$ (keeping $m$ fixed) that $\binom{n+1}{m} = \binom{n}{m} + \binom{n}{m-1}$. Hence prove the binomial theorem, again by induction on $n$,

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

22. What is the largest prime number that you can prove is prime? (Note: Of course, there is no largest prime; Hint: if a number $n$ is not prime then it is divisible by an integer smaller than $\sqrt{n}$.)

23. Write a computer program which defines $N = 2.3.5.7.11 \ldots 97$, and then gives the highest common factor of $N$ and any other integer $M$. Use it further to find the prime factor decomposition of (fairly small) integers, say 499201.

# 3 Rational Numbers

While the natural numbers and integers are good at describing "whole" objects, they cannot be used for "measurements" because these often come in "fractions"; we usually wish to measure something in arbitrarily small step values to get accurate measurements. This means that we want a unit of measurement $a$ such that for any given object of size say $b$, we can measure $b$ using $a$ as $b = na$. But the integers are inadequate for such requirements e.g. $8 = 5n$ has no integer solutions. We need new numbers to tackle this situation.

**Definition** A **rational number** $q$ is a pair of integers $a, b \in \mathbb{Z}$ with $b \neq 0$.

The first integer is called the **numerator** of $q$, while the second integer is called the **denominator** of $q$.

We usually write the pair as $a/b$ or $\frac{a}{b}$ to distinguish between them. The rational numbers of the form $\frac{a}{1}$ are simply written as $a$.

**Definition** Two rational numbers $p, q$ are **equal** when

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc \text{ as integers}$$

The **addition** of $p$ and $q$ is defined by,

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

The **product** (or *multiplication*) of $p$ and $q$ is defined by

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

$p$ is **less than or equal** to $q$ when, for $b$ and $d$ positive integers,

$$\frac{a}{b} \leqslant \frac{c}{d} \Leftrightarrow ad \leqslant bc \text{ as integers}$$

Notes: 1. The denominator in the definitions of $p + q$ and $pq$ is non-zero as both $b$ and $d$ are non-zero.

2. The relations $p < q, p \geqslant q, p > q$ are defined in similar ways.

3. From the definition of equality, we find that $\frac{a}{b} = \frac{-a}{-b}$. Therefore, we can always assume the denominator to be a *positive* integer; if it is not, we can multiply the numerator and denominator by $-1$, to make it positive.

4. Also, $-\frac{a}{b} = \frac{-a}{b}$, since $-1 \cdot \frac{a}{b} = \frac{-a}{b}$.

5. The rational numbers $0/b$ are all equal to 0: $\frac{0}{b} = \frac{0}{1}$ since $0 \times 1 = 0 = 0b$.

6. Any rational number $\frac{a}{b}$ is equal to another $\frac{c}{d}$ with $c, d$ coprime. Suppose $a, b$ have a common factor $e$, then $a = ec$ and $b = ed$; therefore $ad = (ec)d = c(ed) = cb$ ie $\frac{a}{b} = \frac{c}{d}$. We can therefore eliminate any common factors from $a$ and $b$ until they are coprime. This process of removing the common factors is called *"reduction to lowest terms"*

**Properties of $\mathbb{Q}$**

Rational numbers have the following properties: $\forall p, q, r \in \mathbb{Q}$

| | | |
|---|---|---|
| associativity | $(p+q)+r = p+(q+r)$ | $(pq)r = p(qr)$ |
| commutativity | $p+q = q+p$ | $pq = qp$ |
| identities | $p+0 = p$ | $p1 = p$ |
| inverses | $p+(-p) = 0$ | $\forall p \neq 0 \quad p(p^{-1}) = 1$ |
| distributivity | $p(q+r) = pq + pr$ | |
| less than | $p \leqslant q \text{ and } q \leqslant r \;\Rightarrow\; p \leqslant r$ | |
| | $p < q \text{ or } p = q \text{ or } p > q$ | |
| | $\forall r \quad p \leqslant q \;\Rightarrow\; p+r \leqslant q+r, \forall r > 0 \quad p \leqslant q \;\Rightarrow\; pr \leqslant qr$ | |

Note that addition, multiplication and less than have all the properties of integers with the important addition that non-zero rational numbers have inverses $p^{-1}$.

Proof. Associativity:

$$\begin{aligned}(\frac{a}{b}+\frac{c}{d})+\frac{e}{f} &= \tfrac{ad+bc}{bd}+\tfrac{e}{f} = \tfrac{(ad+bc)f+e(bd)}{(bd)f} = \tfrac{a(df)+b(cf+ed)}{b(df)} \\ &= \tfrac{a}{b}+\tfrac{cf+ed}{df} = \tfrac{a}{b}+(\tfrac{c}{d}+\tfrac{e}{f}) \\ (\tfrac{a}{b}\tfrac{c}{d})\tfrac{e}{f} &= (\tfrac{ac}{bd})\tfrac{e}{f} = \tfrac{(ac)e}{(bd)f} = \tfrac{a(ce)}{b(df)} = \tfrac{a}{b}\tfrac{ce}{df} = \tfrac{a}{b}(\tfrac{c}{d}\tfrac{e}{f})\end{aligned}$$

Commutativity:

$$\frac{a}{b}+\frac{c}{d} = \frac{ad+bc}{bd} = \frac{bc+ad}{bd} = \frac{cb+da}{db} = \frac{c}{d}+\frac{a}{b}$$

$$\frac{a}{b}\frac{c}{d} = \frac{ac}{bd} = \frac{ca}{db} = \frac{c}{d}\frac{a}{b}$$

Identities:

$$\frac{a}{b}+\frac{0}{1}=\frac{a1+0b}{b1}=\frac{a+0}{b}=\frac{a}{b}$$

$$\frac{a}{b}\frac{1}{1}=\frac{a1}{b1}=\frac{a}{b}$$

Inverses: Given $p=\frac{a}{b}$, let $-p=\frac{-a}{b}$.

$$\frac{a}{b}+\frac{-a}{b}=\frac{ab-ba}{b^2}=\frac{0}{b^2}=0$$

Also let $p^{-1}=\frac{b}{a}$; this is possible when $a\neq 0$ ie when $p\neq 0$.

$$\frac{a}{b}\frac{b}{a}=\frac{ab}{ba}=\frac{1}{1}=1$$

Distributivity:

$$\begin{aligned}\tfrac{a}{b}(\tfrac{c}{d}+\tfrac{e}{f}) &= \tfrac{a}{b}\tfrac{cf+ed}{df}=\tfrac{a(cf+ed)}{b(df)}=\tfrac{acf+aed}{bdf}\\ &= \tfrac{acf}{bdf}+\tfrac{aed}{bdf}=\tfrac{ac}{bd}+\tfrac{ae}{bf}=\tfrac{a}{b}\tfrac{c}{d}+\tfrac{a}{b}\tfrac{e}{f}\end{aligned}$$

Less than: Given $\frac{a}{b}\leqslant\frac{c}{d}$ and $\frac{c}{d}\leqslant\frac{e}{f}$, assuming without loss of generality that all the denominators are positive, by definition these inequalities mean that $ad\leqslant bc$ and $cf\leqslant de$. Therefore, $(ad)f\leqslant bcf\leqslant(bd)e$, which can be written as $\frac{a}{b}=\frac{ad}{bd}\leqslant\frac{e}{f}$.

Finally, given $\frac{a}{b}$ and $\frac{c}{d}$, with $b,d>0$, consider the integers $ad$ and $bc$. One of $ad>bc$ or $ad=bc$ or $ad<bc$ must be true. Therefore, $\frac{a}{b}>\frac{c}{d}$ or $\frac{a}{b}=\frac{c}{d}$ or $\frac{a}{b}<\frac{c}{d}$ must be true.

The last two properties are left as exercises.

*Proposition* 3.0.1

**The equation $px=q$ where $p\neq 0,q$ are rational numbers, has a unique solution $x=p^{-1}q$.**

Proof. Suppose $x$ is a solution of the equation $px=q$. Then multiplying by $p^{-1}$ on both sides we get $x=1x=(p^{-1}p)x=p^{-1}(px)=p^{-1}q$.

Let us check that $p^{-1}q$ does indeed satisfy the equation: $px=p(p^{-1}q)=(pp^{-1})q=1q=q$.

□

One can prove other propositions, similar to the ones for integers, in the same way, since rational numbers have the same properties as integers; for example $0p = 0$, $-(-p) = p$, $pq = 0 \Rightarrow p = 0$ *or* $q = 0$.

*Proposition* 3.0.2

**$\mathbb{Q}$ is dense i.e. between any two rationals there is another rational.**

$$\forall p, q \in \mathbb{Q} : p < q \quad \exists r \quad p < r < q$$

Proof. Let $r$ be the average of $p$ and $q$.

□

Thus the set of rational numbers has no 'atoms' — you can keep on dividing an interval into smaller and smaller intervals.

**Corollary**

**(Archimedean Property for $\mathbb{Q}$)** $\forall \epsilon > 0 \; \exists n \in \mathbb{N} \quad 0 < \frac{1}{n} < \epsilon$

Proof. Between 0 and $\epsilon$ there is a rational number $0 < \frac{m}{n} < \epsilon$; hence $0 < \frac{1}{n} < \frac{m}{n} < \epsilon$.

□

Now that we can solve equations of type $ax = b$, we go on to study the equation $x^2 = a$ but we immediately run into problems:

*Proposition* 3.0.3

**There are no rational numbers that solve the equations $x^2 = 2$ and $x^2 = 3$.**

Proof.

(i) Suppose $x = \frac{a}{b}$ solves $x^2 = 2$ i.e. $(\frac{a}{b})^2 = 2$. Therefore $\frac{2}{1} = \frac{a}{b}\frac{a}{b} = \frac{a^2}{b^2}$. We can moreover assume that $x$ is in its lowest terms i.e. $a, b$ are coprime (if not, first reduce it).

Therefore, $a^2 = 2b^2 \quad \ldots(*)$. $a^2$ is even, and so $a$ must also be even (why? see the exercises for integers) i.e. $a = 2k$. Substituting into (*), we get $4k^2 = 2b^2$ which implies $b^2 = 2k^2$ an even number. Hence, again, $b$ is even. Thus, both $a$ and $b$ are even; but $a$,$b$ were presumed to be coprime with no common factors — contradiction: no rational number can satisfy the equation.

(ii) Suppose $x = \frac{a}{b}$ satisfies $x^2 = 3$, again assuming, without loss of generality, that $x$ is reduced to its lowest terms with $a$, $b$ coprime.

Then, $a^2 = 3b^2 \quad \ldots(**)$ is a multiple of 3. Claim: $a$ must also be a multiple of 3; since if $a = 3k + 1$ then $a^2 = (3k + 1)^2 = 9k^2 + 6k + 1$ not a multiple of 3; if $a = 3k + 2$ then $a^2 = (3k + 2)^2 = 9k^2 + 12k + 4$, again not a multiple of 3; therefore the only possibility is that $a = 3k$.

Substituting into (**), we get, $9k^2 = 3b^2$ and so $b^2 = 3k^2$; hence again, since $b^2$ is a multiple of 3, so must $b$ be a multiple of 3. But then both $a$ and $b$ have the common factor 3, which is a contradiction.

□

This kind of proof also shows that $x^2 = 5$, $x^2 = 7$ etc cannot have rational solutions. In fact most quadratic equations $ax^2 + bx + c = 0$ even with $a, b, c \in \mathbb{Z}$ do not have rational solutions.

## 3.1 Exercises

1. Prove that the equation $ax + b = c$, where $a \neq 0, b, c$ are rational numbers, has a unique solution.

2. Prove that $x^2 = 3$ has no rational solution. Deduce that $\sqrt[2n]{3}$ is irrational.

3. If $\frac{a}{b}$ and $\frac{c}{d}$ are two rational numbers, show that $\frac{a+c}{b+d}$ is a rational number in between the two.

4. Show that $\sqrt{2} + \sqrt{3}$ and $2\sqrt{2} - \sqrt{10}$ cannot be rational.

5. The following is a simpler proof that $\sqrt{2}$ is not rational: Suppose $\sqrt{2} = a/b$ with $a, b$ having no common factors. Then $a^2 = 2b^2$; but the left hand side must have an even number of primes, whereas the right hand side has an odd, and this is impossible. Generalize this proof to show

that the square root of any integer that has a prime factor repeated an odd number of times (including once only) is irrational.

6. Generalize this argument even further: suppose $c/d$ is a rational number that satisfies the polynomial equation $a_n x^n + \cdots + a_0 = 0$ where $a_i \in \mathbb{Z}$. Show that $c|a_0$ and $d|a_n$.

7. Use the preceding exercise to show that the equations $x^4 + 4x^2 - 1 = 0$ and $x^6 - 3x^4 + 3x^2 - 3 = 0$ cannot have rational solutions. Deduce that $\sqrt{\sqrt{5} - 2}$ and $\sqrt{\sqrt[3]{2} + 1}$ are irrational.

# 4 Sets

A set is a collection of **elements**, which we can write explicitly as $\{ a, b, c, \dots \}$. For example, the collection $\{ 1, 2, 4 \}$ is a set with the elements 1, 2 and 3. However we will be needing a more general definition.

**Definition** A **set** is a collection of objects $x$ which satisfy a certain property or statement $\phi(x)$.

$$A = \{ x : \ \phi(x) \}$$

We say that $x$ is an **element** of $A$, and write $x \in A$ when $\phi(x)$ is true.

In practice, the objects $x$ come from some universal set $V$, that would be understood in context. For example it could be the set of integers. Strictly speaking, we should therefore write $\{ x \in V : \ \phi(x) \}$ instead of $\{ x : \ \phi(x) \}$ to avoid confusion.

### 4.0.1 Examples

1. The set $\{ x \in \mathbb{Q} : \ x^2 = 1 \}$ consists of the elements 1 and $-1$; it can also be written as $\{ 1, -1 \}$.
2. The set $\{ x \in \mathbb{C} : \ x^2 = -1 \}$ has two elements $i$ and $-i$.
3. $\{ n \in \mathbb{Z} : \ 4|n \}$ consists of all multiples of 4; more generally, the set of all multiples of $n$ is $M_n = \{ x \in \mathbb{Z} : \ n|x \}$.

## 4.1 Subsets, Intersections, Unions, ...

**Definition** The **empty set** is the set with no elements

$$\varnothing = \{ \}$$

**Definition** Two sets $A$, $B$ are **equal** when they have the same elements:

$$A = B \ \Leftrightarrow \ \forall x \quad (x \in A \ \Leftrightarrow \ x \in B)$$

If $A = \{\, x :\ \phi(x) \,\}$ and $B = \{\, x :\ \psi(x) \,\}$, then $A = B$ with this definition would mean $\forall x \quad \phi(x) \Leftrightarrow \psi(x)$.

**Definition** $A$ is a **subset** of $B$ when all elements of $A$ are also elements of $B$:

$$A \subseteq B \Leftrightarrow \forall x \quad (x \in A \ \Rightarrow\ x \in B)$$

In terms of $\phi(x)$ and $\psi(x)$, this would be true when $\forall x \quad \phi(x) \ \Rightarrow\ \psi(x)$.

Note that if $A \subseteq B$ and $B \subseteq A$ then $A = B$ (i.e. if $\phi \ \Rightarrow\ \psi$ and $\psi \ \Rightarrow\ \phi$ then $\phi \Leftrightarrow \psi$).

Note also that $\varnothing \subseteq A$ is always true.

**Definition** The **complement** of a set $A$ consists of all those elements of the universal set which are *not* elements of $A$:

$$A' = \{\, x :\ x \notin A \,\} = \{\, x :\ \text{NOT}\ \phi(x) \,\}$$

We also write,

$$B - A = \{x :\ x \in B \ \text{AND}\ x \notin A\}$$

Exercise: Show that $A'' = A$; $\varnothing' = V$; $V' = \varnothing$;

Example: $M_2'$ is the set of all odd numbers.

**Definition** The **union** of two sets $A$ and $B$ is the set of the elements of $A$ combined with those of $B$:

$$A \cup B = \{\, x :\ x \in A \ \text{OR}\ \ x \in B \,\} = \{\, x : \phi(x) \ \text{OR}\ \ \psi(x) \,\}$$

**Definition** The **intersection** of two sets $A$ and $B$ is the set of elements that are in both $A$ *and* $B$:

$$A \cap B = \{\, x :\ x \in A \ \text{AND}\ \ x \in B \,\} = \{\, x :\ \phi(x) \ \text{AND}\ \ \psi(x) \,\}$$

Note that $A \cup A = A$; $A \cap A = A$; $A \cup A' = \varnothing$; $A \cup A' = V$. (Prove these statements!)

**Definition** Two sets are said to be **disjoint** when they have no elements in common i.e. when $A \cap B = \varnothing$.

We can obviously generalize to unions and intersections of a larger number of sets e.g. $A \cup B \cup C$ or $A \cap B \cap C$ etc.

*Proposition* 4.1.1

**1.** $A \subseteq B \Leftrightarrow B' \subseteq A'$

**2.** $(A \cap B)' = A' \cup B'$**;** $(A \cup B)' = A' \cap B'$

**3.** $A \cup A' = V$**;** $A \cap A' = \varnothing$**.**

Proof. 1. We are given that $A \subseteq B$. This means that $\forall x\ x \in A \Rightarrow x \in B$ (*).

Let $x$ be any element of $B'$. This means that $x \notin B$; but by the implication in (*) this implies that $x \notin A$ i.e. $x \in A'$. Hence $B' \subseteq A'$.

2. $x \in (A \cap B)'$ means $x \notin (A \cap B)$ i.e. NOT $(x \in A$ AND $x \in B)$ which is equivalent to $x \notin A$ OR $x \notin B$; this we can write as $x \in A'$ OR $x \in B'$ i.e. $x \in (A' \cup B')$. Since the two statements are equivalent we have just shown that $(A \cap B)' = (A' \cup B')$.

Similarly, $x \in (A \cup B)'$ means $x \notin (A \cup B)$ i.e. NOT $(x \in (A \cup B))$. Remembering how to take opposites of statements, we find that this is equivalent to $x \notin A$ AND $x \notin B$, which is the same as $x \in A'$ AND $x \in B'$ i.e. $x \in (A' \cap B')$.

3. For each $x$ either $x \in A$ or $x \notin A$ must be true i.e. $x \in (A \cup A')$ is always true. But $x \in V$ is also always true; therefore they are the same statement and the two sets are equal.

On the other hand, $x \in A$ and $x \notin A$ cannot both be true i.e. $x \in (A \cap A')$ is always false, which means that $(A \cap A')$ has no elements and is therefore the empty set.

□

## 4.2 Products of Sets ...

**Definition** An **ordered pair** of elements is denoted by $(x, y)$.

The order that the elements are written down is important in this definition i.e. $(x, y)$ is not the same as $(y, x)$ in general.

We can generalize this to any ordered list of elements $(x_1, x_2, \ldots, x_n)$.

**Definition** The (Cartesian) **product** of two sets $A$ and $B$ is the set of all ordered pairs of elements, in which the first elements in the pair is chosen from $A$ and the second from $B$:

$$A \times B = \{\, (x, y) : \ x \in A \text{ AND } \ y \in B \,\}$$

Again we can generalize to a product of more than two sets e.g. $A \times B \times C = \{\, (x, y, z) : \ x \in A, y \in B, z \in C \,\}$.

We write $A^2$ for $A \times A$, $A^3$ for $A \times A \times A$ etc.

Note that $A \times B$ and $B \times A$ are different sets. The first consists of pairs $(x, y)$ where $x \in A$ and $y \in B$, while the second consists of pairs $(y, x)$ with $y \in B$ and $x \in A$.

Sometimes we will need to consider unions, intersections and products of an infinite number of sets; so we make the following definition:

**Definition** Let $A_1$, $A_2$, ... be an infinite number of sets; then

$$\bigcup_{i=1}^{\infty} A_i = \{\, x : \ x \in A_i \ \exists i \,\}$$

$$\bigcap_{i=1}^{\infty} A_i = \{\, x : \ x \in A_i \ \forall i \,\}$$

$$\prod_{i=1}^{\infty} A_i = \{\, (x_1, x_2, \ldots) : \ x_i \in A_i \ \forall i \,\}$$

**Definition** The **power set** of a set $A$ is a set of all the subsets of $A$:

$$P(A) = \{\, B : \ B \subseteq A \,\}$$

Note carefully that the elements of $P(A)$ are themselves sets, in fact the subsets of $A$. For example, the power set of the set $\{\, 1, 2, 3 \,\}$ is the set $P(\{\, 1, 2, 3 \,\}) = \{\, \varnothing, \{\, 1 \,\}, \{\, 2 \,\}, \{\, 3 \,\}, \{\, 1, 2 \,\}, \{\, 1, 3 \,\}, \{\, 2, 3 \,\}, \{\, 1, 2, 3 \,\} \,\}$.

Sometimes the power set $P(A)$ is written as $2^A$.

**Definition** We say that the sets $A_i$ **cover** the set $B$ when

$$B \subseteq \bigcup_i A_i$$

or equivalently, $\forall x \in B \; \exists i \quad x \in A_i$.

For example, the sets $A_n = \{\, x \in \mathbb{Q} : \; n - \frac{3}{4} \leqslant x \leqslant n + \frac{3}{4} \,\}$ is a cover of $\mathbb{Q}$.

**Definition** A **partition** of a set $B$ are sets $A_i$ such that:

1. $A_i$ cover $B$ i.e. $B \subseteq \bigcup_i A_i$;
2. the $A_i$'s are disjoint i.e. $i \neq j \;\Rightarrow\; A_i \cap A_j = \varnothing$.

Note that in a partition, each element of $B$ belongs to exactly one set $A_i$.

## 4.3 Exercises

1. Let

   $$A = \{(x, y) : x \in \mathbb{R},\; y \in \mathbb{R},\; x^2 + y^2 = 1\}$$
   $$B = \{(x, y) : x \in \mathbb{R},\; y \in \mathbb{R},\; y^2 = 4x\}$$
   $$C = \{(x, y) : x \in \mathbb{R},\; y \in \mathbb{R},\; y^2 = x^3\}$$

   Draw the sets and find $A \cap B$, $A \cap C$, $B \cap C$, $A \cap B \cap C$, $A \cup B$, $(A \cup B) \cap C$, $(A \cap C) \cup (B \cap C)$.

2. Prove

   (a) $(A \cup B) \cap C \subseteq (A \cap C) \cup (B \cap C)$;

   (b) $(A \cup B) \cap C \supseteq (A \cap C) \cup (B \cap C)$.

   What conclusion can we draw from (i) and (ii)?

3. Prove or find a counterexample for:

   (a) $A - B = \varnothing \;\Rightarrow\; A \subseteq B$;

   (b) $A - (B - A) = A$;

(c) $(A \cup B)' = A' \cup B'$;

(d) $A \cap (B - C) = (A \cap B) - (A \cap C)$;

(e) $A \subseteq B \Leftrightarrow B - (B - A) = A$;

(f) $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

4. For each positive rational number $q \in \mathbb{Q}^+$ and positive integer $n \in \mathbb{N}$, let

   $A_q = \{x \in \mathbb{Q} : \ -\frac{1}{q} \leqslant x \leqslant \frac{1}{q}\}$

   $B_n = \{x \inf \mathbb{Q} : \ -\frac{1}{n} < x \leqslant n\}$

   Find $\bigcap_{q \in \mathbb{Q}^+} A_q$, $\bigcup_{n \in \mathbb{N}} B_n$, and $\bigcap_{n \in \mathbb{N}} B_n$.

5. Prove

   (a) $[(A \cup B)' \cup A]' = B \cap A'$

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

   (c) $(A \cup B')' = A' \cap B$

6. Write down $\{\,1, 2, 3\,\} \times \{\,1, 2\,\}$ and $\mathrm{P}(\{\,1, 2, 3, 4\,\})$. How many elements do they have?

7. Prove that

   (a) union of sets is distributive over intersection

   (b) intersection is distributive over union

8. Show that if $A \subseteq \mathbb{N}$, $0 \in A$ and $n \in A \ \Rightarrow \ n^+ \in A$ then $A = \mathbb{N}$. This is just the principle of induction written in set notation.

# 5 Relations

Very often we need to write sentences about two objects; e.g. *$x$ is the father of $y$*; *$x$ is taller than $y$*; *$x$ rhymes with $y$*; *$x$ and $y$ are produced by the same firm*; *$x$ is symmetric to $y$*; $x \leqslant y$; $x = y + 2$.

Such statements about $x$ and $y$ are called relations and will be denoted by $x \sim y$. Obviously relations will not always be true for any $x$ and $y$. So the effect of a relation is to associate certain $x$'s with those $y$'s that make the statement true.

**Definition** A **relation** is a statement about two objects $(x, y)$, denoted by $x \sim y$.

The **inverse relation** of $x \sim y$ is $x \sim^{-1} y$ which would be true exactly when $y \sim x$.

What kind of properties can relations have? Here are four properties that are of importance:

**Definition** A relation $\sim$ is said to be:

1. **reflexive** when $\forall x \in X \quad x \sim x$;
2. **symmetric** when $\forall x, y \in X \quad x \sim y \Leftrightarrow y \sim x$;
3. **transitive** when $\forall x, y, z \in X \quad x \sim y \text{ AND } y \sim z \Rightarrow x \sim z$;
4. **antisymmetric** when $\forall x, y \in X \quad x \sim y \text{ AND } y \sim x \Rightarrow x = y$.

For a symmetric relation, the order in which one writes $x \sim y$ or $y \sim x$ is not important — they both mean the same; but for non-symmetric relations the order may or may not make a difference.

For an anti-symmetric relation, it makes a big difference whether one writes $x \sim y$ or $y \sim x$; in fact they can never both be true unless $x = y$.

## 5.1 Equivalence Relations

**Definition** An **equivalence relation** is a relation which is reflexive, symmetric and transitive.

For each $x \in X$, we can find those elements $y$ which are related to $x$ and form a set from them.

**Definition** The **equivalence class** of $x$ is the set,

$$[x] = \{\, y \in X : \; y \sim x \,\}$$

**Theorem** A

**Given an equivalence relation $\sim$ on a set $X$, then the equivalence classes of $\sim$ form a partition of $X$.**

Proof. We need to show that the sets $[x]$ cover $X$ and are disjoint.

(i) Suppose $x \in X$. Then $x \sim x$ by the reflexive property of $\sim$. Therefore $x \in [x]$ since $x$ is related to itself i.e. $x$ is in at least one equivalence class, and as this is true for any $x$, the sets $[x]$ cover all of $X$.

(ii) We would like to show that the sets $[x]$ are disjoint i.e. $[x] \neq [y] \;\Rightarrow\; [x] \cap [y] = \varnothing$. We can show this by proving its contrapositive statement: $[x] \cap [y] \neq \varnothing \;\Rightarrow\; [x] = [y]$.

Suppose $z$ is an element of $[x] \cap [y]$, so that $z \in [x]$ and $z \in [y]$. These statements mean that $z \sim x$ and $z \sim y$. Now we can use the symmetric property of $\sim$ to switch round $z$ and $x$ to get $x \sim z$, which together with $z \sim y$ and the transitive property of $\sim$ imply that $x \sim y$. This is going to be a useful piece of information that we have gathered. We still have to show that $[x] = [y]$.

So let $a$ be any element of $[x]$ i.e. $a \in [x]$ which means $a \sim x$. Together with $x \sim y$, it implies that $a \sim y$ (why?), and so $a \in [y]$. Conversely, if $a \in [y]$ then $a \sim y$ which together with $y \sim x$ (how do we know $y \sim x$?) implies that $a \sim x$ i.e. $a \in [x]$. Thus all the elements of $[x]$ are in $[y]$ and vice-versa, so that the two sets are the same.

□

**Theorem** B

**Let $A_i$ be a partition of the set $X$, then we can create an equivalence relation $\sim$ on $X$ whose equivalence classes are precisely the $A_i$'s.**

Proof. The $A_i$'s form a partition of $X$. This means that $X = \bigcup_i A_i$ (i.e. $\forall x \in X \exists i\ x \in A_i$) and $i \neq j \ \Rightarrow\ A_i \cap A_j = \emptyset$. Every element will be covered by a single set $A_i$; of course if we pick two elements at random, $x$ and $y$, they might not be in the same set.

Let us define the relation $x \sim y$ to mean *$x$ and $y$ belong to the same set* $A_i$ i.e. $\exists i\ x, y \in A_i$. We would like to show that $\sim$ is an equivalence relation.

(i) Reflexive. $x$ lies in some set $A_i$, as these cover $X$. Hence $x$ and $x$ are both in the same $A_i$ i.e $x \sim x$.

(ii) Symmetric. Suppose $x \sim y$ i.e. $x, y \in A_i$; then changing the order of $x$ and $y$ obviously does not change the fact that they are in the same set i.e. $y, x \in A_i$ i.e. $y \sim x$.

(iii) Transitive. Suppose $x \sim y$ and $y \sim z$. These mean according to our definition, that $x$ and $y$ belong to the same set, say $A_i$, while $y$ and $z$ belong to the same set, say $A_j$. So $y$ is in both $A_i$ and $A_j$ i.e. $A_i \cap A_j \neq \emptyset$. Since the sets $A_i$ are disjoint, this can only be true when $A_i = A_j$, so that $x$, $y$ and $z$ all belong to the same set; in particular $x$ and $z$ are in $A_i$, and hence $x \sim z$.

We finally have to show that the equivalence classes of $\sim$ are the sets $A_i$. By definition, $[x] = \{\, y \in X :\ y \sim x \,\} = \{\, y \in X :\ x, y \in A_i \,\}$. Therefore $[x]$ consists of all those $y$ which are in the same set $A_i$ as $x$. What are these elements? One moment's thought reveals that it is precisely the elements of $A_i$ which are in the same set as $x$ i.e. $[x] = A_i$.

□

### 5.1.1 Example

Let $a$ be a fixed integer. Define the relation $\sim$ on integers to mean $a|(x-y)$. Claim: $\sim$ is an equivalence relation.

*Reflexive*: $\forall x \in \mathbb{Z},\ a|0 = (x - x)$;

*Symmetric*: $\forall x, y \in \mathbb{Z}$, if $a|(x-y)$ i.e. $x - y = ka$, then $y - x = (-k)a$ and so $a|(y-x)$ i.e. $y \sim x$;

*Transitive*: $\forall x, y, z \in \mathbb{Z}$, if $x \sim y$ and $y \sim z$ then $a|(x-y)$ and $a|(y-z)$, so that $a|((x-y)+(y-z)) = (x-z)$ i.e. $x \sim z$.

Since this relation is used often, it is customary to write $x \equiv y \pmod{a}$ instead of $x \sim y$. What are its equivalence classes? If we pick $x$, then $[x] = \{\, y \in \mathbb{Z} :\ y \sim x \,\} = \{\, y :\ a|(y-x) \,\}$. But $a|(y-x)$ means $y - x = ka$ i.e. $y = x + ka$ for some integer $k$. Therefore $[x] = \{\, x + ka :\ k \in \mathbb{Z} \,\}$. In

particular note that $[0] = M_a$ the multiples of $a$; also, if we choose $a = 2$, then $[0]$ is the set of even numbers, while $[1]$ is the set of odd numbers: in fact these two form a partition of the set $\mathbb{Z}$, as the theorem assures us happens for all equivalence relations.

## 5.2 Example

Consider the set $\mathbb{R}^2$ whose elements are $\mathbf{u} = (x, y), x, y \in \mathbb{R}$. Let $\mathbf{u} \sim \mathbf{v}$ be the relation on the elements $\mathbf{u}, \mathbf{v}$:

$$|\mathbf{u}| = |\mathbf{v}|$$

The statements $|\mathbf{u}| = |\mathbf{u}|$, $|\mathbf{u}| = |\mathbf{v}| \Leftrightarrow |\mathbf{v}| = |\mathbf{u}|$, and $|\mathbf{u}| = |\mathbf{v}|$ AND $\|\mathbf{v}| = |\mathbf{w}| \Rightarrow |\mathbf{u}| = |\mathbf{w}|$ are exactly what is required to show that $\sim$ is reflexive, symmetric and transitive, and hence an equivalence relation.

Its equivalence classes are $[\mathbf{u}] = \{\, \mathbf{v} \in \mathbb{R}^2 : \ |\mathbf{v}| = |\mathbf{u}| \,\}$. Which points $\mathbf{v}$ have the same length $|\mathbf{v}|$ as $\mathbf{u}$? Precisely those points on a circle with radius equal to the length of $\mathbf{u}$ i.e. $[\mathbf{u}]$ is a circle centred at the origin with radius $|\mathbf{u}|$.

## 5.3 Order Relations

**Definition** An **order relation** is a relation which is reflexive, transitive and antisymmetric; and is denoted by $x \preceq y$.

For example, the relation $x|y$ on the set of *positive* integers is an order relation, since it is obviously reflexive and transitive and moreover, if $x|y$ and $y|x$ then $x = y$ (as we are restricting to the positive integers).

**Definition** An order relation $\preceq$ is called a **linear order** if it also has the property that

$$\forall x, y \in X \quad x \preceq y \text{ OR } y \preceq x$$

The most important example of a linear order is the *less than* relation $\leqslant$. We know that for any rational numbers $p, q \in \mathbb{Q}$, $p \leqslant q$ and $q \leqslant p$ together would imply that $p = q$, so that $\leqslant$ is antisymmetric; also one of $p \leqslant q$ or $q \leqslant p$ has to be true, so that $\leqslant$ is a linear order. In what follows we will only consider this linear order $\leqslant$, but most of the definitions can be generalized to any linear order $\preceq$.

**Definition** Suppose $A$ is a subset of $X$, which has a linear order $\leqslant$ defined on it.

1. $b$ is an **upperbound** of $A$ means $\forall a \in A \quad a \leqslant b$; we also say that $A$ is **bounded above** by $a$.
2. $\alpha$ is a **least upperbound** (or **supremum**) of $A$, written as $\alpha = \sup A$, means that
   (a) $\alpha$ is an upperbound of $A$ i.e. $\forall a \in A \quad a \leqslant \alpha$
   (b) all the other upperbounds of $A$ are larger than $\alpha$ i.e. if $b$ is an upperbound then $\alpha \leqslant b$.
3. $\alpha$ is a **maximum** of $A$, written as $\alpha = \max A$, means that
   (a) $\alpha$ is an upperbound of $A$;
   (b) $\alpha \in A$

Similarly define, **Definition** $c$ is a **lowerbound** of $A$ when $\forall a \in A \quad c \leqslant a$; and we say that $A$ is **bounded below** by $c$;

$\gamma$ is a **greatest lowerbound** (or **infimum**) of $A$, written as $\gamma = \inf A$, when $\gamma$ is a lowerbound of $A$ and every other lowerbound of $A$ is smaller than $\gamma$.

$\gamma$ is a **minimum** of $A$, written as $\gamma = \min A$, when it is a lowerbound and an element of $A$.

Note that a maximum of $A$ is a least upperbound of $A$; suppose $b$ is any upperbound of $A$ and let $\alpha$ be the maximum of $A$; then, since $\alpha$ is an element of $A$, it must be smaller than $b$; as this is true for all upperbounds $b$, $\alpha$ is the least upperbound of $A$. Similarly a minimum of a set must be a greatest lower bound (check!).

There can only be ONE least upperbound of a set $A$, and ONE greatest lowerbound; this is quite obvious since if $\alpha$ and $\beta$ are both least upperbounds of $A$, then $\alpha \leqslant \beta$ (because $\alpha$ is the least upperbound) and $\beta \leqslant \alpha$ (because $\beta$ is the least upperbound); hence, by the anti-symmetric property of $\leqslant$ it follows that $\alpha = \beta$.

### 5.3.1 Exercises

1. Find relations that have any combination of the reflexive, symmetric and transitive properties.

2. Show that, for the set of triangles in the plane, the relations "is congruent to" and "is similar to" are equivalence relations.

3. Let $\sim$ be the relation on $\mathbb{R}^2$ defined by

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \sim \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \Leftrightarrow y_1 x_2^2 = y_2 x_1^2.$$

   Show that $\sim$ is an equivalence relation and find its equivalence classes.

4. Let the plane $\mathbb{R}^2$ be partitioned into circles of radius $r$ i.e. $\mathbb{R}^2 = \cup_r S_r$ where $S_r = \{\, \mathbf{x} \in \mathbb{R}^2 : |\mathbf{x}| = r \,\}, r \geqslant 0$. Show that the sets $S_r$ form a partition of the plane. What is the associated equivalence relation?

5. Repeat the exercise above for the straight lines through the origin, $B_{a,b} = \{\, \mathbf{x} = (x, y) \in \mathbb{R}^2 : ay = bx \text{ AND } \mathbf{x} \neq \mathbf{0} \,\}$.

6. What is wrong with the following "proof" that a symmetric and transitive relation is always reflexive:

$$x \sim y \;\Rightarrow\; y \sim x,$$

$$\therefore x \sim y \;\Rightarrow\; (y \sim x \text{ AND } x \sim y) \;\Rightarrow\; x \sim x,$$

$$\therefore x \sim x.$$

7. * Suppose we start with an equivalence relation $\sim$; the associated partition of equivalence classes induces a new equivalence relation. Show that this is identical to $\sim$ itself.

8. Show that the relation $x|y$ ($x$ divides $y$) on $\mathbb{N}$ is an order relation.

9. Show that the set of natural numbers is not bounded above.

10. Show that the set of numbers $x_n = 1 + 1/2 + 1/2^2 + 1/2^3 + \cdots + 1/2^n$ is bounded above by 2. (Hint: use induction and the equation $x_{n+1} = 1 + x_n/2$.)

11. Deduce that the set of numbers $y_n = 1 + 1 + 1/2! + 1/3! + \cdots + 1/n!$ is bounded above by 3.

12. Define $A + B = \{\, a + b : a \in A, b \in B \,\}$. Show that $\sup(A + B) = \sup A + \sup B$.

13. * Consider the set of positive integers with the order relation $a|b$. Show that it is in fact an order relation, and that the supremum and infimum of two integers are their lcm and hcf respectively. (Remember to substitute $a|b$ instead of $a \leqslant b$ throughout the definitions)

# 6 Real Numbers

Using the rational numbers, we have seen that it is impossible to solve the equation $x^2 = 2$. Let us examine why. It is not because there aren't many rational numbers; in fact $\mathbb{Q}$ is dense. Moreover we can find rational numbers that are as good an approximation to the solution as we want them to be, but they cannot ever equal the exact solution. The real numbers we are going to consider in this chapter are a *completion* of the rational numbers; we 'invent' new numbers, called *real*, to "fill in the gaps".

### 6.0.2 Example

Let us take $x^2 = 2$ as our model problem (but we can choose any other such equation). Consider the set of rational numbers

$$A := \{\, x \in \mathbb{Q} : x^2 < 2 \,\}.$$

For example, $1, \frac{1}{2}, 1.1$ are all elements of $A$.

$A$ is bounded above, for example by 2; since let $x \in A$ ie $x^2 < 2$. Suppose $x \geqslant 2$, then $x^2 \geqslant 4 \;\Rightarrow\; x \notin A$ so that $x \in A \;\Rightarrow\; x < 2$.

Claim: there are rational numbers $x$ such that $x^2$ is as close an approximation to 2 as we wish.

Claim reworded rigorously: For any rational number $\epsilon > 0$, there is a rational number $p = m/n$ such that $2 - \epsilon < p < 2$.

Proof of claim: Suppose that $\epsilon > 0$ is given, and let us assume that $\epsilon < 1$; then we can use the Archimedean property for rational numbers to deduce that there is a natural number $n < \epsilon/10$. Now find another natural number $m$ such that $(m/n + \epsilon/10)^2 > 2$; this will be possible because the left-hand side will grow to infinity as $m$ increases in value. In fact choose the smallest such $m$ so that $((m-1)/n + \epsilon/10)^2 < 2$ (it cannot equal 2, why?).

We deduce two facts. Firstly, the last inequality shows that

$$\frac{m^2}{n^2} < \left(\frac{m}{n} + \frac{\epsilon}{10} - \frac{1}{n}\right)^2 = \left(\frac{m-1}{n} + \frac{\epsilon}{10}\right)^2 < 2.$$

This in turn implies that $m/n < 2$. Secondly, expanding out $(m/n + \epsilon/10)^2 > 2$ gives

$$\begin{aligned} \tfrac{m^2}{n^2} &> 2 - 2\tfrac{m}{n}\tfrac{\epsilon}{10} - \tfrac{\epsilon^2}{100} \\ &> 2 - \tfrac{4\epsilon}{10} - \tfrac{\epsilon^2}{100} \\ &> 2 - \tfrac{4\epsilon}{10} - \tfrac{\epsilon}{100} \\ &> 2 - \epsilon \end{aligned}$$

Hence $2 - \epsilon < m^2/n^2 < 2$.

Using a very similar argument, we can show that there are rational numbers $m/n$ such that $2 < m^2/n^2 < 2 + \epsilon$, no matter how small $\epsilon$ is.

From this it follows that the set $A$ does not have a *least* upperbound:

1. The upperbounds of $A$ satisfy $p^2 > 2$; since suppose $p$ is an upperbound of $A$ with $p^2 \leqslant 2$, then $p^2 < 2$ since no rational number when squared gives 2; hence there is a $p' > p$ such that $(p')^2 < 2$ ie $p' > p$ and $p' \in A$; but $p$ was supposed to be an upperbound; hence $p^2 > 2$.

2. Let $p$ be an upperbound of $A$; hence $p^2 > 2$; then $\exists p' \in \mathbb{Q}$ such that $(p')^2 > 2$ and $p' < p$; this means $p'$ is another upperbound of $A$ smaller than $p$; hence there cannot be a *least* upperbound of $A$.

This problem with the rational numbers is actually very common, not just in trying to solve equations like $x^2 = 2$, $x^3 = 5$ etc but also many other equations of the type $f(x) = 0$. We often can get close to the solutions but not exactly ie the sets $\{\, x \in \mathbb{Q} : x^2 < 2 \,\}, \{\, x \in \mathbb{Q} : x^3 < 5 \,\}$, and more generally $\{\, x \in \mathbb{Q} : f(x) < 0 \,\}$ have upperbounds but not *least* upperbounds.

Hence we introduce the real numbers as numbers having all the properties that rational numbers have, but in addition have the *completeness axiom* which states:

*Every nonempty set in $\mathbb{R}$ that has an upperbound, has a least upperbound.*

Would such an axiom help in solving the equation $x^2 = 2$. Let us take the set $A = \{\, x \in \mathbb{R} : x^2 < 2 \,\}$. As before it is non-empty ($1 \in A$), it has upperbounds (e.g. 2); hence with this completeness axiom it would have a *least* upperbound, $\alpha$. Suppose that $\alpha^2 < 2$; then we would be able to find another real number $x$ such that $x \in A$ and $\alpha < x$ as we did for the rational numbers; but this is a contradiction since $\alpha$ is an upperbound for $A$. Suppose that $\alpha^2 > 2$; then we can again find a real number $y$ such that $y^2 > 2$ but $y < \alpha$; this means that $y$ is a smaller upperbound than $\alpha$ which is impossible. The only remaining possibility is that $\alpha^2 = 2$ which solves the equation $x^2 = 2$.

The **Real Number** system is defined to be a set of numbers on which are defined addition, multiplication and 'less than', having the properties (axioms):

Addition:

| | |
|---|---|
| Associative | 1. $(a+b)+c = a+(b+c)$ |
| Commutative | 2. $a+b = b+a$ |
| Identity (zero) | 3. $a+0 = a$ |
| Inverses | 4. $a+(-a) = 0$. |

Multiplication

| | |
|---|---|
| Associative | 5. $(ab)c = a(bc)$ |
| Commutative | 6. $ab = ba$ |
| Identity (one) | 7. $a1 = a$ for $a \neq 0$ |
| Inverses | 8. $\forall a \neq 0\ a\frac{1}{a} = 1$ |
| Distributive | 9. $a(b+c) = ab+ac$ |

Less Than

| | |
|---|---|
| Transitive | 10. $a \leqslant b$ and $b \leqslant c \ \Rightarrow\ a \leqslant c$ |
| Linear | 11. $a < b$ or $a = b$ or $a > b$ |
| | 12. $a \leqslant b \ \Rightarrow\ a+c \leqslant b+c$ |
| | 13. $a \leqslant b$ and $c \geqslant 0 \ \Rightarrow\ ac \leqslant bc$ |

Completeness 14. Every nonempty set with an upperbound has a least upperbound (the supremum).

Note: It also follows that every nonempty set with a lowerbound has a greatest lowerbound (the infimum).

We have only stated what properties we would *like* the real numbers to have, but we have not yet defined them. We will take a straightforward but tedious approach — there are more elegant, though abstract, ways of defining $\mathbb{R}$.

**Definition** A **real** number is an infinite series of fractions (base 10 say),

$$x = m + \frac{m_1}{10} + \frac{m_2}{100} + \ldots + \frac{m_n}{10^n} + \ldots,$$

where $m \in \mathbb{Z}$, $m_n \in \{\,0, 1, 2, \ldots, 9\,\}$.

This is often written as $m \cdot m_1 m_2 \cdots$; eg $1.789000\cdots$ and $2.8182536\cdots$ are both real numbers.

Addition, multiplication and 'less than' can be defined as follows:

For $x = m.m_1m_2\cdots$ and $y = n.n_1n_2\cdots$, let

$$x + y := (m+n) + (m_1+n_1)/10 + (m_2+n_2)/10^2 + \ldots,$$

$$xy := (mn) + (mn_1 + nm_1)/10 + (mn_2 + m_1n_1 + nm_2)/10^2 + \ldots,$$
$$x < y \Leftrightarrow m < n \text{ OR } (m = n, \ldots, m_k = n_k, m_{k+1} < n_{k+1}).$$

A lot of care must be taken in interpreting these definitions for addition and multiplication: whenever the digits sum up to more than their denominator, then they must carry over to the preceding decimal place e.g. $\pi + e = 3.14159265\cdots + 2.71828182\cdots = 5.85987448\cdots$.

Note that, with these operations, it is possible to get decimal expansions that end in a string of 9s i.e. $m.m_1\cdots m_n 9999\cdots$; such numbers are *identified* with the number $m.m_1\cdots(m_n+1)000\cdots$, and it is assumed that real numbers are in this standard format.

**Definition** The **absolute** value of a real number is

$$|x| = \begin{cases} x & \text{if } x \geqslant 0 \\ -x & \text{if } x < 0 \end{cases}$$

The **integer part** of a real number $x = m.m_1m_2\cdots$ is $\lfloor x \rfloor = m$. The **fractional part** is $x - \lfloor x \rfloor = 0.m_1m_2\cdots$.

Hence $|x| \geqslant 0$ no matter what sign $x$ has.

**Definition** An interval of real numbers is defined as a set of type

$$(a,b) = \{\, x \in \mathbb{R} : a < x < b \,\}, \quad [a,b] = \{\, x \in \mathbb{R} : a \leqslant x \leqslant b \,\},$$
$$(a,b] = \{\, x \in \mathbb{R} : a < x \leqslant b \,\}, \quad [a,b) = \{\, x \in \mathbb{R} : a \leqslant x < b \,\}$$
$$(-\infty,a) = \{\, x \in \mathbb{R} : x < a \,\}, \quad (a,\infty) = \{\, x \in \mathbb{R} : a < x \,\}$$
$$(-\infty,a] = \{\, x \in \mathbb{R} : x \leqslant a \,\}, \quad [a,\infty) = \{\, x \in \mathbb{R} : a \leqslant x \,\},$$
$$(-\infty,\infty) = \mathbb{R}.$$

One can check that the real numbers, so defined, satisfy axioms 1 to 14, but it is very tedious and slightly difficult to do so, although they follow from the same properties for the rational numbers. We ought to prove the completeness axiom, but we will only give a sketch proof (you can fill in the details):

*Sketch proof of completeness axiom.* Let $A$ be a non-empty set of real numbers that has an upperbound. Consider the set of all integers that are

upperbounds of $A$; take the smallest such upperbound, and let $m$ be that integer which is one smaller than it. Subdivide the interval $[m, m+1)$ into tenths — again find which are still upperbounds and take that tenth $m_1/10$ which is just smaller than these. Continue this process, dividing into hundredths, etc, each time obtaining a digit $m_n$. The number so obtained $\alpha = m.m_1m_2\ldots$ is smaller than all the upperbounds, but bigger than all the elements of $A$, hence must be the least upperbound.

*Proposition* 6.0.1

**Let $\alpha$ be the supremum of $A$; then there are elements of $A$ that are as close to $\alpha$ as you wish ie**

$$\forall \epsilon > 0 \ \exists a \in A \quad \alpha - \epsilon < a \leqslant \alpha.$$

Proof. $\alpha$ is the *least* upperbound of $A$. It follows that $\alpha - \epsilon$ is not an upperbound of $A$; hence there is an element $a \in A$ such that $a > \alpha - \epsilon$. But $a \leqslant \alpha$ since $a \in A$ and $\alpha$ is an upperbound of $A$.

□

*Proposition* 6.0.2

**(Archimedean Property for the Reals)**

$$\forall \epsilon > 0 \ \exists n \in \mathbb{N} \quad 0 < \frac{1}{n} < \epsilon.$$

Proof. We are required to show that for any real number $\epsilon > 0$, there is a natural number $n \in \mathbb{N}$ such that $1/\epsilon < n$. But this is obvious: take the integer part of $1/\epsilon$ and add one to get a larger natural number.

□

*Proposition* 6.0.3

**The rational numbers are dense in the reals i.e.**

$$\forall x, y \in \mathbb{R}, (\textbf{say } x < y), \ \exists p \in \mathbb{Q} \quad x < p < y.$$

Proof. Let $\epsilon = (y - x)$; then by the Archimedean property there is an $n \in \mathbb{N}$ such that $1/n < \epsilon$. Also by the Archimedean property there is an $m \in \mathbb{N}$ such that $1/m < 1/(nx)$ i.e. $m/n > x$. In fact choose the smallest such natural number $m$. Then $(m-1)/n < x$ so that $m/n < x + 1/n < x + \epsilon = y$. □

A simpler proof is to take the decimal expansions of $x$ and $y$, see where they differ and take that rational number which agrees with the first few identical digits of $x$ and $y$, but stops at the decimal place where they differ e.g. if $x = 3.12345\ldots$ and $y = 3.12389\ldots$ then take $p = 3.1235$.

*Proposition* 6.0.4

**The rational numbers are precisely those real numbers with a *recurring* decimal expansion i.e.**

$$p = m.m_1 \cdots m_n k_1 \cdots k_r k_1 \cdots k_r \cdots$$

Proof. Let $x$ be a real number with a recurring expansion. Then

$$\begin{aligned} x &= m.m_1 \cdots m_n k_1 \cdots k_r k_1 \cdots k_r \cdots \\ \therefore 10^n x &= m m_1 \cdots m_n.k_1 \cdots k_r k_1 \cdots k_r \cdots \\ \therefore 10^(r+n)x &= m m_1 \cdots m_n k_1 \cdots k_r.k_1 \cdots k_r k_1 \cdots k_r \cdots \end{aligned}$$

Subtracting gives an integer

$$10^{r+n}x - 10^n x = m m_1 \cdots m_n k_1 \cdots k_r - m m_1 \cdots m_n = N.$$

Hence $x = N/10^n(10^r - 1) \in \mathbb{Q}$, a rational number.

Conversely, suppose that $p = M/N$ is a rational number. Then we can divide $M$ by $N$ to give an integer $m$ and a remainder $r_1 < N$. We can write this as $M = mN + r_1$. This implies $p = M/N = m + r_1/N$. Repeat the argument with $10r_1$ to get $10r_1 = m_1 N + r_2$.

$$\begin{aligned} M &= mN + r_1 \\ 10r_1 &= m_1 N + r_2 \\ 10r_2 &= m_2 N + r_3 \\ &\cdots \end{aligned}$$

$$\begin{aligned}\frac{M}{N} &= m + \frac{r_1}{N} \\ &= m + \frac{m_1}{10} + \frac{r_2}{10N} \\ &= m + \frac{m_1}{10} + \frac{m_2}{100} + \frac{r_3}{100N} \\ &\dots\end{aligned}$$

This gives the decimal expansion of $p$; but all the remainders $r_k$ are less than $N$, so that there are at most $N$ different such remainders. After at most $N$ such divisions, the next remainder must be one of the values $r_1, \dots, r_N$, and hence we end up in a cycle i.e. a recurring decimal expansion.

□

**Definition** The set of **irrational** numbers is $\mathbb{R} - \mathbb{Q}$.

### 6.0.3 Exercises

1. Show that if $|x| < \epsilon$ then $-\epsilon < x < \epsilon$.
2. Prove the following properties of the absolute value:
$$|-a| = |a|, \quad |a+b| \leqslant |a| + |b|.$$
3. Prove that distinct real numbers cannot have the same decimal expansion as follows: suppose $x$ and $y$ are two distinct real numbers. Use the Archimedean property to show that there is an $n \in \mathbb{N}$ such that $1/10^n < |x-y|$, and hence that they differ at the $n$th decimal place or before.
4. Find the binary expansion (the first few terms) of $\pi$ and $e$.
5. Write the real number $0 \cdot 185324324\dots$ as a fraction.
6. Show that the set of numbers $\{\, 1, 1.1, 1.11, \dots \}$ has a supremum equal to $10/9$ which is not a maximum.
7. Show, by contradiction, that the sum or product of a rational number and an irrational number is irrational.
8. Deduce that the set of irrational numbers is dense in $\mathbb{R}$.

# 7 Complex Numbers ℂ

With the set of real numbers $\mathbb{R}$, we cannot solve the equation $x^2+1=0$, since $x^2 \geqslant 0$ for any real number $x$ (see the proof that $m^2 \geqslant 0$ for the integers).

**Definition** A **complex** number is a pair of real numbers $z=(a,b)$; the set of complex numbers $\mathbb{C}=\mathbb{R}\times\mathbb{R}$.

*Addition* and *multiplication* of complex numbers is defined by:

$$(a,b)+(c,d)=(a+c,b+d)$$

$$(a,b)\cdot(c,d)=(ac-bd,ad+bc)$$

For convenience we write $a=(a,0)$ and $ib=(0,b)$ so that every complex number can be written as

$$z=(a,b)=(a,0)+(0,b)=a+ib.$$

Hence the addition and multiplication of complex numbers in this notation is

$$(a+ib)+(c+id)=(a+c)+i(b+d),$$

$$(a+ib)(c+id)=(ac-bd)+i(ad+bc).$$

The notation is consistent in the sense that $ai=(a,0)\cdot(0,1)=(0,a)$. Complex numbers of the type $ib$ are sometimes called purely imaginary; they may have seemed mysterious a long time ago, but you can see that there's really nothing fictitious about them.

Notice that now $i^2=(0,1)\cdot(0,1)=(-1,0)=-1$. Similarly $(-i)^2=-1$. We have found two complex solutions to the equation $x^2+1=0$.

We cannot define a 'less than' relation on $\mathbb{C}$, since suppose there were such a relation $\leqslant$; then whether $0<i$ or $0>i$ (in which case $-i>0$), we have $0<i^2=-1$ (or $0<(-i)^2=-1$) which implies that $1<0<-1$ (by adding 1 on both sides); hence, multiplying by the 'positive' $-1$ we get $1<0<1$ a contradiction.

We can check that the associative, commutative, identity, inverses and distributive properties hold for $\mathbb{C}$. For example the zero complex number is $0=(0,0)$, the negative of $z=a+ib$ is $-z=(-a)+i(-b)$, while its multiplicative inverse is $z^{-1}=\frac{a}{a^2+b^2}+i\frac{-b}{a^2+b^2}$.

So now we have reached our aim of having a number system with the usual algebraic properties, but without a compatible order relation, which solves all linear equations as well as $x^2 + 1 = 0$. What about the other polynomial equations? The remarkable "fundamental theorem of algebra" (which is proved in a course on complex numbers) states that *every* polynomial equation (even those with complex number coefficients) have solutions in $\mathbb{C}$. As far as algebraic equations are concerned, the set of complex numbers is sufficient to get all solutions; we do not need to extend any further to more esoteric number systems.

**Definition** The **modulus** of a complex number $z = a + ib$ is defined as

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

## 7.1 Exponential Function

**Definition**

$$e^z = \sum_{n=0}^{\infty} \frac{1}{n!} z^n$$

In particular, when $z = x$ is real, then the exponential function reduces to the familiar real exponential function.

*Proposition* 7.1.1

$$\textbf{(i)} \qquad \frac{d}{dz} e^z = e^z;$$

$$\textbf{(ii)} \qquad e^{z_1+z_2} = e^{z_1} e^{z_2}.$$

Proof. Differentiating with respect to $x$ gives $\frac{d^{dx}}{dd^{dx}} e^x = \sum_{n=0}^{\infty} \frac{1}{n!} n x^{n-1} = \sum_{n=1}^{\infty} \frac{1}{(n-1)!} x^{n-1} = e^x$. More generally, $\frac{d^{dz}}{dd^{dz}} e^z = e^z$.

Now consider the function $f(z) = e^{z_2 - z} e^z$, and differentiate with respect to $z$: $f'(z) = -e^{z_2-z} e^z + e^{z_2-z} e^z = 0$, hence $f(z) = c$ constant; but $f(0) =$

$e^{z_2}$ so that $e^{z_2} = e^{z_2-z}e^z$ for any $z$ and $z_2$. Substitute $z = z_1 + z_2$ to get $e^{z_2} = e^{-z_1}e^{z_2+z_2}$ (1). Putting $z_2 = 0$ shows that $1 = e^{-z}e^z$ for any $z \in \mathbb{C}$ ie $e^{-z} = 1/e^z$. Hence the required identity is obtained from equation (1).

□

When $z = ix$ is purely imaginary, we get

$$e^{ix} = \sum_{n=0^\infty} \frac{1}{n!} i^n x^n = \left( \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k)!} x^{2k} \right) + i \left( \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k+1)!} x^{2k+1} \right).$$

Its real part is called the cosine of $x$, the imaginary part is called the sine of $x$:

**Definition**

$$\cos x = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n)!} x^{2n},$$

$$\sin x = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)!} x^{2n+1}.$$

Applying this to $z = x + iy$ gives

$$e^{x+iy} = e^x e^{iy} = e^x \cos(y) + ie^x \sin(y).$$

In particular the identity $e^{i\theta}e^{i\psi} = e^{i(\theta+\psi)}$ becomes the identities

$$\cos(\theta + \psi) = \cos(\theta)\cos(\psi) - \sin(\theta)\sin(\psi),$$

$$\sin(\theta + \psi) = \cos(\theta)\sin(\psi) + \sin(\theta)\cos(\psi).$$

### 7.1.1 Polar Form

**Definition** The **argument** (or *angle*) of a complex number $a+ib$ is defined as that real number in the range $-\pi < \theta \leqslant \pi$,

$$\theta = \arctan(b/a) : a + ib = r(\cos\theta + i\sin\theta) = re^{i\theta}.$$

The **logarithm** of $a + ib$ is then defined as

$$\log z = \log r + i\theta.$$

The **power** of two complex numbers is

$$z^w = e^{w \log z}.$$

What other numbers are there? The Algebraic Numbers are those complex numbers that are solutions of some polynomial equation with integer coefficients. These form a countable set. The transcendental numbers are the complex numbers that are not algebraic.

Vectors are ordered sets of real or complex numbers: we can define addition and 'scalar' multiplication on them. On some dimensions we can define a proper multiplication; obviously $\mathbb{C}$ consists of ordered pairs of real numbers, but more generally can define the quaternions on $\mathbb{R}^4$, the octonions (on $\mathbb{R}^8$), the sedonians (on $\mathbb{R}^16$) etc but the multiplication gets more and more complicated, satisfying less and less of the axioms we mentioned.

## 7.2 Exercises

1. Use induction to show that $z^n = |z|^n(\cos n\theta + i \sin n\theta$ for $z = |z|(\cos\theta + i \sin\theta)$.

2. Find the logarithm of $i$, $-i$ and $1 + i$.

3. Show that $\log(zw)$ need not be equal to $\log z + \log w$ for all values of $z, w \in \mathbb{C}$. Deduce that $z^{w_1+w_2} = z^{w_1} z^{w_2}$ need not be true.

4. What is wrong with the following argument? $1 = \sqrt{1} = \sqrt{(-1)(-1)} = \sqrt{-1}\sqrt{-1} = i^2 = -1$.

# 8 Functions

**Definition** A **function** is a rule which takes elements from a set $X$, called the **domain**, and gives an element from a set $Y$, called the **codomain**, denoted by

$$\begin{aligned} f: \ & X \to Y \\ & x \mapsto f(x) \end{aligned}$$

such that for each element $x \in X$ the rule gives a single element $f(x) \in Y$ ie

$$\forall a, b \in X \quad a = b \ \Rightarrow \ f(a) = f(b)$$

Two functions are considered to be equal when they have the same domains and codomains and for each $x \in X$, we have $f(x) = g(x)$.

The graph of a function is the set $\{ (x, f(x)) : x \in X \} \subseteq A \times B$.

Examples: The rules $x \mapsto x^2$ and $x \mapsto e^x$ are both functions on the real numbers and the complex numbers (they are considered as different).

**Definition** A function $f$ can also be used to map subsets of the domain $A \subseteq X$ by

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

Conversely, for a subset $B \subseteq Y$, we denote

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

The **range** or **image** of a function $f$ is the set $fX$. Note that the image of a function need not be the whole of the codomain.

**Definition** A function $f : A \to B$ is called **onto** or **surjective** when its image equals the codomain ie

$$\forall y \in Y, \ \exists x \in X, \quad f(x) = y.$$

A function is called **1-1** or **injective** when distinct elements of $X$ are mapped to distinct elements of $Y$ ie

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

A function is called **bijective** when it is 1-1 and onto.

Notice that by changing the codomain to equal the range, we can always make a function onto. By restricting the domain, we can always make a function 1-1.

### 8.0.1 Examples

The exponential function exp: $\mathbb{R} \to \mathbb{R}$ defined by $x \mapsto e^x$ is not onto but is 1-1. The sine function $\sin : \mathbb{R} \to \mathbb{R}$ is not onto and not 1-1. The cubic function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^3 - x$ is onto but not 1-1. The tangent function $\tan : (-\pi/2, \pi/2) \to \mathbb{R}$ is 1-1 and onto.

*Proposition* 8.0.1

$$f(A \cup B) = fA \cup fB,$$

$$\textbf{i.e. } x \in A \cup B \Leftrightarrow f(x) \in fA \cup fB.$$

Proof. Let $y \in f(A \cup B)$; that is $y = f(x)$ for some $x \in A \cup B$. Then,

$$y = f(x) \quad \exists x \in A \text{ OR } x \in B,$$

$$\Leftrightarrow y \in fA \text{ OR } y \in fB,$$

$$\Leftrightarrow y \in fA \cup fB.$$

□

*Proposition* 8.0.2

$$f(A \cap B) \subseteq fA \cap fB,$$

$$x \in A \cap B \;\Rightarrow\; f(x) \in fA \cap fB.$$

Proof. Let $y \in f(A \cap B)$, that is $y = f(x)$ with $x \in A \cap B$. Then $y = f(x) \in fA$ since $x \in A$ and $y = f(x) \in fB$ since $x \in B$, so that $y \in fA \cap fB$.

□

Note that the converse is false ie $f(x) \in fA \cap fB \not\Rightarrow x \in A \cap B$.

## 8.1 Composition

**Definition** The **composition** of two functions, $f : X \to Y$ and $g : Y \to Z$ is the function $g \circ f : X \to Z$ defined by

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

*Proposition* 8.1.1

**The composition of functions is associative,**

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

Proof. To show that the two functions $h \circ (g \circ f)$ and $(h \circ g) \circ f$ are equal we need to check that their domains and codomains are the same, and that they map the elements in identical ways.

The domains of both functions is $X$, and their codomains are $Z$. Now let $x \in X$; then $g \circ f(x) = g(f(x))$ so that $h \circ (g \circ f)(x) = h((g \circ f)(x)) = h(g(f(x)))$; similarly $((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x))$.

□

Note that composition of functions is not in general commutative ie $f \circ g \neq g \circ f$. For example, $\sin(x^2) \neq (\sin x)^2$.

*Proposition* 8.1.2

**(i) If $f$ and $g$ are 1-1, then so is $g \circ f$.**
**(ii) If $f$ and $g$ are onto, then so is $g \circ f$.**

Proof. Suppose that $g \circ f(x) = g \circ f(y)$. Then $g(f(x)) = g(f(y))$, therefore $f(x) = f(y)$ since $g$ is 1-1, and so $x = y$ since $f$ is 1-1.

Let $z \in Z$; then there is an element $y \in Y$ such that $g(y) = z$ since $g$ is onto. Then there is also another element $x \in X$ such that $f(x) = y$ since $f$ is onto. Combining the two we get,

$$g \circ f(x) = g(f(x)) = g(y) = z.$$

□

## 8.2 Identity Function

**Definition** The identity function on a set $X$ is the function

$$\begin{aligned} \iota_X : X &\to X \\ x &\mapsto x \end{aligned}$$

*Proposition* 8.2.1

$$\iota_Y \circ f = f, \qquad f \circ \iota_X = f.$$

Proof. The domains of $\iota_Y \circ f$, $f \circ \iota_X$ and $f$ are all $X$; their codomains are all $Y$. Moreover, letting $x \in X$ we get

$$\iota_Y \circ f(x) = \iota_Y(f(x)) = f(x),$$

$$f \circ \iota_X(x) = f(\iota_X(x)) = f(x).$$

□

## 8.3 Inverse Functions

**Definition** The **inverse** of a function $f : X \to Y$ is another function, denoted by $f^{-1} : Y \to X$ such that $f^{-1} \circ f = \iota$ and $f \circ f^{-1} = \iota$.

Not every function has an inverse function. Functions that are not onto, or that are not 1-1 cannot have inverse functions, either because it would not be defined on the whole of $Y$ or because there would be more than one $x \in X$ to map to.

*Proposition* 8.3.1

**A function has an inverse function if, and only if, it is bijective.**

Proof. Suppose $f$ is invertible; then $f^{-1}(f(x)) = x$, and $f(f^{-1}(y)) = y$. Suppose that $f(x_1) = y = f(x_2)$; then $x_1 = f^{-1}(f(x_1)) = f^{-1}(y) = f^{-1}(f(x_2)) = x_2$ so that $f$ is 1-1. Next, let $y \in Y$, and let $x = f^{-1}(y)$; then $f(x) = f(f^{-1}(y)) = y$, so that $f$ is onto as well.

Conversely, suppose $f : X \to Y$ is bijective (1-1 and onto). Then for every $y \in Y$ there will always be elements $x \in X$ such that $f(x) = y$. But since $f$ is 1-1, there must be exactly one element $x$ which maps to $y$. Hence we can define the map $f^{-1} : Y \to X$ by mapping $y$ to this unique $x$. Moreover,

$$f^{-1} \circ f(x) = f^{-1}(f(x)) = f^{-1}(y) = x,$$

$$f \circ f^{-1}(y) = f(f^{-1}(y)) = f(x) = y.$$

□

## 8.4 Exercises

1. Find examples of functions that are (i) bijective, (ii) 1-1 but not onto, (iii) onto but not 1-1, (iv) neither 1-1 nor onto.

2. Show that if $f$ is 1-1, then $f(A \cap B) = fA \cap fB$, and $(fA)' \subseteq f(A')$ for any subset $A$ of the domain. When does equality hold?

3. Show that for any function $f : X \to Y$ and any subsets $B \subseteq Y$ and $A \subseteq X$, then $A \subseteq f^{-1}fA$ and $ff^{-1}B \subseteq B$. Moreover prove that when $f$ is 1-1, $A = f^{-1}fA$ and when $f$ is onto, $ff^{-1}B = B$. Find examples of functions for which these equalities are false.

4. Let $f(x) = (ax + b)/(cx + d)$ be defined on all real numbers except $x = -d/c$. Show that it is bijective when $ad - bc \neq 0$, and find its inverse. Now let $g(x) = (px + q)/(rx + d)$ with $ps - qr \neq 0$. Show that $g \circ f$ is another function of the same type, and verify that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

5. Show that the function $f(x) = (x + 1/x)/2$ is a bijection on the set $J = \{\, x \in \mathbb{R} : x \geqslant 1 \,\}$.

6. Use the functions $f(x) = x + 1$ and $g(x) = x - 1/x$ to show that the statement "$f \circ g$ is a bijection $\Rightarrow$ $f, g$ are bijections" is false.

7. Let $f : X \to Y$ be a function. Define the relation $\sim$ on the set $X$ by

$$x_1 \sim x_2 \Leftrightarrow f(x_1) = f(x_2).$$

Show that $\sim$ is an equivalence relation and find the equivalence classes.

# 9 Cardinality

How do we count objects? We take the set of objects and mentally label each element by a number in the order 1, 2, 3, etc. When we arrive at the last object, the number last called out is the number of the set.

| ♠ | ♡ | ♢ | ♣ | © | £ |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 |

To count correctly, we need to make sure that we don't leave any object out and that we don't count an object twice. Mathematically speaking, we are creating a function from the set of objects to a subset of the natural numbers which is 1-1 and onto ie a bijection,

$$f : \{ \spadesuit, \heartsuit, \diamondsuit, \clubsuit, ©, £ \} \to \{ 1, 2, 3, 4, 5, 6 \}$$

**Definition** Two sets are **cardinally equivalent**, $A \equiv B$, when there is a bijection map between them, $f : A \to B$ 1-1 and onto.

In this point of view, the sets $\{ 1, 2, 3 \}, \{ \text{one}, \text{two}, \text{three} \}, \{ I, II, III \}$ are all essentially the "same" as far as sets are concerned.

*Proposition* 9.0.1

**Cardinal equivalence is an equivalence relation.**

Proof. For any set $A$, $A \equiv A$ since $\iota : A \to A$ is a bijective map, so that the relation is reflexive.

If $A \equiv B$ then there is a bijective map $f : A \to B$. Then $f^{-1} : B \to A$ is also a bijective map, so that $B \equiv A$, and the relation is symmetric.

If $A \equiv B$ and $B \equiv C$ then we have two bijective maps $f : A \to B$ and $g : B \to C$. Then $g \circ f : A \to C$ is also a bijective map, so that $A \equiv C$, and the relation is transitive.

□

This means that we can partition all the sets into equivalence classes. Each equivalence class can be assigned a cardinal number, that is a set of numbers that has the same number of elements.

The simplest equivalence class is that of the empty set itself. Its cardinal number is defined to be $0 = \{ \} = \varnothing$.

Next, there are all the sets with one element, and assigned the cardinal number $1 = \{\,0\,\}$.

The sets with two elements are all cardinally equivalent to the number $2 = \{\,0, 1\,\}$; and so on.

**Definition** A set is called **finite** if it has cardinality equal to $n$ for some $n \in \mathbb{N}$; that is, if it is cardinally equivalent to a set $\{\,0, 1, \ldots, n-1\,\}$.

Otherwise, it is called **infinite**.

Of course, not all sets are finite. For example, the set of natural numbers $\mathbb{N}$ is not finite; for suppose $\{\,0, \ldots, N\,\} \equiv \mathbb{N}$, then there is a map $f$ with $f(0) = n_0, f(1) = n_1, \ldots, f(N) = n_N$. But take the maximum of the numbers $n_0, \ldots, n_N$; there is a natural number greater than all of them, say M. Then $f$ is not onto since it does not map to it, which is a contradiction.

**Definition** A set is called **countably infinite** when it is cardinally equivalent to the set of natural numbers, $A \equiv \mathbb{N}$.

A set is called *countable* when it is either countably infinite or finite.

*Proposition* 9.0.2

**The set of integers is countably infinite, $\mathbb{Z} \equiv \mathbb{N}$.**

Proof. Consider the function

$$\begin{aligned} f : \quad & \mathbb{N} \to \mathbb{Z} \\ & n \mapsto \begin{cases} -k & \text{when } n = 2k \\ k & \text{when } n = 2k-1 \end{cases} \end{aligned}$$

Then $f$ is 1-1, since suppose that $f(n_1) = f(n_2) = k$; then if $k$ is positive, it must be the case that $n_1 = 2k - 1 = n_2$; if negative then $n_1 = 2k = n_2$. In either case $n_1 = n_2$.

$f$ is also onto, since let $a \in \mathbb{Z}$. If $a$ is positive, let $n = 2a - 1$, so that $f(n) = a$; if $a$ is negative, let $n = -2a$ so that $f(n) = -(-a) = a$.

Hence $f$ is a bijection between $\mathbb{Z}$ and $\mathbb{N}$.

□

*Proposition* 9.0.3

**If $A_1$, $A_2$, ... are countably infinite, then so is $\bigcup_{n=1}^{\infty} A_n$.**

Proof. The fact that the sets $A_n$ are countably infinite means that there are bijective maps $f_n : \mathbb{N} \to A_n$, say mapping $f_n(m) = a_{nm}$. Hence we have the following lists,

$$A_1 = \{\, a_{11}, a_{12}, a_{13}, \dots \}$$
$$A_2 = \{\, a_{21}, a_{22}, a_{23}, \dots \}$$
$$A_3 = \{\, a_{31}, a_{32}, a_{33}, \dots \}$$
$$\dots$$

We can therefore make a list of $\bigcup_{n=1}^{\infty} A_n$ by listing the elements diagonally as

$$\{\, a_{11}, a_{12}, a_{21}, a_{13}, a_{22}, a_{31}, \dots \},$$

and so create the function $g : \mathbb{N} \to \bigcup_n A_n$ by letting $g(1) = a_{11}, g(2) = a_{12}, g(3) = a_{21}, g(4) = a_{13}, g(5) = a_{22}, \dots$. This function is 1-1 and onto because we never repeat elements and we don't leave out any $a_{nm}$. Hence $\mathbb{N} \equiv \bigcup_n A_n$.

□

**Corollary**

**If $A$ is countably infinite, then so is $A \cup \{\, x \,\}$.**

*Proposition* 9.0.4

**If $A$ is countable, then so is any subset $B \subseteq A$.**

Proof. Exercise.

*Proposition* 9.0.5

**If $A$ and $B$ are countably infinite, then so is $A \times B$.**

Proof. Let $A = \{\, a_1, a_2, \dots \}$ and $B = \{\, b_2, b_2, \dots \}$ be countably infinite sets. Then we can use the same diagonal listing sequence as in the previous proposition to make a listing of $A \times B$ as

$$A \times B = \{\, (a_1, b_1), (a_1, b_2), (a_2, b_1), (a_1, b_3), (a_2, b_2), \dots \}.$$

Hence we can create a bijective map from $\mathbb{N}$ to $A \times B$.

□

*Proposition* 9.0.6

**The set of rational numbers is countably infinite, $\mathbb{Q} \equiv \mathbb{N}$.**

Proof. The set of integers is countably infinite. Hence $\mathbb{Z} \times \mathbb{Z}$ is also countably infinite; but $\mathbb{Q}$ is a subset of $\mathbb{Z}^2$ since each rational number is a pair of integers, hence it is itself countably infinite.

□

**Theorem** A

**The set of real numbers is not countably infinite.**

Proof. Suppose that $\mathbb{R} \equiv \mathbb{N}$, that is it can be listed as $\mathbb{R} = \{ x_1, x_2, x_3, \dots \}$. Write out each real number in the list as a decimal expansion:

$$\begin{aligned} x_1 &= m_1 \cdot n_{11} n_{12} n_{13} \dots \\ x_2 &= m_2 \cdot n_{21} n_{22} n_{23} \dots \\ x_3 &= m_3 \cdot n_{31} n_{32} n_{33} \dots \\ &\dots \end{aligned}$$

Now consider the real number $y = 0.m_1 m_2 m_3 \dots$ where $m_1 \neq n_{11}, m_2 \neq n_{22}, m_3 \neq n_{33}, \dots, m_k \neq n_{kk}, \dots$. It follows that $y \neq x_1$ since they differ in the first decimal position (ie $m_1 \neq n_{11}$); similarly $y \neq x_2$ because they differ in the second decimal position etc. In fact $y \neq x_n$, $\forall n$. That is $y$ is a real number that is not in the list; but the list was supposed to be exhaustive of all the real numbers, a contradiction.

□

This is a stunning result, that not all infinite sets are cardinally equivalent; some infinite sets have more elements than other infinite sets! In fact, there are infinite sets which are not cardinally equivalent to either $\mathbb{N}$ or to $\mathbb{R}$; the

number of equivalence classes of infinite sets is itself infinite: there are an infinity of infinities!

We can arrange sets in increasing order of their cardinality, as follows:

| Sets | Cardinal Number |
|---|---|
| $\varnothing$ | 0 |
| $\{ * \}$ | 1 |
| $\{ *, \circ \}$ | 2 |
| $\ldots$ | |
| $\{ a_1, \ldots, a_n \}$ | n |
| $\ldots$ | |
| $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \ldots$ | $\omega$ |
| $\mathbb{R}, \mathbb{C}, \ldots$ | c |
| $\ldots$ | $\ldots$ |

We assign the cardinal number $\omega$ to all the countably infinite sets, and the cardinal number $c$ to all the sets that are cardinally equivalent to $\mathbb{R}$.

For example, every interval of the type $[a, b], [a, b), (a, b)$ etc. have cardinality equal to $c$.

The set of irrational numbers $\mathbb{R} - \mathbb{Q}$ is uncountable since suppose it were countable; then $\mathbb{R} = \mathbb{Q} \cup \mathbb{Q}'$ would itself be countable, which it isn't.

## 9.1 Exercises

1. Show that (i) the set of square numbers $\{ 1, 4, 9, \ldots \}$, (ii) $\mathbb{Q} \times \mathbb{Q}$, are countably infinite.

2. Prove that every infinite set has a proper subset which is itself infinite.

3. Show that if the sets $\{ 1, \ldots, n \}$ and $\{ 1, \ldots, m \}$ are cardinally equivalent then $n = m$.

4. Prove that $\mathbb{C}$ is cardinally equivalent to $\mathbb{R}$.

5. Show that the set of functions $f : \mathbb{N} \to \mathbb{N}$ is uncountable.

6. Show that the set of polynomials with integer coefficients is countably infinite. Deduce that the set of algebraic numbers (the roots of such polynomials) is also countably infinite; and hence that the set of transcendental numbers is uncountable.