

LEARNING TO CRAWL:
ELEMENTARY ALGEBRA

LUKE COLLINS
maths.com.mt

Version 0.6* (23rd January, 2020)

*Algebra is generous; she often gives more
 than is asked of her.*

— Jean-Baptiste le Rond d’Alembert

Contents

1	Introduction	3
1.1	Preliminary Techniques	3
1.2	The Real Numbers	6
2	Square Roots and Indices	12
2.1	Square Roots	12
2.2	Surds and Surd Form	15
2.3	Indices	20
3	Quadratics	24
3.1	Solving Quadratic Equations	24
3.2	Theory of Quadratic Equations	32
4	Logarithms	40

*If you find any mathematical, grammatical or typographical errors whilst reading these notes, please let the author know via email: luke.collins@um.edu.mt.

5	Polynomials	44
5.1	The Basics and Polynomial Division	44
5.2	The Remainder and Factor Theorems	53
5.3	Partial Fractions	63
6	The Binomial Theorem	68
6.1	The Binomial Theorem	68
6.2	Pascal's Triangle and Recursion	68
	Appendix A Naïve Set Theory	69
	Appendix B Supplementary Proofs	79
	B.1 Proof of Corollary on Quadratic Equations	79
	Appendix C Answers to Exercises	81

1 Introduction

The word *algebra*, from the Arabic *al-jabr* (in Maltese, *għall-gabra*) refers to the study of manipulation of mathematical symbols. The goal of algebra is to abstract away unnecessary details so that we can think more generally, using symbols in place of more concrete objects (such as numbers).

Throughout these notes, we assume basic symbols and notations of sets. Take a look at [appendix A](#) if any of the symbols are new to you.

We take quite a formal approach to things, building off definitions and proving things every step of the way. It is not important to learn the proofs here by heart, but it is important to read and understand them well. In the exam, you will have to produce proofs of your own, often of results which you have never seen before. Thus the way proofs are written and presented, as well as the difference between what we are allowed to assume and what we aren't, are essential to proving things correctly.

Moreover, in more advanced topics, mathematical jargon of the kind we present here is vital to be able to explain things as succinctly as possible. Thus, even if it seems like we are using verbose language to describe something which could otherwise be stated more matter-of-factly; the goal is to familiarise you with language we will rely on in the future.

It is important to work through all the exercises, not only to reinforce what you have learned, but to also garner sufficient instincts for what is to come. It is not enough to be able to do the exercises—by the end of them, you should be able to do similar exercises *easily*, almost without thinking. This way, when we go on to more advanced topics, your focus will be entirely on the new material, and you will not sacrifice any of your brain's “processing power” to understand the basic algebra.

When exercises are annotated with a ☞ symbol, this is instructing you to pour yourself some tea and dedicate some time to think about the problem, it might be harder than the others.

1.1 Preliminary Techniques

Before we start the material of the course, you are encouraged to work through the following exercise. The ability to solve such basic problems will be assumed.

Exercise 1.1. 1. LINEAR EQUATIONS IN ONE VARIABLE

Solve the following equations.

a) $3x + 4 = 16$

b) $7x - 4 = 24$

c) $3x + 4 = x + 16$

d) $3x - 5 + 2x = 1 - x + 5x$

e) $\frac{x}{2} - \frac{x}{3} = 8$

f) $\frac{y}{6} + \frac{y}{4} = 5$

g) $\frac{n}{5} + n = \frac{n}{3} + 13$

h) $\frac{t}{4} - \frac{t}{5} = \frac{t}{2} - 18$

i) $\frac{m}{3} + \frac{m}{2} = m - \frac{1}{6}$

j) $\frac{\theta}{4} + \frac{1}{2} + 3\theta = 2\theta + 3$

k) $\frac{5}{q+5} = \frac{3}{q+7}$

l) $\frac{1-y}{1+y} = \frac{2}{3}$

m) $\frac{1}{7}(x+1) - \frac{1}{11}(x-2) = 1$

n) $\frac{1}{x+1} = \frac{3}{4(x+1)} + \frac{1}{12}$

o) $\frac{4}{2s+1} - \frac{2}{3(2s+1)} = \frac{5}{9}$

p) $\frac{1}{7}(x+2) + 3 = \frac{x+3}{2}$

q) $\frac{3x}{2} \left(2 + \frac{2}{x} \right) + 7x - 3 = \frac{1}{4}(39x + 7)$

2. SIMULTANEOUS LINEAR EQUATIONS IN TWO VARIABLES

Solve each of the following systems of equations.

a)
$$\begin{cases} 6x + 2y = 30 \\ 4x + 3y = 30 \end{cases}$$

b)
$$\begin{cases} 2x + 21 = 5y \\ 4x + 3y = 23 \end{cases}$$

c)
$$\begin{cases} 3x + 33 = 9y \\ 5x + 4y = 40 \end{cases}$$

d)
$$\begin{cases} 3x + 3 = 6y \\ 5x - 6y = 7 \end{cases}$$

e)
$$\begin{cases} x + 9y = 34 \\ 4x - 5y = 13 \end{cases}$$

f)
$$\begin{cases} 6x - 3y = 3 \\ 4x + 5 = 3y \end{cases}$$

g) Alice has more money than Bob. If Alice gave Bob €20, they would have the same amount. While if Bob gave Alice €22, Alice would then have twice as much as Bob. How much does each one actually have?

h) A woman is now 30 years older than her son. 15 years ago, she was twice as old. What are the present ages of the woman and her son?

3. Solve for x .

a) $x + y = 2x - 3z$

b) $x + yx + zx = 3 - x + 4xyz$

c) $x = \frac{x + y + z^2}{y - 3z}$


d) $\frac{1}{x} + \frac{1}{w} = \frac{1}{z}$

e) $\frac{1}{w} + \frac{1}{y} + \frac{1}{x} = \frac{1}{z}$

f) $yz = \frac{y + z/x}{z + y/x}$

4. A man was looking at a portrait. Someone asks him: “Whose picture are you looking at?” He replied: “Brothers and sisters I have none, but this man’s father, is my father’s son.” (“This man’s father”, means of course, the father of the man in the picture).

Whose picture was the man looking at?

 5. Consider three brothers named John, James and William. John and James (the two J’s) always lie, but William always tells the truth. The three are indistinguishable in appearance. You meet one of the three brothers on the street one day and wish to find out whether he is John (because John owes you money). You are allowed to ask him one question answerable by yes or no, but the question may not contain more than three words!

What question would you ask?^a

^aThis delightful problem was taken from the excellent book *To Mock a Mocking Bird* by Raymond Smullyan, which provides a nice informal introduction to combinatory logic using these kinds of logical puzzles (equivalent to the λ -calculus, for those of who study computing.)

1.2 The Real Numbers

The set of real numbers \mathbb{R} is the object we work with the most throughout the course, although we will consider other mathematical objects in later topics (functions, vectors, matrices, complex numbers, etc.). The essential, defining properties which the real numbers obey are summarised nicely in [theorem 1.2](#).

Theorem 1.2 (\mathbb{R} is an Ordered Field). *Let $x, y, z \in \mathbb{R}$, and let $+$ and \cdot denote addition and multiplication. Then the following properties hold.*

- I. $x + y \in \mathbb{R}$ (CLOSURE OF $+$)
- II. $x + (y + z) = (x + y) + z$ (ASSOCIATIVITY OF $+$)
- III. *There is a number $0 \in \mathbb{R}$ such that for any x , $x + 0 = 0 + x = x$* (IDENTITY FOR $+$)
- IV. *For each x , there is a number $-x \in \mathbb{R}$, such that $x + -x = -x + x = 0$* (INVERSE FOR $+$)
- V. $x + y = y + x$ (COMMUTATIVITY OF $+$)
- VI. $x \cdot y \in \mathbb{R}$ (CLOSURE OF \cdot)
- VII. $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ (ASSOCIATIVITY OF \cdot)
- VIII. *There is a number $1 \in \mathbb{R}$ such that for any x , $x \cdot 1 = 1 \cdot x = x$* (IDENTITY FOR \cdot)
- IX. *For each x , if $x \neq 0$, then there is a number $\frac{1}{x}$ such that $x \cdot \frac{1}{x} = \frac{1}{x} \cdot x = 1$* (INVERSE FOR \cdot)
- X. $x \cdot y = y \cdot x$ (COMMUTATIVITY OF \cdot)
- XI. $x \cdot (y + z) = x \cdot y + x \cdot z$ (DISTRIBUTIVITY OF \cdot OVER $+$)
- XII. *If $x \leq y$ and $y \leq x$, then $x = y$* (ANTISYMMETRY OF \leq)
- XIII. *If $x \leq y$ and $y \leq z$, then $x \leq z$* (TRANSITIVITY OF \leq)
- XIV. $x \leq y$ or $y \leq x$ (TOTALITY OF \leq)
- XV. *If $x \leq y$, then $x + z \leq y + z$* (ORDER PRESERVATION $+$)
- XVI. *If $0 \leq x$ and $0 \leq y$, then $0 \leq x \cdot y$* (ORDER PRESERVATION \cdot)

We are actually glossing over a key detail here. Upon reading these “defining properties”, a natural you might ask is: “then what’s the difference between

\mathbb{Q} and \mathbb{R} ?”, and indeed, you would be right in asking this, because the rationals are also an ordered field (i.e., they obey all the properties I–XVI of [theorem 1.2](#) too). The rationals \mathbb{Q} are, in a sense, the “smallest” set of numbers obeying these properties, but it has “holes”, i.e., numbers which “should” be there, but aren’t (such as $\sqrt{2}$, which we proved is not rational in [appendix A](#)). When we think of the number line, we think of a continuum of numbers without holes. So in the case of $\sqrt{2}$, we have the approximations

$$\begin{array}{ll}
 1.4 = \frac{14}{10} & 1.4^2 = 1.96 \\
 1.41 = \frac{141}{100} & 1.41^2 = 1.9881 \\
 1.414 = \frac{1414}{1000} & 1.414^2 = 1.999396 \\
 1.4142 = \frac{14142}{10000} & 1.4142^2 = 1.99996164 \\
 1.41421 = \frac{141421}{100000} & 1.41421^2 = 1.9999899241 \\
 1.414213 = \frac{1414213}{1000000} & 1.414213^2 = 1.999998409369 \\
 & \vdots
 \end{array}$$

each of which is rational, but we should also have a number at the end of this process whose square is *exactly* 2, namely $\sqrt{2}$, having infinitely many decimals in its expansion. (Note that just because a number has infinitely many decimals, doesn’t necessarily mean it isn’t rational, think of $1/3 = 0.333\dots$). We will explore the more technical details behind this in later chapters, but for now, we will simply say that the real numbers \mathbb{R} are defined by the properties I – XVI, plus the property

XVII. *Any integer followed by an infinite sequence of decimals defines a valid real number,*

which is called the *completeness of the real numbers*.¹ We will not talk more of completeness in this chapter, since it is more of an analytic property of the real numbers rather than an algebraic one.²

¹See https://en.wikipedia.org/wiki/Completeness_of_the_real_numbers if you are interested in more details.

²When we say “analytic”, we are referring to (real) analysis, which is the study of continuous things, which heavily relies on the completeness of the real numbers in particular.

From now on, we will assume nothing about the real numbers apart from the properties listed above in [theorem 1.2](#). Even though you likely have previous knowledge of additional properties of real numbers, we approach the subject as if this is all we are allowed to use. Any other claims must be justified with proofs, which we will give throughout the notes (unless the proofs are tedious/complicated and derail us from the topic at hand, often these will be proofs involving the notion of completeness).

In fact, to expand our toolbox, let us start by proving some easy results about real numbers which follow from [theorem 1.2](#). All of these probably seem obvious to you, but how to prove them, allowing ourselves to only use I–XVI, is not always obvious!

Proposition 1.3. *Let $a, x, y \in \mathbb{R}$. Then*

- i) *The numbers 0 and 1 are unique,³*
- ii) *For each x , there is only one $-x$ and $\frac{1}{x}$ (where $x \neq 0$ for the latter),*
- iii) *$-(-x) = x$,*
- iv) *$x + a = y + a \implies x = y$,*
- v) *If $a \neq 0$, then $xa = ya \implies x = y$,*
- vi) *$x \cdot 0 = 0 \cdot x = 0$,*
- vii) *$x \cdot (-y) = (-x) \cdot y = -(x \cdot y)$,*
- viii) *$(-x) \cdot (-y) = x \cdot y$,*
- ix) *$(-1) \cdot x = -x$,*
- x) *$(-1) \cdot (-1) = 1$.*

Proof. For (i), suppose that there are two zeros, 0 and $\hat{0}$ both satisfying III, where $0 \neq \hat{0}$. Then by III,

$$0 = 0 + \hat{0} = \hat{0} + 0 = \hat{0},$$

contradicting that $0 \neq \hat{0}$. Replacing 0 and $\hat{0}$ with 1 and $\hat{1}$ above, the proof for 1 is the same by VIII.

Algebra on the other hand doesn't care about the real numbers particularly, but more about solving equations and manipulating expressions, whether they contain integers, rationals or reals.

³Meaning that 0 and 1 are the only numbers in \mathbb{R} satisfying III and VIII of [theorem 1.2](#) respectively.

For (ii), again suppose we have two minus x 's, $-x$ and $\ominus x$, both satisfying IV. Then by II, III and IV,

$$-x = -x + 0 = -x + (x + \ominus x) = (-x + x) + \ominus x = 0 + \ominus x = \ominus x,$$

contradicting that $-x \neq \ominus x$. A similar argument proves the uniqueness of $\frac{1}{x}$.

For (iii), by IV for $-x$, we have

$$\begin{aligned} -x + -(-x) &= 0 \implies x + (-x + -(-x)) = x + 0 \\ &\implies (x + -x) + -(-x) = x \\ &\implies 0 + -(-x) = x \\ &\implies -(-x) = x, \end{aligned}$$

as required.

For (iv),

$$\begin{aligned} x + a = y + a &\implies (x + a) + -a = (y + a) + -a \\ &\implies x + (a + -a) = y + (a + -a) \\ &\implies x + 0 = y + 0 \\ &\implies x = y, \end{aligned}$$

as required. A similar argument proves (v).

For (vi), we have

$$0 + x \cdot 0 = x \cdot 0 = x \cdot (0 + 0) = (x \cdot 0) + (x \cdot 0)$$

by XI. Hence by (iv), $0 = x \cdot 0 = 0 \cdot x$ by X.

For (vii), observe that

$$x \cdot y + x \cdot (-y) = x \cdot (y + -y) = x \cdot 0 = 0$$

by XI and (vi). Hence by (ii), $x \cdot (-y)$ is the unique inverse $-(x \cdot y)$ of $x \cdot y$. Similarly $(-x) \cdot y = -(x \cdot y)$.

Now for (viii), we have

$$(-x) \cdot (-y) = -((-x) \cdot y) = -(-(x \cdot y)) = x \cdot y$$

by (ii) and by (iii).

For (ix), observe that

$$x + (-1) \cdot x = x \cdot 1 + x \cdot (-1) = x \cdot (1 + -1) = x \cdot 0 = 0$$

by VIII, XI and (vi). Thus by (ii), $(-1) \cdot x$ is the unique inverse $-x$ of x .

Finally (x) follows by (ix) with $x = -1$, and we get $(-1) \cdot (-1) = -(-1) = 1$ by (iii). \square

Notice that proving these “obvious” results is quite similar to playing chess in some sense; we know what tile (on the chessboard) we want to get to, but we can only make valid moves according to the rules of the game. In our case, the “valid moves” are the properties of [theorem 1.2](#), and subsequent results we established from them.

Notation (Algebraic conventions). We relax the rigid notation introduced in [theorem 1.2](#) as follows.

- The product $x \cdot y$ is written simply as xy .
- The sum $x + -y$ is written simply as $x - y$.
- The product $x \cdot \frac{1}{y}$ is written as $\frac{x}{y}$. We call x the *numerator* and y the *denominator*.
- $x + (y + z) = (x + y) + z$ is denoted simply as $x + y + z$, and similarly $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ by xyz . Other similar relaxations are made when brackets are not necessary.

So for example, we write

$$\frac{3x - 5y}{1 + xyz} \quad \text{instead of} \quad (3 \cdot x + -(5 \cdot y)) \cdot \frac{1}{1 + x \cdot (y \cdot z)}.$$

Some consequences of our new notation are the familiar properties of [proposition 1.4](#).

Proposition 1.4. *Let $w, x, y, z \in \mathbb{R}$. Then*

- i) $\frac{1}{x} \cdot \frac{1}{y} = \frac{1}{xy}$,
- ii) $\frac{x}{y} \cdot \frac{w}{z} = \frac{xw}{yz}$,
- iii) $\frac{xy}{xz} = \frac{y}{z}$,
- iv) $\frac{x}{z} + \frac{y}{z} = \frac{x+y}{z}$,

$$v) \frac{x}{y} + \frac{w}{z} = \frac{xz+yw}{yz}.$$

Proof. For (i), notice that if we do

$$\begin{aligned} (xy) \cdot \left(\frac{1}{x} \cdot \frac{1}{y}\right) &= (yx) \cdot \left(\frac{1}{x} \cdot \frac{1}{y}\right) = y\left(x \cdot \left(\frac{1}{x} \cdot \frac{1}{y}\right)\right) \\ &= y\left(\left(x \cdot \frac{1}{x}\right) \cdot \frac{1}{y}\right) \\ &= y\left(1 \cdot \frac{1}{y}\right) = y \cdot \frac{1}{y} = 1, \end{aligned}$$

and consequently $\left(\frac{1}{x} \cdot \frac{1}{y}\right) \cdot (xy) = 1$ also by **theorem 1.2(x)**. Combining these facts, by **proposition 1.3(ii)**, it follows that $\frac{1}{x} \cdot \frac{1}{y}$ is the unique inverse $\frac{1}{xy}$ of xy , as required.

Then (ii) follows from (i) since $\frac{x}{y} \cdot \frac{w}{z} = x \frac{1}{y} \cdot w \frac{1}{z} = (xw) \cdot \left(\frac{1}{y} \cdot \frac{1}{z}\right) = xw \cdot \frac{1}{yz} = \frac{xw}{yz}$.

(iii) then follows easily from (ii): $\frac{xy}{xz} = \frac{x}{x} \cdot \frac{y}{z} = x \cdot \frac{1}{x} \cdot \frac{y}{z} = 1 \cdot \frac{y}{z} = \frac{y}{z}$.

(iv) uses **theorem 1.2(XI)**: $\frac{x}{z} + \frac{y}{z} = x \cdot \frac{1}{z} + y \cdot \frac{1}{z} = \frac{1}{z} \cdot x + \frac{1}{z} \cdot y = \frac{1}{z}(x + y) = (x + y) \frac{1}{z} = \frac{x+y}{z}$.

Finally (v) follows by (iii) and (iv): $\frac{x}{y} + \frac{w}{z} = \frac{zx}{zy} + \frac{yw}{yz} = \frac{zx}{yz} + \frac{yw}{yz} = \frac{xz+yw}{yz}$. \square

Exercise 1.5. Unless told otherwise, you may only use the facts of **theorem 1.2** to justify your answers to the following.

1. Why is $x + x = 2x$?
2. Solve the equation $2x + 1 = 3$, justifying each step you make by referencing one of **theorem 1.2**, **proposition 1.3** or **1.4**.
3. Do the same for the equation $\frac{x}{2} + \frac{x}{3} = 3 + \frac{1}{3}$.
4. Prove that $(a + b)(c + d) = ac + bc + ad + bd$.
5. Prove that $\frac{-x}{y} = \frac{x}{-y} = -\frac{x}{y}$.
6. Show that $x \leq x$ for any $x \in \mathbb{R}$.
7. If $x \leq y$, we also write $y \geq x$. If $x \leq y$ and $x \neq y$, we write $x > y$ or $y < x$.

What would the equivalents of XII–XVI be for \geq , $<$ and $>$?

Prove that these equivalents are true using only **theorem 1.2**.

2 Square Roots and Indices

2.1 Square Roots

In geometry, the area of a square is $y \cdot y$, where y is its the length of a side. Consequently, we refer to the quantity $y \cdot y$ as y *squared*. The natural reversed question, “what is the side length of a square, given that its area is x ?” gives rise to the idea of a square root.

Definition 2.1 (Square Root). Let $x \in \mathbb{R}$. Any $y \in \mathbb{R}$ which satisfies the property $y \cdot y = x$ is said to be a *square root* of x .

Example. 3 is a square root of 9, since $3 \cdot 3 = 9$. We also have that -3 is a square root of 9, since $(-3) \cdot (-3) = 9$.

Notice that we write “a square root”, not “the square root” in [definition 2.1](#), since using the definite article “the” implies that it is unique. In fact, as we have seen in the example, a square root is not unique: 9 has two square roots, 3 and -3 .

Notation. For $y \in \mathbb{R}$, we abbreviate $y \cdot y$ to y^2 .

Proposition 2.2. *If $x \in \mathbb{R}$, then $x^2 \geq 0$.*

Proof. By [theorem 1.2\(XIV\)](#), for any $x \in \mathbb{R}$, either $x \geq 0$ or $x \leq 0$.

If $x \geq 0$, then $x^2 = x \cdot x \geq 0$ by [theorem 1.2\(XVI\)](#).

If $x \leq 0$, then $x - x \leq 0 - x$, hence $0 \leq -x$. By XVI in [exercise 1.5\(7\)](#), we get $0 \leq (-x) \cdot (-x) = x^2$ by [proposition 1.3\(viii\)](#). \square

[Proposition 2.2](#) immediately gives us the following.

Corollary 2.3. *Let $x \in \mathbb{R}$. If $x < 0$, then x does not have a square root.*

Proof. By contradiction: suppose $x < 0$ and x does have a square root; call it y . Then by definition, $y^2 = x < 0$ (XVI in [exercise 1.5\(7\)](#)).

But also $y^2 \geq 0$ by [proposition 2.2](#), contradicting that $y^2 < 0$. \square

Thus no negative (< 0) real numbers have a square root. What about non-negative (≥ 0) real numbers? We will explore those in a moment, we first need this lemma.

Lemma 2.4 (Difference of two Squares). *Let $x, y \in \mathbb{R}$. Then*

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

Proof. Let $t = x + y$. Then

$$\begin{aligned}
 (x + y)(x - y) &= t(x - y) \\
 &= xt - yt \\
 &= x(x + y) - y(x + y) \\
 &= x^2 + xy - yx - y^2 \\
 &= x^2 - y^2,
 \end{aligned}$$

as required. \square

The following theorem really belongs in [section 1.2](#) with all the other properties of the real numbers.

Theorem 2.5 (\mathbb{R} is an Integral Domain). *Let $x, y \in \mathbb{R}$ such that $xy = 0$. Then one of x, y must be zero.*

Proof. We prove this by contradiction. Suppose $x, y \in \mathbb{R}$ and $xy = 0$, but neither x nor y are zero. In particular since $x \neq 0$, the number $\frac{1}{x}$ exists. Thus

$$xy = 0 \implies \frac{1}{x} \cdot xy = \frac{1}{x} \cdot 0 \implies 1y = 0 \implies y = 0,$$

contradicting that $y \neq 0$. \square

Examples 2.6. This important fact about real numbers allows us to solve equations such as $x(x - 1) = 0$, since it tells us that one of x or $(x - 1)$ must be zero, so we get either $x = 0$ or $x - 1 = 0 \implies x = 1$; and therefore the two solutions are $x = 0$ or $x = 1$.

Another example, consider the equation $x^2 - 16 = 0$. Since $16 = 4^2$, the left-hand side becomes $x^2 - 16 = x^2 - 4^2$, which by [lemma 2.4](#) becomes $(x + 4)(x - 4) = 0$. Thus the equation we have is $(x + 4)(x - 4) = 0$, which by the theorem yields $x + 4 = 0$ or $x - 4 = 0$, i.e., $x = -4$ or $x = 4$.

Theorem 2.7. *Let $x \in \mathbb{R}$ such that $x \geq 0$. Then x has two square roots in \mathbb{R} , given by y and $-y$, where $y \in [0, \infty)$ is unique.*

Proof. We will not prove the existence of square roots in \mathbb{R} , because it is a consequence of the completeness property. But the uniqueness part is easy. Indeed, suppose y and z are both square roots of x , but $y \neq z$. Then by definition, $y^2 = x$ and $z^2 = x$. In particular, $y^2 = z^2$, that is, $y^2 - z^2 = 0$, which by [lemma 2.4](#) gives $(y + z)(y - z) = 0$. But by [theorem 2.5](#), this gives

either $y + z = 0$ or $y - z = 0$, i.e., either $z = -y$ or $z = y$. Since we assumed that $z \neq y$, it follows that $z = -y$. This means that the only square root of x different from y is $-y$, as required. \square

Notation. We denote the unique non-negative y provided in [theorem 2.7](#) by \sqrt{x} .

Theorem 2.8. *Let a, b, c be non-negative real numbers. Then*

- i) $\sqrt{ab} = \sqrt{a}\sqrt{b}$,
- ii) $x\sqrt{a} \cdot y\sqrt{b} = xy\sqrt{ab}$ for any $x, y \in \mathbb{R}$,
- iii) $\sqrt{abbc} = b\sqrt{ac}$.

Proof. For (i), observe that \sqrt{ab} denotes the unique non-negative number y such that $y^2 = ab$, similarly \sqrt{a} denotes the unique non-negative number ℓ such that $\ell^2 = a$, and \sqrt{b} denotes the unique non-negative number k such that $k^2 = b$. We therefore have

$$y^2 = ab = \ell^2 k^2 = \ell \cdot \ell \cdot k \cdot k = (\ell k)(\ell k).$$

In particular, this means that ℓk is a square root of ab since it agrees with [definition 2.1](#), and moreover, ℓk is non-negative since both ℓ and k are (see XVI in [theorem 1.2](#)). But by [theorem 2.7](#), the non-negative square root is unique, so we must have $y = \ell k$, that is, $\sqrt{ab} = \sqrt{a}\sqrt{b}$.

(ii) and (iii) follow easily from (i):

$$\begin{aligned} x\sqrt{a} \cdot y\sqrt{b} &= xy\sqrt{a}\sqrt{b} = xy\sqrt{ab}, \\ \sqrt{abbc} &= \sqrt{(bb)(ac)} = \sqrt{bb}\sqrt{ac} = b\sqrt{ac} \end{aligned}$$

since $bb = bb \implies \sqrt{bb} = b$. \square

Exercise 2.9. Let $a, b \in \mathbb{R}$ with $a \geq 0$ and $b > 0$. Prove that

$$\sqrt{\frac{a}{b}} = \frac{\sqrt{a}}{\sqrt{b}}.$$

2.2 Surds and Surd Form

At some point during your education—probably in primary school—you would have been told that it’s “impolite” to leave, for example, $\frac{4}{8}$ as the answer to a maths problem, and you should instead write $\frac{1}{2}$ like a civilised member of society.

Here we introduce an analogue for square roots. Notice that, for example, $\sqrt{8}$ could be written as $\sqrt{2 \cdot 2 \cdot 2} = 2\sqrt{2}$. You are encouraged to “prefer” the latter. For larger examples, it might be clearer why this is preferable; e.g. $\sqrt{106\,722}$ is just $231\sqrt{2}$.

Notice that we are using [theorem 2.8\(iii\)](#) to simplify here, removing every pair of equal numbers below a square root and placing one outside. So for example, $\sqrt{72}$ is $6\sqrt{2}$ because $72 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3$, so

$$\sqrt{72} = \sqrt{\underbrace{2 \cdot 2 \cdot 2}_{2 \cdot 2} \cdot \underbrace{3 \cdot 3}_{3 \cdot 3}} = 2 \cdot 3 \sqrt{2} = 6\sqrt{2}.$$

Alternatively, one could recognise that $72 = 4 \cdot 9 \cdot 2$, then by [theorem 2.8\(i\)](#), we get

$$\sqrt{72} = \sqrt{4 \cdot 9 \cdot 2} = \sqrt{4} \sqrt{9 \cdot 2} = 2 \sqrt{9} \sqrt{2} = 2 \cdot 3 \sqrt{2} = 6\sqrt{2}.$$

Either method is fine. But what makes $\sqrt{2}$ “unsimplifyable”, where $\sqrt{72}$ wasn’t? Is it because it is prime? Consider this example:

$$\sqrt{120} = \sqrt{4 \cdot 30} = 2\sqrt{30},$$

30 is not prime, but it cannot be reduced further; if we break it up into as many factors as we can (its *prime factorisation*), we get $30 = 2 \cdot 3 \cdot 5$. Thus by the reasoning before, we cannot “take out” any pairs from underneath the square root.

Thus this is when an integer below a square root is “unsimplifyable” in this sense: when its prime factorisation contains no repeated factors. We call these numbers *surds*:

Definition 2.10 (Surd). A *surd* is a positive real number of the form

$$\sqrt{p_1 \cdot p_2 \cdots p_n},$$

where p_i is prime for all $i = 1, \dots, n$, and $p_i \neq p_j$ for $i \neq j$.

Examples 2.11. For example, $\sqrt{2}$ is a surd, since $\sqrt{2} = \sqrt{p_1}$ where $p_1 = 2$, and p_1 is prime. Similarly we have that $\sqrt{3}, \sqrt{5}, \sqrt{7}, \dots$ are all surds.

Another example, $\sqrt{6}$ is a surd, since $\sqrt{6} = \sqrt{2 \cdot 3} = \sqrt{p_1 \cdot p_2}$, where $p_1 = 2$ and $p_2 = 3$, each p_i is prime, and $p_1 \neq p_2$, i.e., $p_i \neq p_j$ whenever i and j are different.

One final example, $\sqrt{1155}$ is a surd, since $\sqrt{1155} = \sqrt{3 \cdot 5 \cdot 7 \cdot 11}$, so $p_1 = 3$, $p_2 = 5$, $p_3 = 7$, $p_4 = 11$, each p_i is prime, and $p_i \neq p_j$ when $i \neq j$.

$\sqrt{20}$ is *not* a surd, since $\sqrt{20} = \sqrt{2 \cdot 2 \cdot 5}$, so $p_1 = 2$, $p_2 = 2$, $p_3 = 5$. Each p_i is prime, but we have $p_1 = p_2$ even though $1 \neq 2$.

Theorem 2.12. *Every surd is irrational, that is, if x is a surd, then there are no two integers $a, b \in \mathbb{Z}$ such that $x = a/b$ where $b \neq 0$.*

Proof. A proof similar to the irrationality of $\sqrt{2}$ in [appendix A](#) can be adapted to prove this more general theorem. \square

Definition 2.13 (Linear Combination over \mathbb{Q}). Let $\{x_1, x_2, \dots, x_n\} \subseteq \mathbb{R}$. Then a *linear combination over \mathbb{Q}* of $\{x_1, x_2, \dots, x_n\}$ is a real number of the form

$$a_1x_1 + a_2x_2 + \dots + a_nx_n$$

where $a_1, a_2, \dots, a_n \in \mathbb{Q}$.

Example 2.14. If $S = \{\pi, \sqrt{2}, 1 - \sqrt{5}\}$, then some rational linear combinations of these numbers are

$$\begin{aligned} 2\pi + 3\sqrt{2} + 7(1 - \sqrt{5}) \\ 3\pi - \frac{\sqrt{2}}{2} - (1 - \sqrt{5}) &= 3\pi + (-\tfrac{1}{2})\sqrt{2} + (-1)(1 - \sqrt{5}) \\ \pi + \sqrt{2} &= 1\pi + 1\sqrt{2} + 0(1 - \sqrt{5}) \end{aligned}$$

Definition 2.15 (Surd Form). Let \mathbb{S} denote the set of all surds. A real number is said to be in *surd form* if it is expressed as a linear combination over \mathbb{Q} of $\mathbb{S} \cup \{1\}$.

Examples 2.16. We give some examples of how we may transform some real numbers into surd form.

- i) $\frac{1}{2} + 5\sqrt{2}$ is in surd form, since it equals $\frac{1}{2} \cdot 1 + 5 \cdot \sqrt{2}$, and $\frac{1}{2}, 5 \in \mathbb{Q}$ and $1, \sqrt{2} \in \mathbb{S} \cup \{1\}$.

- ii) $\sqrt{60} + \sqrt{800}$ is not in surd form, since $\sqrt{60}, \sqrt{800} \notin \mathbb{S}$, because $60 = 2^2 \cdot 3 \cdot 5$ and $800 = 2^5 \cdot 5^2$, and therefore $\sqrt{60}$ and $\sqrt{800}$ is not made up of a product of *unequal* primes ($p_i \neq p_j$) under the square root. However using [theorem 2.8\(iii\)](#), we have

$$\sqrt{60} = \sqrt{2 \cdot 2 \cdot 3 \cdot 5} = 2\sqrt{3 \cdot 5} = 2\sqrt{15},$$

where $\sqrt{15} \in \mathbb{S}$, and similarly

$$\begin{aligned} \sqrt{800} &= \sqrt{2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 5 \cdot 5} = 2\sqrt{2 \cdot 2 \cdot 2 \cdot 5 \cdot 5} \\ &= 2 \cdot 2\sqrt{2 \cdot 5 \cdot 5} \\ &= 2 \cdot 2 \cdot 5\sqrt{2} \\ &= 20\sqrt{2}. \end{aligned}$$

Thus we may write $\sqrt{60} + \sqrt{800}$ in surd form as $2\sqrt{15} + 20\sqrt{2}$, since $2, 20 \in \mathbb{Q}$ and $\sqrt{15}, \sqrt{2} \in \mathbb{S} \cup \{1\}$.

- iii) $\frac{7-5\sqrt{3}}{3}$ is nearly in surd form, however to write it more precisely as a linear combination over \mathbb{Q} , we express it as $(\frac{7}{3})1 + (-\frac{5}{3})\sqrt{3}$, this way it is clear that $\frac{7}{3}, -\frac{5}{3} \in \mathbb{Q}$, and $1, \sqrt{3} \in \mathbb{S} \cup \{1\}$.
- iv) $(\sqrt{2}+5\sqrt{3})(7\sqrt{12}-\sqrt{18})$ is not in surd form. We can start by observing that the second term has square roots which can be reduced.

$$7\sqrt{12} - \sqrt{18} = 7\sqrt{2 \cdot 2 \cdot 3} - \sqrt{2 \cdot 3 \cdot 3} = 14\sqrt{3} - 3\sqrt{2},$$

Hence we have the product $(\sqrt{2}+5\sqrt{3})(14\sqrt{3}-3\sqrt{2})$. But this is still not in surd form: it's a product, not a linear combination of surds. [Exercise 1.5\(4\)](#) and [theorem 2.8\(ii\)](#) can help us in expanding this out:

$$\begin{aligned} &(\sqrt{2} + 5\sqrt{3})(14\sqrt{3} - 3\sqrt{2}) \\ &= 14\sqrt{2 \cdot 3} - 3\sqrt{2 \cdot 2} + 5\sqrt{3 \cdot 3} - 5 \cdot 3\sqrt{3 \cdot 2} \\ &= 14\sqrt{6} - 3 \cdot 2 + 5 \cdot 3 - 15\sqrt{6} \\ &= 204 - \sqrt{6}, \end{aligned}$$

which is in surd form.

- v) $\frac{5}{\sqrt{5}} + \frac{\sqrt{5}}{5}$ is not in surd form, the first term $\frac{5}{\sqrt{5}}$ is neither a surd nor rational. However multiplying the numerator and denominator by $\sqrt{5}$, we get $\frac{5\sqrt{5}}{\sqrt{5}\sqrt{5}}$, which by definition of $\sqrt{}$ becomes $\frac{5\sqrt{5}}{5}$. Therefore we have $\frac{5\sqrt{5}}{5} + \frac{\sqrt{5}}{5}$, which is equal to $\frac{6\sqrt{5}}{5}$, or $\frac{6}{5}\sqrt{5}$, which is in surd form.

When surds appear in the denominator, it is not immediately clear whether that number can be expressed in surd form (unlike a surd in the numerator; $\frac{\sqrt{5}}{5}$ is clearly just $\frac{1}{5}\sqrt{5}$). Thus surds should always be “removed” from the denominator. This process of removing surds from the denominator is called *rationalising the denominator* (since the denominator becomes rational as a consequence).

- vi) $\frac{2}{\sqrt{2}+\sqrt{3}}$ is not in surd form. If we try the same technique as we did in example (iv), that is, multiplying the numerator and denominator by what is in the denominator, it will not work, since multiplying the denominator by itself does not entirely get rid of square roots: $(\sqrt{2} + \sqrt{3})(\sqrt{2} + \sqrt{3}) = 2 + 3 + 2\sqrt{6}$. This is due to the fact that $(a + b)(a + b) = a^2 + b^2 + 2ab$. But if we instead consider what [lemma 2.4](#) gives us, i.e., $(a + b)(a - b) = a^2 - b^2$, notice that no terms appear here without being squared. So multiplying the numerator and denominator by the denominator with *one of the signs reversed*, we get

$$\frac{2}{\sqrt{2} + \sqrt{3}} = \frac{2(\sqrt{2} - \sqrt{3})}{(\sqrt{2} + \sqrt{3})(\sqrt{2} - \sqrt{3})} = \frac{2\sqrt{2} - 2\sqrt{3}}{-1} = 2\sqrt{3} - 2\sqrt{2},$$

which is now clearly in surd form.

- vii) $5\sqrt{2/3}$ is not in surd form. But by [exercise 2.9](#), we can express

$$5\sqrt{\frac{2}{3}} = 5\frac{\sqrt{2}}{\sqrt{3}},$$

and so $5\sqrt{3/2} = 5\frac{\sqrt{2}\sqrt{3}}{\sqrt{3}\sqrt{3}} = \frac{5\sqrt{6}}{3}$, which is in surd form.

Exercise 2.17. 1. Express the following in surd form.

a) $\sqrt{243}$

b) $8\sqrt{1250}$

c) $\sqrt{44}$

d) $\frac{1 + \sqrt{2}}{\sqrt{3}}$

e) $\sqrt{60}$

f) $\sqrt{500} - \sqrt{124} + 5\sqrt{49}$

g) $\frac{6 + \sqrt{2}}{\sqrt{2} + 7}$

h) $(2\sqrt{12} - 3)\frac{3}{4 - \sqrt{2}}$

i) $(4\sqrt{7} + 3)(4\sqrt{7} + 3)$

j) $(4\sqrt{7} + 3)(4\sqrt{7} - 3)$

k) $\frac{\sqrt{2}}{\sqrt{2}-1}$

l) $\frac{4}{1+\sqrt{2}}$

m) $24\sqrt{400}$

n) $\frac{2\sqrt{2}+3\sqrt{3}+5\sqrt{5}}{6\sqrt{6}+7\sqrt{7}}$

o) $5+\sqrt{18}+9-\sqrt{36}$

p) $(2\sqrt{2}-3\sqrt{3})(\frac{1}{2\sqrt{2}}+\frac{1}{3\sqrt{3}})$

2. Simplify the expression $\frac{1}{\sqrt{3}} - \frac{\sqrt{3}}{1-\sqrt{3}}$ writing your answer in the form $(a+b\sqrt{3})/c$, where $a, b, c \in \mathbb{Z}$.


(MATSEC Sept '15)

3. Express $\frac{\sqrt{2}-1}{2\sqrt{2}+3} + \frac{3}{2\sqrt{2}-3}$ in the form $(a+b\sqrt{2})$.

(MATSEC May '15)

4. Notice that in [examples 2.16\(iv\)](#), we simplified the second term in the product so that both were in surd form, and subsequently multiplied them. Once we multiplied and combined like-terms, all square roots which appeared were surds—we didn't need to simplify further.

Is it always the case that if we start with two numbers in surd form, their product (expanded and like-terms combined) will be in surd form?

-  5. Express $\frac{1}{\sqrt{2}+2\sqrt{3}+3\sqrt{5}}$ in surd form.

Do you think that we can rationalise the denominator for any linear combination of surds, not just two or three? Give an example to illustrate why you come to this conclusion (no need for a proof).

6. Solve the equation

$$\frac{1}{\sqrt{2}+\sqrt{3}} = \frac{1}{x} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}},$$

giving your answer in surd form.

2.3 Indices

Just as n copies of x added together ($x + \cdots + x$) may be written as nx (recall [exercise 1.5\(1\)](#)), here we introduce a shorthand for multiplication.

Definition 2.18 (Power⁴). Let $n \in \mathbb{N}$. For any $x \in \mathbb{R}$, we define the notation x^n by

$$x^n := \underbrace{x \cdot x \cdots x}_{n \text{ times}},$$

where n here is called a *power* (or *index* or *exponent*) of x .

This definition immediately gives us the following theorem.

Theorem 2.19 (Laws of Indices). Let $a, b \in \mathbb{N}$, and let $x, y \in \mathbb{R}$. We have the following laws.

- | | |
|---|--|
| I. $x^a \cdot x^b = x^{a+b}$ | II. $\frac{x^a}{x^b} = x^{a-b}$, for $a > b$ |
| III. $(x^a)^b = x^{ab}$ | IV. $(xy)^a = x^a y^a$, for x and y not both negative |
| V. $\left(\frac{x}{y}\right)^a = \frac{x^a}{y^a}$ | |

Proof. We give the proof of law III here, the other four can easily be proved in a similar fashion.

$$\begin{aligned}
 (x^a)^b &= \underbrace{x^a \cdot x^a \cdots x^a}_{b \text{ times}} && \text{(by definition 2.18)} \\
 &= \underbrace{\underbrace{x \cdot x \cdots x}_{a \text{ times}} \cdot \underbrace{x \cdot x \cdots x}_{a \text{ times}} \cdots \underbrace{x \cdot x \cdots x}_{a \text{ times}}}_{b \text{ times}} && \text{(again by definition 2.18)} \\
 &= \underbrace{x \cdot x \cdots x}_{ab \text{ times}} = x^{ab}, && \text{(again by definition 2.18)}
 \end{aligned}$$

as required. □

⁴The definition here is not entirely precise, a more formal definition would be expressed *recursively*. This is something we will revisit later in [section 6.2](#). In general, when one sees dots (\cdots) in a mathematical definition/proof, it's a sign that things are a bit hand-wavy!

In mathematics, we seldom use the word “law”, as this implies something unquestionable or doctrinal. The “laws” of indices are mere immediate consequences of the definition: for example, the first one says that if you write down two x ’s, and then three x ’s, you get five x ’s:

$$x^2 \cdot x^3 = xx \cdot xxx = xxxxx = x^5,$$

very straightforward stuff.

Observe that the power notation we have introduced is consistent with the notation of squaring $y \cdot y$ which we denoted by y^2 in [section 2.1](#). Thus we naturally generalise the idea of *square root* (corresponding to $y^2 = x$) to any n th power.

Definition 2.20 (*n th Root*). Let $x \in \mathbb{R}$, and $n \in \mathbb{N}$. Any $y \in \mathbb{R}$ which satisfies the property $y^n = x$ is said to be an *n th root* of x .

The following theorems are analogues of [theorem 2.7](#) for n th roots. Their proofs require real analysis so we will skip them.

Theorem 2.21. *Let $x \in \mathbb{R}$, and suppose $n \in \mathbb{N}$ is odd. Then x has one unique n th root $y \in \mathbb{R}$.*

Theorem 2.22. *Let $x \in \mathbb{R}$ such that $x \geq 0$, and suppose $n \in \mathbb{N}$ is even. Then x has two n th roots in \mathbb{R} , given by y and $-y$, where $y \in [0, \infty)$ is unique.*

Notation. The unique n th root y provided to us by [theorems 2.21](#) and [2.22](#) is denoted by $\sqrt[n]{x}$.

Definition 2.23 (*Integer Power*). Let $x \in \mathbb{R}$, and $n \in \mathbb{Z}$. We extend the definition of x^n , by defining

$$x^n := \begin{cases} \underbrace{x \cdot x \cdot x \cdots x}_{n \text{ times}} & \text{if } n > 0 \\ 1 & \text{if } n = 0 \\ \frac{1}{\underbrace{x \cdot x \cdot x \cdots x}_{-n \text{ times}}} & \text{if } n < 0 \text{ and } x \neq 0 \end{cases}$$

With this definition, the results of [theorem 2.19](#) are true for any $a, b \in \mathbb{Z}$.

For example,

$$3^8 \cdot 3^{-5} = 3^8 \cdot \frac{1}{3 \cdot 3 \cdot 3 \cdot 3 \cdot 3} = \frac{\cancel{3} \cdot \cancel{3} \cdot \cancel{3} \cdot \cancel{3} \cdot \cancel{3} \cdot 3 \cdot 3 \cdot 3}{\cancel{3} \cdot \cancel{3} \cdot \cancel{3} \cdot \cancel{3} \cdot \cancel{3}} = 3 \cdot 3 \cdot 3 = 3^{8+(-5)},$$

showing that law I holds. In fact, the motivation for defining x^n this way, and not any other way, is so that the nice properties of [theorem 2.19](#) remain true. Indeed, with this in mind, we have the following definition.

Definition 2.24 (Rational Power). Let $x \in \mathbb{R}$, and $a/b \in \mathbb{Q}$. We define $x^{a/b}$ by

$$x^{a/b} := \sqrt[b]{x^a}.$$

Again, this definition is formulated in such a way that the results of [theorem 2.19](#) still hold (which indeed, they do for rational powers), and that it still agrees with [definition 2.23](#) for integers (which it does). The easiest way to see why we take this definition is a consequence of law III. Indeed, consider the value $3^{\frac{4}{5}}$. We want that law III holds, that is,

$$\left(3^{4/5}\right)^5 \stackrel{\text{we want}}{=} 3^{\frac{4}{5} \cdot 5} = 3^4.$$

Note that the desired equation above gives us that $3^{4/5}$ is precisely the unique 5th root of 3^4 , since it agrees with [definition 2.20](#) (and is unique by [theorem 2.21](#)). Thus we are forced to take this as our definition.

Later on, we see that the number x^y can be defined for all powers $y \in \mathbb{R}$, and even for y in sets larger than \mathbb{R} ; always in such a way that all the definitions here are respected, and that the results of [theorem 2.19](#) still hold. For now, we will simply give some intuition as to what this “should” be when $x > 0$.

We will see later that we want things of the form x^y to be continuous in y . All this means, intuitively, is that if we vary y by a small quantity, then x^y will also change by a reasonably small quantity. Thus,

$$3^{\sqrt{2}},$$

for example, should be reasonably close to $3^{1.4}$ (which we can evaluate by [definition 2.24](#) since 1.4 is rational) closer to $3^{1.414}$, even closer to $3^{1.4142135}$, and so on, so that the more digits we take in the power, the more accurate our approximation. The number $3^{\sqrt{2}}$ should be thought of as the “completion” of this process, similar to the way in which $\sqrt{2}$ itself is similarly a completion.

Exercise 2.25. 1. Evaluate the following WITHOUT A CALCULATOR.

- | | | |
|-----------------------------|-----------------------------------|--------------------------------|
| a) 2^3 | b) 4^{-2} | c) $[2.314 \times 10^{-37}]^0$ |
| d) $5^{2/3}5^{4/3}$ | e) 2^{-9} | f) $64^{-\frac{1}{4}}$ |
| g) $16^0 \times 243^{1/5}$ | h) $\pi^2\pi^{-3} \times \pi5^2$ | i) $153^2 - 47^2$ |
| j) 2^{2^3} | k) $(\frac{3}{7})^2(1/49)^{-1/2}$ | l) $22 - 4^3(\frac{1}{2})^3$ |
| m) $(-1)^{207841}(4)^{1/2}$ | n) $(\frac{1}{2})^{3/2}$ | o) $\sqrt{\sqrt{\sqrt{900}}}$ |

2. a) Prove that $\sqrt[3]{ab} = \sqrt[3]{a}\sqrt[3]{b}$ in the style of **theorem 2.8**.
 b) Similarly prove that $\sqrt[3]{abb^2c} = b\sqrt[3]{ac}$.
 c) Allowing yourself to use ideas from this section, how could you prove these two results for any n th root easily?
3. Prove that **definition 2.24** of x^r for $r \in \mathbb{Q}$ does not depend on how we choose to represent r (e.g., $x^{1/2} = x^{4/8}$).
4. How would you generalise the definition of surds and surd form for cube roots ($\sqrt[3]{}$)? Express

$$\frac{1}{\sqrt[3]{2} + \sqrt[3]{3}}$$

is your new surd form.

[Hint: look up the “sum of two cubes” formula in the A-level booklet!]

3 Quadratics

3.1 Solving Quadratic Equations

Definition 3.1 (Quadratic). A *quadratic* is an algebraic expression of the form

$$ax^2 + bx + c,$$

where x is a variable, and $a, b, c \in \mathbb{R}$ and $a \neq 0$. An equation $\phi(x) = 0$ where ϕ is a quadratic is said to be a *quadratic equation* (QE).

Definition 3.2 (Root). Let F be a set containing 0, and let $\phi(x) \in F$ be an expression dependent on x . A *root* or *zero* of ϕ is an element $x \in F$ such that $\phi(x) = 0$.

In particular, we say that x is a *real root* if we put $F = \mathbb{R}$.

Sometimes if we have a quadratic equation $\phi(x) = 0$, we call its solutions its *roots* or its *zeros*, in view of the definition above.

Examples 3.3. $x^2 - 1$, $5x^2 - x$, and $3x^2 + 5x - 12$ are three examples of *quadratics*, whereas $x^2 - 1 = 0$, $5x^2 - x = 0$, and $3x^2 + 5x - 12 = 0$ are examples of *quadratic equations*.

$x = 1$ is a *root* of $x^2 - 1$ since $(1)^2 - 1 = 1 - 1 = 0$, it is also a *solution* of $x^2 - 1 = 0$.

Notation. To abbreviate “ $x = a$ or $x = -a$ ”, we write $x = \pm a$.

Remark 3.4. Sometimes quadratic equations can be solved if they are transformed into products of linear factors, as we did in [examples 2.6](#). This is called *factorisation*, and can be done by close inspection of the quadratic. A few examples:

$$\begin{aligned} x^2 - 9 = 0 &\implies (x + 3)(x - 3) = 0 \implies x = \pm 3 \\ x^2 - 5x + 6 = 0 &\implies (x - 2)(x - 3) = 0 \implies x = 2, x = 3 \\ 6x^2 + 7x - 3 = 0 &\implies (3x - 1)(2x + 3) = 0 \implies x = \frac{1}{3}, x = -\frac{3}{2} \end{aligned}$$

This cannot always be done, however. E.g., try to factorise $x^2 + x + 1$. (We will see a criterion for when this possible in the next section, [corollary 3.14](#).)

Lemma 3.5. Suppose $x, a \in \mathbb{R}$ and $a \geq 0$. Then

$$x^2 = a \iff x = \pm\sqrt{a}.$$

Proof. This follows immediately from [theorem 2.7](#). □

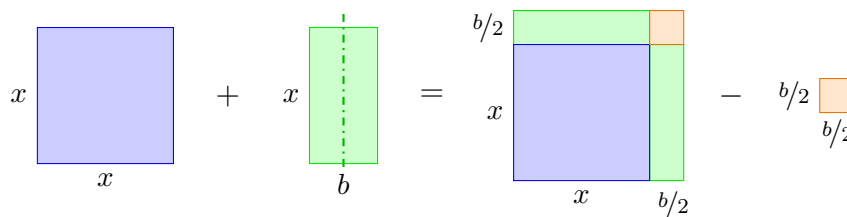


FIGURE 1: Visualisation of Completing the Square

The following result is a fundamental identity which you are encouraged to commit to memory!

Theorem 3.6 (Completing the square). *Let $b \in \mathbb{R}$. Then for all $x \in \mathbb{R}$,*

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

Proof. We have

$$\left(x + \frac{b}{2}\right)^2 - \left(\frac{b}{2}\right)^2 = x^2 + bx + \left(\frac{b}{2}\right)^2 - \left(\frac{b}{2}\right)^2 = x^2 + bx,$$

as required. \square

Exercise 3.7. Refer to the illustration in [figure 1](#). Provide a geometric argument for [theorem 3.6](#) (you may assume $b > 0$).

Example 3.8. This theorem allows us to solve *any* quadratic equation! Suppose we have $x^2 - 4x + 1 = 0$. Applying the theorem to the left-hand side we get

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

Thus $x^2 - 4x + 1 = 0$ becomes $(x - 2)^2 - 3 = 0$, i.e., $(x - 2)^2 = 3$, which by [lemma 3.5](#) becomes $x - 2 = \pm\sqrt{3}$, so the solutions are $x = 2 \pm \sqrt{3}$.

Examples 3.9. Here we solve a few different quadratic equations. To keep things simple, all the quadratics given here are solvable by factorising—but the reasoning applies to any quadratic equations, and equation solving problems in general.

i) $12x^2 + 2x - 4 = 0$.

The first thing we notice is that there is a common factor of 2, so dividing both sides of the equation by 2 (i.e., multiplying throughout by $1/2$) will give an equation whose left-hand side might prove easier to factorise.

$$\begin{aligned} 6x^2 + x - 2 &= 0 \\ \implies (3x + 2)(2x - 1) &= 0 \\ \implies x = -2/3, x = 1/2 \end{aligned}$$

ii) $17x^2 + 81x - 20 = 0$.

The coefficient 17 of x^2 might make this seem harder at first, but being prime, this actually gives us fewer options for factorisation. The left hand side factorises to $(17x - 4)(x + 5) = 0$, and so the solutions are $x = 4/17, x = -5$.

iii) $28x^2 + 7x - 7 = 7x^2 + 5x + 1$.

Horror! We don't have $= 0$ on the end! This is quite simple to get around as I'm sure you guessed, we can move everything over to the other side and solve normally (this actually corresponds to adding $-7x^2$, $-5x$ and -1 to both sides, if we reason about it in the [section 1.2](#) sense).

In fact, so we don't forget about [section 1.2](#), let's justify each step in solving this equation properly:

$$\begin{aligned} &28x^2 + 7x - 7 = 7x^2 + 5x + 1 \\ \implies &(28x^2 + 7x - 7) - 7x^2 = (7x^2 + 5x + 1) - 7x^2 \\ \implies &28x^2 - 7x^2 + 7x - 7 = 7x^2 - 7x^2 + 5x + 1 \\ \implies &(28 - 7)x^2 + 7x - 7 = 0 + 5x + 1 \\ \implies &21x^2 + 7x - 7 = 5x + 1 \\ &\vdots \\ \implies &21x^2 + 2x - 8 = 0 \\ \implies &(7x - 4)(3x + 2) = 0 \\ \implies &7x - 4 = 0 \quad \text{or} \quad 3x + 2 = 0 \\ \implies &7x = 4 \quad \text{or} \quad 3x = -2 \end{aligned}$$

$$\begin{aligned} \implies & \frac{1}{7}7x = \frac{1}{7}4 \quad \text{or} \quad \frac{1}{3}3x = \frac{1}{3}(-2) \\ \implies & x = \frac{4}{7} \quad \text{or} \quad x = -\frac{2}{3}, \end{aligned}$$

as you can see, we did skip some step justifications here. Perhaps this will cause you to appreciate how many algebraic steps we are used to applying automatically—we usually solve something like this in 3 to 4 steps!

iv) $x^2 - 4 = 0$.

This can be solved in three ways: we could either recognise the left-hand side as a difference of two squares, and do

$$(x - 2)(x + 2) = 0 \implies x = 2, x = -2.$$

Alternatively, we could simply take the 4 over to the right hand side and by [lemma 3.5](#) we get

$$x^2 = 4 \implies x = \pm\sqrt{4} = \pm 2,$$

or we could look at it as we do the usual quadratic with a non-zero coefficient of x :

$$x^2 + 0x - 4 = 0 \implies (x - 2)(x + 2) = 0 \implies x = 2, x = -2.$$

v) $x^2 - 3x = 0$.

This is quite an easy equation to solve, one simply has to notice that x is a common factor of the left-hand side, and do

$$x^2 - 3x = 0 \implies x(x - 3) = 0 \implies x = 0, x = 3.$$

Perhaps a word of caution: notice that in the very first example, we divided by 2 because it was a common factor of the left-hand-side. Why not divide by x here then?

Well, perhaps the way we should look at “dividing by 2” is the following:

$$\begin{aligned} 12x^2 + 2x - 4 = 0 & \implies 2(6x^2 + x - 2) = 0 \\ & \implies 2 = 0 \quad \text{or} \quad 6x^2 + x - 2 = 0. \end{aligned}$$

Clearly $2 = 0$ is a nonsensical conclusion, so we dismiss it and focus on the other solution. (After all, what we conclude when we apply

theorem 2.5 is an OR statement, meaning at least one of the two conclusions is true, not necessarily both).

And in fact, it is precisely the fact that 2 is not 0 which allows us to divide by 2 in the first place (which is actually *multiplication by $1/2$*). In the case where we have $x(x - 3) = 0$, we cannot divide by x (i.e., multiply by $1/x$) if x could possibly be zero: $1/x$ does not even exist in that case! (by **theorem 1.2**). Thus we should always think of “dividing both sides of an equation” in the sense of the above, where we get silly conclusions such as $2 = 0$ which we discard. This way, we never lose any possible solutions which we would miss by “dividing”.

vi) $x^5 - 13x^3 + 36x = 0$.

“This isn’t a quadratic!”, you might protest. But let’s give it a go. First of all, notice that just as in the previous example, x is a common factor:

$$x(x^4 - 13x^2 + 36) = 0 \implies x = 0 \quad \text{or} \quad x^4 - 13x^2 + 36 = 0,$$

so we already found a solution. Let’s focus on $x^4 - 13x^2 + 36 = 0$ now. What could this give us, and more importantly, how do we solve it? If we stare at it long enough, we notice that even though it’s not exactly a quadratic, it has a quadratic form. In fact, if we let $t = x^2$, then the equation is simply $t^2 - 13t + 36 = 0$.

Thus we have

$$\begin{aligned} t^2 - 13t + 36 &= 0 \\ \implies (t - 4)(t - 9) &= 0 \\ \implies t = 4 \quad \text{or} \quad t &= 9 \\ \implies x^2 = 4 \quad \text{or} \quad x^2 &= 9 \\ \implies x = \pm 2 \quad \text{or} \quad x &= \pm 3 \end{aligned}$$

by **lemma 3.5**. Thus the solutions are $x = 0, x = \pm 2, x = \pm 3$. The introduction of a new variable t makes things clear (just as in, say, the proof of **lemma 2.4**), but it is unnecessary. We could work without it:

$$\begin{aligned} x^4 - 13x^2 + 36 &= 0 \\ \implies (x^2)^2 - 13x^2 + 36 &= 0 \\ \implies (x^2 - 4)(x^2 - 9) &= 0 \end{aligned}$$

$$\begin{aligned}\implies x^2 &= 4 \quad \text{or} \quad x^2 = 9 \\ \implies x &= \pm 2 \quad \text{or} \quad x = \pm 3.\end{aligned}$$

Notice we get 5 solutions to this equation.

vii) $2x = \sqrt{7 - 27x}$.

Again, this isn't clearly a quadratic: but remember, what is the definition of the $\sqrt{}$ symbol? Well, it means that $2x$ is a square root of $7 - 27x$, so by [definition 2.1](#),

$$\begin{aligned}(2x)^2 &= 7 - 27x \\ \implies 4x^2 + 27x - 7 &= 0 \\ \implies (4x - 1)(x + 7) &= 0 \\ \implies x = \frac{1}{4} \quad \text{or} \quad x &= -7.\end{aligned}$$

Even though we did this with none of the other examples, let's check that these answers are right. What does it mean that these are "answers"? Well, it means that substitution in the left-hand side and the right-hand side of the given equation should make them equal. Let's start with $x = \frac{1}{4}$:

$$\begin{aligned}\text{LHS} &= 2x = 2\left(\frac{1}{4}\right) = \frac{1}{2} \\ \text{RHS} &= \sqrt{7 - 27x} = \sqrt{7 - 27\left(\frac{1}{4}\right)} = \sqrt{\frac{28}{4} - \frac{27}{4}} \\ &= \sqrt{\frac{28-27}{4}} = \sqrt{\frac{1}{4}} = \frac{\sqrt{1}}{\sqrt{4}} = \frac{1}{2},\end{aligned}$$

so the left- and right-hand sides are equal with $x = \frac{1}{4}$. Now what about $x = -7$?

$$\begin{aligned}\text{LHS} &= 2x = 2(-7) = -14 \\ \text{RHS} &= \sqrt{7 - 27x} = \sqrt{7 - 27(-7)} = \sqrt{7 + 189} = \sqrt{196} = 14,\end{aligned}$$

Here $\text{LHS} \neq \text{RHS}$! What's going on?

Well, strictly speaking we should always check the answers when we conclude an OR statement. For example, if we declare that $z = 2$, then it follows that $z \cdot z = 2 \cdot 2$, i.e., $z^2 = 4$. But from this, by [lemma 3.5](#), we conclude that

$$z = 2 \quad \text{or} \quad z = -2,$$

which is correct: we do indeed have that “ $z = 2$ OR $z = -2$ ” is true—and this does not mean that both give meaningful answers to what we started with, only that at least one of them does. (In fact, this is similar to how we obtained $2 = 0$ in example (v).)

The reason we didn’t bother checking the other equations is because if we were to carefully check the directions of our implications (\Rightarrow or \Leftarrow), each of them could go both ways (\Leftrightarrow). For example,

$$x^2 - 5x + 6 = 0 \Leftrightarrow (x - 2)(x - 3) = 0 \Leftrightarrow x = 2 \text{ or } x = 3.$$

Thus x being 2 or 3 is equivalent to $x^2 - 5x + 6$ equalling zero. On the other hand, in our $z = 2$ case, we have $z = 2 \Rightarrow z^2 = 4$, but not $z = 2 \Leftarrow z^2 = 4$. Indeed, if $z = -2$, it is true that $z^2 = 4$, but we cannot conclude that $z = 2$.

Similarly in the equation we solved, it is the first step, where we do

$$2x = \sqrt{7 - 27x} \Rightarrow (2x)^2 = 7 - 27x$$

which is a strictly one-sided implication. In fact, if $(2x)^2 = 7 - 27x$, we know by [lemma 3.5](#) that what we can say is $2x = \pm\sqrt{7 - 27x}$, which is consistent with the LHS = -14 and RHS = 14 situation. Indeed, had we started with the equation $-2x = \sqrt{7 - 27x}$ instead, then applying the definition of square root (which we could see as *squaring both sides*) will result in the same equation $4x^2 + 27x - 7 = 0$. Thus information about the sign of the left-hand/right-hand sides is lost when we square both sides; we only retain equality up to sign.

Thus in general, when we “square both sides” of an equation, information about the sign is lost, so extra solutions (corresponding to LHS = $-$ RHS) are introduced. Extra care should be taken when performing this operation—check your answers!

Exercise 3.10. 1. Solve the following equations by factorising.

a) $x^2 + 7x + 12 = 0$

b) $x^2 - 3x - 4 = 0$

c) $x^2 + 5x + 6 = 0$

d) $10x^2 + x = 21$

e) $x^2 + 4x - 10 = 2x + 5$

f) $x^2 - 16 = 0$

g) $x^2 + 3x = x$

h) $x^4 - 26x^2 + 25 = 0$

i) $\sqrt{2x-1} = x$

j) $\sqrt{9-5x^2} = 2x$

2. Solve the following equations.

a) $x^2 - 8x - 48 = 0$

b) $x^2 + 2x - 48 = -6$

c) $5x^2 - 21 = 10x$

d) $1 = \sqrt{7x - x^2}$

e) $x^2 + 13x + 22 = 7$

f) $x^2 - 9x - 39 = -9$

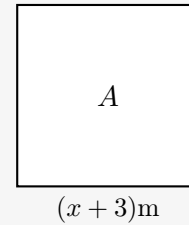
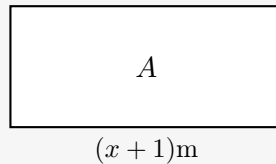
g) $2x^2 + 12x + 10 = 0$


h) $5x^2 + 19x - 68 = -2$

i) $3x^2 + 20x + 36 = 4$

j) $19x + x^5 = x + 10x^3$

3. A rectangle and a square have the same area. Their dimensions are shown in metres below.

Find the area A .4. A rectangular field with an area of 75 m^2 is enclosed by a wooden fence. One side of the fence is 3 m longer than its adjacent side. What are the dimensions of the fence? Give answers accurate to 2 d.p.s.

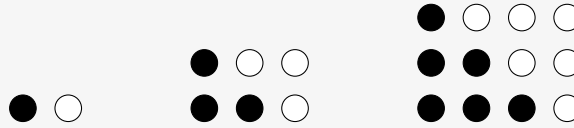
 5. Two boats start sailing from the same point. One travels north at 25 km/h. Two hours later the second boat starts travelling east at 20 km/h. How much time must pass from the departure of the first boat for them to be exactly 300 km apart?

6. (The Quadratic Formula). Use completing the square to show that if $a \neq 0$, then

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

Hence deduce that if $b^2 - 4ac \geq 0$, the solutions of the QE $ax^2 + bx + c = 0$ are given by $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$.

7. Consider the three arrays below.



- How many dots are there in the fourth array of this pattern? How many of them are black?
- How many dots are there in the n th pattern? How many of them are black?
- Which array in this pattern contains 4950 black dots?
- In array 3, the number of black dots can be written $1+2+3$. Express the number of black dots in array 7 as a sum of integers in a similar way.
- What is the result of the sum $1 + 2 + 3 + \cdots + 999 + 1000$?

8. Solve the equation

$$\frac{1}{x + \sqrt{2} + \sqrt{3}} = \frac{1}{x} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}},$$

giving your answer in surd form.

(MATSEC Sept '17)

3.2 Theory of Quadratic Equations

Here we try to demystify the relationship between quadratics' coefficients and their roots. In [exercise 3.10\(6\)](#), the number $b^2 - 4ac$ cropped up. This important constant can tell us a lot about the corresponding quadratic.

Definition 3.11 (Discriminant). Let $\phi(x) = ax^2 + bx + c$ be a quadratic. The *discriminant* of ϕ , denoted $\Delta(\phi)$ or Δ , is the real number defined by

$$\Delta(\phi) = b^2 - 4ac.$$

Theorem 3.12. Let $\phi(x) = ax^2 + bx + c$ be a quadratic, and let Δ be its discriminant.

- If $\Delta > 0$, then ϕ has two distinct real roots, given by $\frac{-b+\sqrt{\Delta}}{2a}$ and $\frac{-b-\sqrt{\Delta}}{2a}$.

ii) If $\Delta = 0$, then ϕ has one real root called a repeated root, given by $-\frac{b}{2a}$.

iii) If $\Delta < 0$, then ϕ has no real roots.

Furthermore, if $a > 0$ then $\phi(x) > 0$ for all $x \in \mathbb{R}$, whereas if $a < 0$, then $\phi(x) < 0$ for all $x \in \mathbb{R}$.

Proof. The result of (i) follows by completing the square. Indeed, to find the roots of $\phi(x) = ax^2 + bx + c$, we solve $\phi(x) = 0$:

$$\begin{aligned}
 \phi(x) = 0 &\implies ax^2 + bx + c = 0 \\
 &\iff x^2 + \frac{b}{a}x + \frac{c}{a} = 0 \\
 &\iff \left(x + \frac{b}{2a}\right)^2 - \left(\frac{b}{2a}\right)^2 + \frac{c}{a} = 0 \\
 &\iff \left(x + \frac{b}{2a}\right)^2 = \left(\frac{b}{2a}\right)^2 - \frac{c}{a} \\
 &\quad = \frac{b^2}{4a^2} - \frac{c}{a} \\
 &\quad = \frac{b^2 - 4ac}{4a^2} \quad (\textcircled{\mathbb{K}}) \\
 &\implies x + \frac{b}{2a} = \pm \sqrt{\frac{b^2 - 4ac}{4a^2}} \quad (\text{lemma 3.5, assuming } \Delta \geq 0) \\
 &\quad = \pm \frac{\sqrt{b^2 - 4ac}}{\sqrt{4a^2}} \quad (\text{exercise 2.9}) \\
 &\quad = \pm \frac{\sqrt{b^2 - 4ac}}{2a} \\
 &\implies x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a},
 \end{aligned}$$

and therefore if $\Delta \geq 0$, we have the solutions $\frac{-b \pm \sqrt{\Delta}}{2a}$. In particular, if $\Delta > 0$, then the two solutions are distinct, since they differ by $\frac{\sqrt{\Delta}}{a} > 0$. If $\Delta = 0$, then they are both equal to $\frac{-b \pm \sqrt{0}}{2a} = -\frac{b}{2a}$.

Now for the case $\Delta < 0$, observe the step in $(\textcircled{\mathbb{K}})$:

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

This is equivalent to the original equation since it was deduced using two-sided implications (\Leftrightarrow). Now since $\Delta < 0$, then $\frac{\Delta}{4a^2} < 0$. But the left-hand side is non-negative independently of x , since no number squared can be negative ([proposition 2.2](#)). Thus this equation can have no solutions.

Moreover, by completing the square, one can show that

$$\phi(x) = ax^2 + bx + c = a \left[\left(x + \frac{b}{2a} \right)^2 + \underbrace{\frac{-\Delta}{4a^2}}_{>0} \right],$$

denote this by $K(x)$

i.e., $\phi(x) = aK(x)$ where $K(x)$ is always a positive number independently of x . Therefore it follows that if $a > 0$, $\phi(x) > 0$, and similarly if $a < 0$, $\phi(x) < 0$. \square

Examples 3.13. We give some examples of applications of this theorem.

- i) $x^2 - 5x + 5$ has real and distinct roots since $\Delta = 5^2 - 4(1)(5) = 5 > 0$.
- ii) $x^2 - 6x + 9$ has a repeated root, since $\Delta = 6^2 - 4(1)(9) = 0$.
- iii) $3x^2 - 5x + 11$ has no real roots, since $\Delta = 5^2 - 4(3)(11) = -107 < 0$. Furthermore, since $a = 3 > 0$, then this quadratic is always positive for any value of x .
- iv) $x^2 + ax + 3a^2$ where a is a non-zero constant has no real roots, since $\Delta = a^2 - 4(1)(3a^2) = -11a^2 < 0$ for all non-zero a .
- v) We determine which values of b make $3x^2 + bx + 3$ have repeated roots. This happens when the discriminant $\Delta = b^2 - 4(3)(3) = 0$, that is, when $b^2 - 36 = 0$, that is, when $b = \pm 6$.
- vi) We prove that $9x^2 - 12ax + 4a^2$ always has repeated roots. Indeed, we have $\Delta = (-12a)^2 - 4(9)(4a^2) = 144a^2 - 144a^2 = 0$, no matter the value of a .

The following corollary tells us when we can factorise quadratics as in **remark 3.4**.

Corollary 3.14. *Let $\phi(x) = ax^2 + bx + c$ be a quadratic, where $a, b, c \in \mathbb{Z}$, and let Δ be its discriminant. If $\Delta \in \{n^2 : n \in \mathbb{Z}\}$, then ϕ can be expressed in the form*

$$\phi(x) = K(mx - s)(nx - t),$$

where $K, m, n, s, t \in \mathbb{Z}$ and $K, m, n \neq 0$.

The proof of this corollary is a bit long and requires some number theory, so it is given in **appendix B.1**. \square

Example 3.15. For example, $6x^2 + x - 2$ can be written as $(2x - 1)(3x + 2)$. Indeed, $\Delta = 1^2 - 4(6)(-2) = 49 = 7^2 \in \{n^2 : n \in \mathbb{Z}\}$.

Thus if you are struggling to determine the factorisation of a quadratic, evaluate its discriminant and check if its a square number. If it isn't, you can stop trying!

Theorem 3.16. *Let $\phi(x) = ax^2 + bx + c$ be a quadratic, and let Δ be its discriminant. If $\Delta \geq 0$, then $\phi(x)$ can be expressed in the form*

$$\phi(x) = a(x - \alpha)(x - \beta),$$

where $\alpha, \beta \in \mathbb{R}$ are its roots. Furthermore, the quadratic $K(x - \alpha)(x - \beta)$ has the same roots as ϕ for any non-zero real number K .

Proof. The roots of the quadratic $\phi(x) = ax^2 + bx + c$ with $\Delta \geq 0$ are $x = \frac{-b \pm \sqrt{\Delta}}{2a}$ (theorem 3.12). Denote these by α, β . Now

$$\begin{aligned} \phi(x) &= ax^2 + bx + c \\ &= a\left(x^2 + \frac{b}{a}x + \frac{c}{a}\right) \\ &= a\left(\left(x + \frac{b}{2a}\right)^2 - \left(\frac{b}{2a}\right)^2 + \frac{c}{a}\right) \\ &= a\left(\left(x + \frac{b}{2a}\right)^2 - \frac{b^2}{4a^2} + \frac{c}{a}\right) \\ &= a\left(\left(x + \frac{b}{2a}\right)^2 - \frac{b^2 + 4ac}{4a^2}\right) \\ &= a\left(\left(x + \frac{b}{2a}\right)^2 - \frac{\Delta}{4a^2}\right) \\ &= a\left(\left(x + \frac{b}{2a}\right)^2 - \left(\frac{\sqrt{\Delta}}{2a}\right)^2\right) \\ &= a\left(\left(x + \frac{b}{2a} + \frac{\sqrt{\Delta}}{2a}\right)\left(x + \frac{b}{2a} - \frac{\sqrt{\Delta}}{2a}\right)\right) \quad (\text{lemma 2.4}) \\ &= a\left(x - \left(\frac{-b - \sqrt{\Delta}}{2a}\right)\right)\left(x - \left(\frac{-b + \sqrt{\Delta}}{2a}\right)\right) \\ &= a(x - \alpha)(x - \beta), \end{aligned}$$

as required. Now to show that $K(x - \alpha)(x - \beta)$ has the same roots for non-zero K , observe that

$$K(x - \alpha)(x - \beta) = 0 \iff K = 0 \quad \text{or} \quad x - \alpha = 0 \quad \text{or} \quad x - \beta = 0,$$

and since $K \neq 0$, the result follows. \square

Example 3.17. The quadratic $2x^2 - 4x - 5$ has roots $(2 \pm \sqrt{14})/2$. Indeed,

$$2\left(x - \frac{2 + \sqrt{14}}{2}\right)\left(x - \frac{2 - \sqrt{14}}{2}\right)$$

$$\begin{aligned}
&= 2x^2 - (2 + \sqrt{14})x - (2 - \sqrt{14})x + 2\left(\frac{2 + \sqrt{14}}{2}\right)\left(\frac{2 - \sqrt{14}}{2}\right) \\
&= 2x^2 - 4x + \frac{2^2 - 14}{2} = 2x^2 - 4x - 5.
\end{aligned}$$

Don't confuse what this theorem is telling us with what [corollary 3.14](#) is saying. What we have is that, in theory, any quadratic with $\Delta \geq 0$ can be factorised, but due to our human limitations, we can't immediately notice the factors unless they are sufficiently “nice” (i.e., rational, as in [corollary 3.14](#)). So *in theory*, you should be able to look at

$$x^2 - x - 1 = 0$$

and say “of course! This factorises as

$$(x - \frac{1+\sqrt{5}}{2})(x - \frac{1-\sqrt{5}}{2}) = 0.”$$

But in practice, we can only manage what [corollary 3.14](#) tells us (by sight).

Theorem 3.18 (Viète's Formulæ for Quadratics). *Let $\phi(x) = ax^2 + bx + c$ be a quadratic. Then*

$$\phi(x) = a(x^2 - (\alpha + \beta)x + \alpha\beta) = a(x^2 - \Sigma x + \Pi),$$

where α, β are its roots, and Σ and Π denote the sum and product of the roots respectively. In other words, $\alpha + \beta = -b/a$ and $\alpha\beta = c/a$.

Proof. By [theorem 3.12](#), ϕ can be expressed as $a(x - \alpha)(x - \beta)$, which when expanded, gives

$$\phi(x) = a(x^2 - (\alpha + \beta)x + \alpha\beta) = ax^2 - a(\alpha + \beta)x + a\alpha\beta.$$

Comparing this with $ax^2 + bx + c$ yields $\alpha + \beta = -b/a$ and $\alpha\beta = c/a$, as required.⁵ \square

Example 3.19. If you want to “create” an equation with solutions $x = 2$ and $x = 5$ (for example), you have two ways. The first is to simplify $K(x - 2)(x - 5)$, where you can choose $K \neq 0$ to be any number you like (you could just take $K = 1$).

⁵The “comparing coefficients” technique is justified in [proposition 5.31](#) later on. The basic idea is that, if two quadratics are equal for any value of x , it follows that their coefficients must be equal.

Alternatively, by Viète's formulæ ([theorem 3.18](#)), we have the sum $\Sigma = 2 + 5 = 7$ and the product $\Pi = 2 \cdot 5 = 10$. Thus $a(x^2 - 7x + 10)$ for any $a \neq 0$ has the required roots.

Example 3.20. Viète's formulæ also allow us to modify roots of quadratics without having to find them. This is not why they are important, but doing this requires you to have a firm understanding of what the theorem is actually saying (and is therefore something which examination boards like to ask of you!). Suppose we have the quadratic $x^2 - 17x + 15$ whose roots are α and β . Can we devise a quadratic whose roots are, for example, $\frac{\alpha}{\beta}$ and $\frac{\beta}{\alpha}$? A naïve way of doing this is to actually find the roots of the quadratic (α and β), then determine $\frac{\alpha}{\beta}$ and $\frac{\beta}{\alpha}$ explicitly, and then simplify the expression $(x - \frac{\alpha}{\beta})(x - \frac{\beta}{\alpha})$, which by [theorem 3.16](#) has the required roots.

Naïve solution: By completing the square, we get that $x^2 - 17x + 15 = (x - \frac{17}{2})^2 - \frac{289}{4} + 15 = (x - \frac{17}{2})^2 - \frac{229}{4}$. Thus the roots are given by $x^2 - 17x + 15 = 0 \implies (x - \frac{17}{2})^2 = \frac{229}{4} \implies x = \frac{17 \pm \sqrt{229}}{2}$. Therefore

$$\frac{\alpha}{\beta} = \frac{\frac{17 + \sqrt{229}}{2}}{\frac{17 - \sqrt{229}}{2}} = \frac{17 + \sqrt{229}}{17 - \sqrt{229}}, \quad \text{and} \quad \frac{\beta}{\alpha} = \frac{1}{\alpha/\beta} = \frac{17 - \sqrt{229}}{17 + \sqrt{229}},$$

so the required quadratic is given by

$$\begin{aligned} & \left(x - \frac{17 + \sqrt{229}}{17 - \sqrt{229}}\right) \left(x - \frac{17 - \sqrt{229}}{17 + \sqrt{229}}\right) \\ &= x^2 - \frac{17 + \sqrt{229}}{17 - \sqrt{229}}x - \frac{17 - \sqrt{229}}{17 + \sqrt{229}}x + \left(\frac{17 + \sqrt{229}}{17 - \sqrt{229}}\right) \left(\frac{17 - \sqrt{229}}{17 + \sqrt{229}}\right) \\ &= x^2 - \frac{(17 + \sqrt{229})^2 + (17 - \sqrt{229})^2}{(17 + \sqrt{229})(17 - \sqrt{229})}x + 1 \\ &= x^2 - \frac{289 + 34\sqrt{229} + 229 + 289 - 34\sqrt{229} + 229}{289 - 229}x + 1 \\ &= x^2 - \frac{259}{15}x + 1, \end{aligned}$$

which we can give as $15x^2 - 259x + 15$, since this has the same roots by [theorem 3.16](#).

Now we proceed to give a simpler solution using [theorem 3.18](#).

Solution using [theorem 3.18](#): By the theorem, we have $\Sigma = \alpha + \beta = 17$, and $\Pi = \alpha\beta = 15$. Now since the required expression is also a quadratic,

then it will be of the same form, that is, $x^2 - \Sigma x + \Pi$, where the new sum (Σ_N) and product (Π_N) are $\Sigma_N = \frac{\alpha}{\beta} + \frac{\beta}{\alpha} = \frac{\alpha^2 + \beta^2}{\alpha\beta} = \frac{(\alpha + \beta)^2 - 2\alpha\beta}{\alpha\beta} = \frac{17^2 - 2(15)}{15} = \frac{259}{15}$, and $\Pi_N = \left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right) = 1$. Hence the required quadratic is $x^2 - \Sigma_N x + \Pi_N = x^2 - \frac{259}{15}x + 1$, which has the same roots as $15x^2 - 259x + 15$.

Exercise 3.21. 1. Determine the nature of the roots of the following quadratic equations without solving them.

a) $x^2 - 2x = -5$

b) $x^2 - 5x + 9 = x$

c) $5x^2 - 5x + 1 = 0$

d) $k^2x^2 + kx + 4 = 0$, given that $k \neq 0$

e) $x^2 - kx + 2k = x + k$, given that $k \neq 1$

f) $kx^2 = k$, given that $k \neq 0$

2. For what value(s) of k do the following quadratics have repeated roots?

a) $x^2 + 2kx + 1$ b) $3x^2 + x + k$ c) $kx^2 + kx + 4$

3. Prove that the roots of the equation $4 + b - bx - x^2 = 0$ are real and distinct for any $b \in \mathbb{R}$.

4. Consider the quadratic $\phi(x) = x^2 - 6x + 13$.

a) Prove that ϕ has no real roots.

b) Suppose that i is a special number with the property that $i^2 = -1$ (we know that there is no such real number, but pretend it exists anyway). Show that $3 + 2i$ and $3 - 2i$ are roots of the quadratic ϕ .

c) Suppose the quadratic $ax^2 + bx + c$ has no real roots. Show that $x = \frac{-b \pm i\sqrt{-\Delta}}{2a}$ are two roots of this quadratic, where i behaves as described in part (b).

5. Prove the following, and **memorise them well!**

a) $\alpha^2 + \beta^2 = (\alpha + \beta)^2 - 2\alpha\beta$

$$\text{b) } \alpha^3 + \beta^3 = (\alpha + \beta)^3 - 3\alpha\beta(\alpha + \beta)$$

6. Given the equation $2x^2 + 7x - 3 = 0$ has roots α and β , form QEs whose roots are given by the following expressions:

$$\text{a) } \alpha^2, \beta^2 \qquad \text{b) } \alpha^3, \beta^3 \qquad \text{c) } \frac{2}{\alpha}, \frac{2}{\beta}$$

$$\text{d) } \frac{1}{\alpha^2}, \frac{1}{\beta^2} \qquad \text{e) } \alpha^3 - 1, \beta^3 - 1 \qquad \text{f) } \frac{\alpha + 1}{\alpha}, \frac{\beta + 1}{\beta}$$

$$\text{g) } \frac{\alpha^2}{\beta}, \frac{\beta^2}{\alpha} \qquad \text{h) } \frac{\alpha}{\alpha + \beta}, \frac{\beta}{\beta + \alpha} \qquad \text{i) } \alpha + 3\beta, \beta + 3\alpha$$

7. The equation $x^2 + (2r - 3)x + 1 = 0$ has the roots α and β . Form an equation whose roots are $\frac{\alpha}{\alpha\beta + 1}$ and $\frac{\beta}{\alpha\beta + 1}$.

8. One of the roots of the equation $x^2 + px + 8 = 0$ is the square of the other. Find p .

9. The equation $rx^2 + p = x + 1$ has one root double the other. Show that $2 = 9r(p - 1)$.

- \supset 10. If α and β are the roots of $x^2 - 2kx + k - 2 = 0$, form the quadratic equation whose roots are $\frac{\alpha^2}{\beta} - 1, \frac{\beta^2}{\alpha} - 1$.

- \supset 11. Given that the equation $ax^2 + bx + c = 0$ has roots α and β , form QEs whose roots are given by:

$$\text{a) } a\alpha, a\beta \qquad \text{b) } \frac{b\alpha}{\beta^2}, \frac{b\beta}{\alpha^2} \qquad \text{c) } \frac{1}{\alpha - c}, \frac{1}{\beta - c}$$

12. If α^2 and β^2 are the roots of the equation $x^2 - 10x + 9 = 0$, where $\alpha, \beta > 0$, evaluate $\alpha\beta$ and $\alpha + \beta$. Hence, write down the equation whose roots are α and β .

13. Show that if a and b are both positive or both negative, then

$$\frac{x}{x - a} + \frac{x}{x - b} = 1$$

has two distinct real solutions.

4 Logarithms

Here we introduce the idea which is, in a sense, the “opposite” of an index.

Definition 4.1 (Logarithm). Let $a, x \in (0, \infty)$ such that $a \neq 1$. The *logarithm of x to base a* , denoted

$$\log_a x,$$

is a number $y \in \mathbb{R}$ such that $a^y = x$.

Example 4.2. For example, $\log_2 8 = 3$, and $\log_5 5 = 1$. Indeed, $\log_x x = 1$ for any $x \in (0, \infty)$.

Theorem 4.3. Let $a, x \in (0, \infty)$ where $a \neq 1$. Then $\log_a x$ exists, and moreover it is unique, that is, there exists only one real number y such that $a^y = x$.

Proving the existence and uniqueness of $\log_a x$ in \mathbb{R} requires a lot of work (analysis) which we will not bother getting into here, but might revisit it later.

Theorem 4.4. Let $a \in (0, \infty)$ where $a \neq 1$. Then $\log_a x$ is an injection, that is, if $\log_a x = \log_a y$, then $x = y$.

Later on when doing functions, we will talk more about injections. The function $f(x) = (x-1)^2$ is not an injection for example, since $f(3) = f(-1)$, but $3 \neq -1$. In general, just because two outputs of a function are the same, it doesn't mean the two inputs are the same. But for \log_a , it is true.

Examples 4.5. We give two examples of applications of logarithms. First, we solve the equation $4^x = 8$. By the definition, the desired x is given by $\log_4 8$. Indeed, plugging this into a calculator gives $x = 3/2$. Let us verify that this is the answer:

$$4^{3/2} = 4^{3 \cdot \frac{1}{2}} = (4^3)^{1/2} = 64^{1/2} = \sqrt{64} = 8,$$

as required.

Now suppose we place €2000 in a bank savings account, which offers 1.2% interest per annum. How many years must pass before the account balance exceeds €2500, assuming that no other deposits/withdrawals are made? Well, the first step here is to notice that the balance after a year is given by $\text{€}2000 + 1.2\%(\text{€}2000) = \text{€}2000(1 + 1.2\%) = \text{€}2024$. Similarly for the next year, we do $\text{€}2024 + 1.2\%(\text{€}2024) = \text{€}2024(1 + 1.2\%) = \text{€}2048.29$. But this is the same as $\text{€}2000(1 + 1.2\%)(1 + 1.2\%)$. In fact for the next year, we

would work out $\text{€}2000(1 + 1.2\%)(1 + 1.2\%)(1 + 1.2\%)$, and in general, after n years, the balance is $\text{€}2000(1 + 1.2\%)^n$.

So what we want is a value n such that $\text{€}2000(1 + 1.2\%)^n = \text{€}2500$. This equation simplifies to $\left(\frac{253}{250}\right)^n = \frac{5}{4}$, so the required n is given by $\lceil \log_{\frac{253}{250}}\left(\frac{5}{4}\right) \rceil = 19$ years.⁶

Theorem 4.6 (Laws of Logarithms). *Let $a, x, y \in (0, \infty)$ such that $a \neq 1$, and let $c \in \mathbb{R}$. Then we have the following laws.*

$$\text{I)} \quad \log_a x + \log_a y = \log_a(xy)$$

$$\text{II)} \quad \log_a x - \log_a y = \log_a\left(\frac{x}{y}\right)$$

$$\text{III)} \quad c \log_a x = \log_a(x^c)$$

Proof. Let $u = \log_a x$ and $v = \log_a y$. By definition of \log_a , it follows that $a^u = x$ and $a^v = y$. Now by law I of indices ([theorem 2.19](#)), we have

$$xy = a^u a^v = a^{u+v},$$

converting this equation to log form we get $\log_a(xy) = u+v = \log_a x + \log_a y$, proving I. Similarly by law II of indices, we have

$$\frac{x}{y} = \frac{a^u}{a^v} = a^{u-v},$$

and converting this equation to log form we get $\log_a\left(\frac{x}{y}\right) = u - v = \log_a x - \log_a y$, proving II. Finally by law III of indices, we have

$$a^u = x \implies (a^u)^c = x^c \implies a^{cu} = x^c,$$

and converting to log form we get $\log_a(x^c) = cu = c \log_a x$, proving III, as required. \square

Example 4.7. Before calculators, these laws were essential to be able to evaluate logarithms using logarithm tables. Given that $\log_2 3 \approx 1.584$ and $\log_2 5 \approx 2.322$, we find $\log_2 5400$. Indeed, $\log_2 5400 = \log_2(2^3 \cdot 5^2 \cdot 3^3)$ by prime factor decomposition. By law I this becomes $\log_2(2^3) + \log_2(5^2) + \log_2(3^3)$, which then by law III becomes $3 \log_2 2 + 2 \log_2 5 + 3 \log_2 3 = 3(1) + 2(2.322) + 3(1.584) = 12.396$.

⁶ $\lceil x \rceil$ denotes the *ceiling* of x , i.e., the smallest integer larger than x . Here we are using it since presumably, the interest is computed at the end of the year. Since 18 years are not sufficient ($\log_{\frac{253}{250}}\left(\frac{5}{4}\right) \approx 18.71$), we round up to 19 years.

Definition 4.8 (Standard Bases). The following conventions are used for different logarithm bases.

- (i) $\log x$ or $\lg x$ denote $\log_{10} x$, which is referred to the *common logarithm*.
- (ii) $\ln x$ denotes $\log_e x$ and is called the *natural logarithm*, where $e \approx 2.718$ is an important constant we will discuss later.
- (iii) $\text{lb } x$ denotes $\log_2 x$, and is called the *binary logarithm*.

Theorem 4.9 (Change of Base). Let $a, x, B \in (0, \infty)$ where $a \neq 1 \neq B$. Then

$$\log_a x = \frac{\log_B x}{\log_B a}.$$

This theorem tells us that the logarithm in any base can be expressed in terms of logarithms of any other base. In fact in some textbooks, the only logarithm introduced is the natural logarithm $\ln x$, and then $\log_a x$ is defined to be short for $\ln x / \ln a$.

Exercise 4.10. 1. Express the following in terms of a , b and c ; where $a = \log x$, $b = \log y$ and $c = \log z$.

- a) $\log xyz$ b) $\log \frac{x}{zy}$ c) $4 \log y \sqrt{x}$
- d) $\log 4x - \log 3y$ e) $\log(xy)^a$ f) $\ln x$

2. Solve the following equations.

- a) $2^x = 32$ b) $7^x = 14$
- c) $\log 5x = 1$ d) $3^{x^2-3x} = 81$
- e) $2^{x+1} + 4 = 9(2^x)$ f) $216(2^{2n} + 3^{2n}) = 793(6^n)$
- g) $12^{3x+1} \times 15^{5-2x} = 2^{2(2x+1)} \times 3^{3x} \times 5$
- h) $3^{2x+1} = 3^{x+2} + \sqrt{1 - 6(3^x) + 3^{2(x+1)}}$
- i) $\log 5 + \log 2x = 2$ j) $\frac{18 \log_8 x - 8}{\log_8 x} = 9 \log_8 x$
- k) $4 \log x = 2 \log x - \log \frac{625}{4}$ l) $\text{lb}(5 - x^2) = 2 \text{lb}(1 - x)$

$$\text{m) } \log_x 27 - \log_x x = \frac{2}{\log_{27} 9} \quad \text{n) } \frac{\ln(35 - x^3)}{\ln(5 - x)} = 3$$

$$\text{o) } 100x^{\log x - 2} + x^{2 - \log x} - 20 = 0$$

$$\text{p) } 2 + \log \sqrt{1+x} + 3 \log \sqrt{1-x} = \log \sqrt{1-x^2}$$

3. Show that the unique solution of the equation $2^x 5^{2x} 7^{3x} = 3$ is given by the real number

$$x = \frac{\ln 3}{\ln 2 + 2 \ln 5 + 3 \ln 7}.$$

4. Solve the following systems of equations.

$$\text{a) } \begin{cases} 2 \log y + \log 2 = \log x \\ 5y = x + 2 \end{cases} \quad \text{b) } \begin{cases} \log_3 x \log_3 y = 6 \\ \log_3 xy = 5 \end{cases}$$

$$\text{c) } \begin{cases} 2 \log_2 y + 2 = \log_2 x \\ x + y = 3 \end{cases} \quad \text{d) } \begin{cases} 2 \log(y-1) = \log x \\ 2x = 4 - y \end{cases}$$

$$\text{e) } \begin{cases} \log_2 x - 4 = \log_4 y \\ \log_2(x-2y) = 5 \end{cases} \quad \text{f) } \begin{cases} \log_2 x + \log_4 y - 4 = 0 \\ 3^{x^2} - 9(3^{15y+2}) = 0 \end{cases}$$

5. An amount of €1500 is deposited in a bank paying an annual interest rate of 5% compound interest per year. How many years must pass for this amount to exceed €2000?
6. A certain strain of E-coli bacteria doubles in number 30 minutes. If there are 100 E-coli bacteria that are allowed to grow under ideal conditions, how long will it take to reach 1 million bacteria?
7. The speed of the wind in a tornado, v (km/h), is related to the distance s (km) it travels before dying out by the equation $v = 93 \log_6 s + 63$. If a tornado has wind speed of 95 m/s, how far does it travel?
8. Show that the solutions of the equation $2 \log_2(x+15) - \log_2 x = 6$ are also the solutions of the equation $x^2 + 255 = 34x$ without actually finding the solutions.
9. Let $a, b > 0$. Show that if $\ln \frac{1}{2}(a+b) = \frac{1}{2}(\ln a + \ln b)$, then $a = b$.

10. Prove the following results WITHOUT USING THE CHANGE OF BASE THEOREM.

a) $\log_a b = \log_B b / \log_B a$ for any $0 < B \neq 1$.

b) $\log_{\sqrt{b}} x = 2 \log_b x$

c) $\log_{1/\sqrt{b}} \sqrt{x} = -\frac{1}{2} \log_b x$

d) $\log_{b^4} x^2 = \log_b \sqrt{x}$

$\frac{iii}{\infty}$ 11. Prove that

$$\frac{1}{\log_2 x} + \frac{1}{\log_3 x} + \frac{1}{\log_4 x} + \cdots + \frac{1}{\log_{100} x} = \frac{1}{\log_{100!} x},$$

where $100! = 100 \cdot 99 \cdot 98 \cdots 2 \cdot 1$.

(MATSEC May '17)

5 Polynomials

Here we generalise the idea of a quadratic to that of an algebraic expression containing larger integer powers of the variable x .

5.1 The Basics and Polynomial Division

Definition 5.1 (Polynomial). Let $n \in \mathbb{N} \cup \{0\}$, and let $a_0, a_1, \dots, a_n \in \mathbb{R}$ with $a_n \neq 0$. Any expression of the form

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$$

is said to be a *polynomial in x* , where x is called an *indeterminate* and the a_i 's are called its *coefficients*. The non-negative integer n is called the *degree* of the polynomial, denoted $\deg p$. a_n is called its *leading coefficient*.

Notation. The set of all polynomials with real coefficients is denoted $\mathbb{R}[x]$.

Examples 5.2. We give some examples.

- (i) The expression $12x^7 - 32x^3 + 5x^2 - 3x + 2$ is a polynomial of degree 7, since it is of the form $a_7 x^7 + a_6 x^6 + a_5 x^5 + a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0$, where $a_7 = 12$, $a_3 = -32$, $a_2 = 5$, $a_1 = -3$, $a_0 = 2$ and $a_6 = a_5 = a_4 = 0$.

- (ii) Any linear expression $ax + b$ is a polynomial of degree 1, since it is of the form $a_1x + a_0$.
- (iii) Any quadratic $ax^2 + bx + c$ is a polynomial of degree 2, since it is of the form $a_2x^2 + a_1x + a_0$.
- (iv) Any non-zero real number a_0 is a polynomial of degree 0.

Notation (Abstract polynomial). We want to make the distinction between the notation p and $p(x)$ where p is a polynomial. When we write p alone, we are referring to the polynomial p in the abstract, in the sense that, p is the object with coefficients, p has a degree, and so on. On the other hand, $p(x)$ denotes a real number obtained when x is plugged into p . Therefore it makes no sense to speak of the degree of $p(x)$, or the coefficients of $p(x)$, since concretely, this is just a number.

Now we will abuse this convention slightly when it makes it convenient to write things down. For instance, when we write $ax^2 + bx + c$ as we did in the section on quadratics, then in most cases, we cared about the quadratic as an abstract entity, rather than its value at some particular x . We could write something abstract looking such as $a\square^2 + b\square + c$ to make the distinction clearer, but this looks a bit strange so we will stick to using x . But make sure that you are aware that a distinction is being made.

When we write things like $p + q$ or pq , we are referring to the polynomials defined by $p(x) + q(x)$ and $p(x)q(x)$ for all x respectively. Similarly, if we say that, e.g., “there exists a polynomial s such that $p = qs$ ”, then this polynomial s is such that equality also holds for all x .

Notice therefore that writing something like $p = q$ is different from writing $p(x) = q(x)$. The former means we have equality *for all values of x* , the latter means we have equality for a particular value of x (unless we are “abusing” the convention and letting x stand for any general possible input).

Definition 5.3 (Polynomial Factors). Let $p, q \in \mathbb{R}[x]$ be polynomials. If there exists a polynomial $s \in \mathbb{R}[x]$ such that $p = qs$, then we say that q is a *factor* of p , or that q *divides* p . This relation is denoted by $q \mid p$, and the polynomial s is denoted by p/q .

Example 5.4. The polynomial $q = x - 3$ is a factor of $p = 2x^2 - 7x + 3$, since p can be written as $p = (x - 3)(2x - 1)$. Similarly $s = x - 2$ divides the polynomial $t = 6x^4 - 10x^3 - 7x^2 + 5x + 2$ because t can be written as $t = (x - 2)(3x + 1)(2x^2 - 1)$.

Remark 5.5. The notation p/q agrees with the usual notation for division of real numbers when it makes sense, i.e., if $p = qs$, then for any x , $s(x)$ will be equal to the value of the real number $p(x)/q(x)$, unless $q(x) = 0$. Notice that in the case that $q(x) = 0$, the value of $s(x)$ is still defined; so we can evaluate $(p/q)(x)$ ($\neq p(x)/q(x)$). This is one of the situations where the distinction between p and $p(x)$ is important!

Example 5.6. In the last example, we had $p = (x-3)(2x-1)$ and $q = (x-3)$ and so $p = qs$ where $s = p/q = 2x-1$. Now $(p/q)(1) = s(1) = 2(1) - 1 = 1$, and also $p(1)/q(1) = ((1-3)(2(1)-1))/(1-3) = 1$. However, $(p/q)(3) = s(3) = 2(3) - 1 = 5$, but $p(3)/q(3)$ is not defined since $q(3) = 0$.

Remark 5.7. The degree of the zero polynomial $p(x) = 0$ for all x is not defined. (In particular, it is *not* zero). The reason for this is that the results of the following theorem would not hold otherwise.

Theorem 5.8 (Degree Laws). *Let $p, q \in \mathbb{R}[x]$ be non-zero polynomials. Then*

- (i) $\deg(pq) = \deg p + \deg q$
- (ii) *If $q \mid p$, then $\deg(p/q) = \deg p - \deg q$*
- (iii) *If $n \in \mathbb{N}$, then $\deg(p^n) = n \deg p$*

Proof. For (i), simply observe that if we have $p = a_n x^n + \cdots + a_0$ and $q = b_m x^m + \cdots + b_0$, then

$$pq = (a_n x^n + \cdots + a_0)(b_m x^m + \cdots + b_0) = a_n b_m x^{n+m} + \cdots + a_0 b_0,$$

so $\deg(pq) = n + m = \deg p + \deg q$.

For (ii), if $q \mid p$, then by definition $p = qs$ for some $s \in \mathbb{R}[x]$. Therefore $\deg p = \deg(qs) = \deg q + \deg s = \deg q + \deg(p/q)$ by (i).

Finally for (iii), observe that by (i), $\deg(p^n) = \deg(p \cdots p) = \deg p + \cdots + \deg p = n \deg p$. \square

Note. Observe the similarity between these degree laws and the laws of logarithms ([theorem 4.6](#)). This is not a coincidence, but sadly we cannot get into it more.

Example 5.9. These laws allow us to determine the degrees of polynomial products on inspection. For example, using law (i), we get

$$\deg((x+2)(3x-4)(x^2+1)) = 1 + 1 + 2 = 4,$$

and another example,

$$\deg((x-3)^2(5-2x)^3(x^3-9x+4)^2) = 2 \cdot 1 + 3 \cdot 1 + 2 \cdot 3 = 11,$$

by (i) and (iii).

Definition 5.10 (Rational Function). A *rational function* is any expression of the form

$$\frac{p}{q}$$

where $p, q \in \mathbb{R}[x]$ are polynomials. Furthermore, if $\deg p < \deg q$, we say that p/q is *proper*. Otherwise if $\deg p \geq \deg q$ we say that p/q is *improper*.

Examples 5.11. The following are rational functions.

$$\frac{5x^2 - 6x}{x^3 + 5x - 4} \quad \frac{x^2 - 3x + 2}{4x^2 - 5x + 3} \quad \frac{x^6}{x^5 + x^2 - 4}$$

The first one is proper, the second two are improper.

In general, $(p/q)(x)$ equals $p(x)/q(x)$ for any x unless $q(x) = 0$, in which case, it is either undefined, or can be assigned a value if p and q have common factors which cancel, so that we can evaluate it as in [remark 5.5](#).

Now, in primary school, fractions such as $\frac{7}{3}$ were described as improper, and we would instead write them as mixed numbers; so $\frac{7}{3}$ becomes $2\frac{1}{3}$ (i.e., $2 + \frac{1}{3}$). The conversion from improper fractions to mixed numbers involved a process called *long division*. Here we introduce an analogue to long division for polynomials.

Theorem 5.12 (Euclidean Algorithm). *Let $p, q \in \mathbb{R}[x]$ with $\deg p \geq \deg q$. Then we may write the rational function p/q as*

$$s + \frac{r}{q},$$

where $s, r \in \mathbb{R}[x]$ are polynomials such that:

- $\deg s = \deg p - \deg q$,
- $r = 0$ or $\deg r < \deg q$ (so that r/q is proper).

Proof. Suppose $p, q \in \mathbb{R}[x]$ are $p = a_n x^n + \cdots a_0$ and $q = b_m x^m + \cdots b_0$, where $\deg p = n \geq m = \deg q$. Define $s = \frac{a_n}{b_m} x^{n-m}$. The key is to observe that we can transform p/q by writing it as

$$\frac{p}{q} = s + \frac{p - qs}{q},$$

where it's easy to see that $\deg(p - qs) < \deg p$, since the leading term $a_n x^n$ is eliminated. If $(p - qs)/q$ is proper, then we are done, if not, then we carry out the same transformation on $(p - qs)/q$, which gives

$$\frac{p}{q} = s + s' + \frac{(p - qs) - qs'}{q},$$

where we are denoting the “new” s by s' . Now $\deg((p - qs) - qs') < \deg(p - qs) < \deg p$. We keep doing this procedure until the degree of the numerator is less than $m = \deg q$ (or if the numerator equals zero), at which point we are done. Clearly the degree of the obtained polynomial $s + s' + \cdots$ is $\deg(s) = n - m = \deg p - \deg q$. \square

Example 5.13. The best way to understand the Euclidean algorithm (and its proof) is to work through an example. Consider the improper rational function

$$\frac{p}{q} = \frac{3x^4 - x + 1}{x^2 + 2x - 1}.$$

In the proof, we defined s as the ratio of the leading term of the polynomial in the numerator ($a_n x^n$ in p) to that in the denominator ($b_m x^m$ in q), so for this example we have $s = 3x^4/x^2 = 3x^2$. Then we used the fact that

$$\frac{p}{q} = \frac{p + qs - qs}{q} = \frac{qs}{q} + \frac{p - qs}{q} = s + \frac{p - qs}{q},$$

and most importantly, since the term $a_n x^n$ appears both in p and in qs , the degree of the numerator $p - qs$ is less than that $n = \deg p$. Applying this reasoning to our example, we have

$$\begin{aligned} \frac{p}{q} &= 3x^2 + \frac{3x^4 - x + 1 - (x^2 + 2x - 1)(3x^2)}{x^2 + 2x - 1} \\ &= 3x^2 + \frac{3x^4 - x + 1 - (3x^4 + 6x^3 - 3x^2)}{x^2 + 2x - 1} \\ &= 3x^2 + \frac{-6x^3 + 3x^2 - x + 1}{x^2 + 2x - 1}, \end{aligned}$$

and as we can see, the degree of the numerator has decreased, however the fraction is still improper. We therefore apply the same procedure again on the result, and the “new” s is now $-6x^3/x^2 = -6x$:

$$\frac{p}{q} = 3x^2 - 6x + \frac{-6x^3 + 3x^2 - x + 1 - (-6x)(x^2 + 2x - 1)}{x^2 + 2x - 1}$$

$$\begin{aligned}
&= 3x^2 - 6x + \frac{-6x^3 + 3x^2 - x + 1 - (-6x^3 - 12x^2 + 6x)}{x^2 + 2x - 1} \\
&= 3x^2 - 6x + \frac{15x^2 - 7x + 1}{x^2 + 2x - 1}.
\end{aligned}$$

The fraction is still improper, however one more iteration yields

$$\begin{aligned}
\frac{p}{q} &= 3x^2 - 6x + 15 + \frac{15x^2 - 7x + 1 - 15(x^2 + 2x - 1)}{x^2 + 2x - 1} \\
&= 3x^2 - 6x + 15 + \frac{16 - 37x}{x^2 + 2x - 1},
\end{aligned}$$

which is finally proper.

Notation. In view of this method being the analogue to *long division* for polynomials, we adopt a similar way of denoting the procedure. Instead of proceeding as we have done in the example above, we instead write out the problem as a long division problem:

$$\begin{array}{r}
x^2 + 2x - 1 \overline{) 3x^4 - x + 1}
\end{array}$$

Notice that we leave room for any terms in x^3 or x^2 to appear, organising the terms in non-overlapping “columns”.

We start the algorithm just as before, by computing the ‘s’ term, which is the result of dividing the right-most term below the division sign with the right-most term of the polynomial outside division sign. This is written above the division sign.

$$\begin{array}{r}
 \\
x^2 + 2x - 1 \overline{) 3x^4 - x + 1}
\end{array}$$

Next we multiply the term above by the polynomial outside the division sign to get the equivalent of qs . This is written underneath the polynomial below the division sign, and the signs are flipped, so that we have $-qs$.

$$\begin{array}{r}
 \\
x^2 + 2x - 1 \overline{) 3x^4 - x + 1} \\
 \underline{- 3x^4 - 6x^3 }
\end{array}$$

Next, we add to get $p - qs$. This will only differ from p in terms of degree 2 or higher, so we can just add those for now, and copy the $-x$ down for the next stage.

$$\begin{array}{r} \quad \quad \quad 3x^2 \\ x^2+2x-1) \overline{3x^4} - x + 1 \\ \underline{-3x^4-6x^3} \\ - x \end{array}$$

If $p - qs$ had degree less than 2, we would be done, but here the degree is 3, so we start the procedure again, dividing the leading coefficient of the remainder by the leading coefficient of the divisor, writing this “new s ” in the appropriate column at the top.

[illegible]

Multiplying this by q and flipping signs, we get the “new $p - qs$ ”

$$\begin{array}{r} \quad \quad \quad 3x^2 - 6x \\ x^2 + 2x - 1) \overline{ 3x^4 - x } \\ \underline{- 3x^4 - 6x^3 } \\ \quad \quad \quad - 6x^3 + 3x^2 - x \\ \quad \quad \quad \underline{6x^3 + 12x^2 - 6x} \end{array}$$

Adding the terms affected (those with degree 1 and higher) and copying the +1 down for the next stage, we get

$$\begin{array}{r} \quad \quad \quad 3x^2 - 6x \\ x^2 + 2x - 1) \overline{ 3x^4 - x } \\ \underline{- 3x^4 - 6x^3 } \phantom{- x } \\ \quad \quad \quad - 6x^3 + 3x^2 - x \\ \quad \quad \quad \underline{6x^3 + 12x^2 - 6x} \\ \quad \quad \quad 15x^2 - 7x + 1 \end{array}$$

We check the degree again, and since it's not less than 2, we repeat the procedure to finally arrive at

[illegible]

Which corresponds to the fact that

$$\frac{3x^4 - x + 1}{x^2 + 2x - 1} = 3x^2 - 6x + 15 + \frac{-37x + 16}{x^2 + 2x + 1},$$

as we obtained previously.

Examples 5.14. Here are two more examples with this new notation. To divide $(x^3 - 8x^2 + 3x - 1)/(x^2 - 7x + 2)$, we do

$$\begin{array}{r} x-1 \\ x^2-7x+2 \overline{) \quad x^3-8x^2+3x-1} \\ \underline{-x^3+7x^2-2x} \\ -x^2+x-1 \\ \underline{x^2-7x+2} \\ -6x+1 \end{array}$$

so

$$\frac{x^3 - 8x^2 + 3x -}{x^2 - 7x + 2} = x - 1 + \frac{1 - 6x}{x^2 - 7x + 2},$$

and for $(2x^2 - 2x + 2)/(3x^2 + 3x + 1)$, we do

$$\begin{array}{r} 2 \\ 3 \\ 3x^2 + 3x + 1 \overline{) 2x^2 - 2x + 2} \\ \underline{- 2x^2 - 2x - \frac{2}{3}} \\ -4x + \frac{4}{3} \end{array}$$

so

$$\frac{2x^2 - 2x + 2}{3x^2 + 3x + 1} = \frac{2}{3} - \frac{12x - 4}{3(3x^2 + 3x + 1)}.$$

Exercise 5.15. 1. State whether the following rational functions are proper or improper.

a) $\frac{4x^2 + 7x - 3}{2x + 1}$

b) $\frac{4t + 1}{3t - 1}$

c) $\frac{4x^2 - 28}{3x}$

d) $\frac{x^3 + x^2 + x + 1}{x^2 + x + 1}$

e) $\frac{4x^4 + 3x^3 + 2x^2 + x}{x + 1}$

f) $\frac{(x - 1)(x - 2)(x - 3)}{(x + 1)(x + 2)}$

g) $\frac{4x^3 + x}{16x^6 - x^2}$

h) $\frac{1}{x + 1}(x^3 - 27)$

i) $\frac{\pi x + 2\pi + \pi^2}{2(x + \pi)}$

j) $\frac{x^4 - x^2 - 2x - 1}{x^2 + x + 1}$

2. Convert the improper fractions from the exercise above to proper fractions.

Now we will conclude with some more theory which will be useful in future sections.

Definition 5.16 (Monic). A polynomial p is said to be *monic* if its leading coefficient is 1, i.e., if $\deg p = n$, then the coefficient of x^n in p is 1.

Recall that the *highest common factor* of two integers a and b is the largest positive integer k such that $k \mid a$ and $k \mid b$ (i.e., k divides both a and b). For example, the highest common factor of 15 and 25 is 5, and that of 27 and 36 is 9.

Definition 5.17 (Polynomial hcf). Let p, q be two polynomials. Then the highest common factor of p and q , denoted $\text{hcf}(p, q)$, is the monic polynomial s of largest degree such that $s \mid p$ and $s \mid q$.

Example 5.18. If $p = x^4 + 2x^3 + x + 2$ and $q = 3x^4 - 4x^3 - 43x^2 - 56x - 20$, we have $\text{hcf}(p, q) = x^2 + 3x + 2$, since in factorised form, these polynomials are $p = (x + 1)(x + 2)(x^2 - x + 1)$, $q = (x + 1)(x + 2)(x - 5)(3x + 2)$ and $x^2 + 3x + 2 = (x + 1)(x + 2)$. Notice we require the additional constraint that the hcf is monic so that it is unique, otherwise any constant multiple of the hcf still divides both p and q .

An important fact about the hcf is the following.

Proposition 5.19. *The highest common factor $\text{hcf}(p, q)$ of two polynomials $p, q \in \mathbb{R}[x]$ exists and is unique.*

We will not prove this fact because it requires some advanced algebra (namely the theory of Euclidean rings). But it plays a key role in the proof of the following result.

Theorem 5.20 (Bézout’s lemma). *Let $p, q \in \mathbb{R}[x]$ be two polynomials. Then there exist $s, t \in \mathbb{R}[x]$ such that*

$$s(x)p(x) + t(x)q(x) = 1,$$

where $\deg(s) < \deg(q)$ and $\deg(t) < \deg(p)$.

We will not prove this result either, but it is essentially a consequence of [theorem 5.12](#) plus some advanced algebra.

5.2 The Remainder and Factor Theorems

With numbers, the term “remainder” refers to the quantity left over when performing division. For example, if we divide 17 by 3, then we get

$$\frac{17}{3} = 5 + \frac{2}{3},$$

so the remainder is 2. Notice that the remainder is always less than the divisor. For polynomials, we have the analogous notion, where we perform long division to get

$$\frac{p}{q} = s + \frac{r}{q},$$

and $\deg(r) < \deg(q)$ (or $r = 0$). Sometimes it is more useful to look at this relation in the form $p = qs + r$. The corresponding equality for the numeric example would be $17 = 3 \cdot 5 + 2$. But unlike numbers, polynomials have a variable which we can substitute for. This allows us to prove the following.

Theorem 5.21 (Remainder theorem). *Let $p \in \mathbb{R}[x]$ be a polynomial. Then the remainder upon division by $(x - \alpha)$ is $p(\alpha)$.*

Proof. First of all notice that if we divide by $(x - \alpha)$, then the remainder has $\deg(r) < \deg(x - \alpha) = 1$, i.e., the remainder is a constant. After division, we can write $p(x) = s(x)(x - \alpha) + r$. In particular, this is true when $x = \alpha$, which gives us that $p(\alpha) = s(\alpha)(0) + r$, i.e., $r = p(\alpha)$. \square

This allows us to determine the remainder of a division without having to actually perform the division! (Albeit limited to linear divisors.)

Example 5.22. Say we divide $p(x) = x^4 + 3x^3 + 5x^2 + 7x + 9$ by $x + 1$. Then the remainder should be equal $p(-1)$ (since $(x + 1) = (x - (-1))$), i.e.,

$$r = p(-1) = (-1)^4 + 3(-1)^3 + 5(-1)^2 + 7(-1) + 9 = 5.$$

Indeed, if we do the division, we get

$$\begin{array}{r}
 x^3 + 2x^2 + 3x + 4 \\
 x + 1 \overline{) x^4 + 3x^3 + 5x^2 + 7x + 9} \\
 \underline{-x^4 - x^3} \\
 2x^3 + 5x^2 \\
 \underline{-2x^3 - 2x^2} \\
 3x^2 + 7x \\
 \underline{-3x^2 - 3x} \\
 4x + 9 \\
 \underline{-4x - 4} \\
 5
 \end{array}$$

which gives

$$\frac{x^4 + 3x^3 + 5x^2 + 7x + 9}{x + 1} = x^2 + 2x + 3x + 4 + \frac{5}{x + 1},$$

as expected.

Remark 5.23. Notice that if we are dividing by a factor of the form $(ax + b)$, for the purposes of the remainder theorem, this is equivalent to dividing by $(x - (-b/a))$. Indeed, if

$$p(x) = s(x)(ax + b) + r,$$

putting $x = -b/a$ gives $p(-b/a) = s0 + r$, i.e., $r = p(-b/a)$.

Why is this theorem particularly useful? Why should we care about being able to find the remainder if we still have to do long division for the quotient? Well, if it happens that the remainder is zero, then we get

$$p(x) = q(x)(x - \alpha) + r = (x - \alpha)q(x),$$

i.e., we will have determined a linear factor of $q(x)$. In other words, we have

Theorem 5.24 (Factor theorem). *Let $p \in \mathbb{R}[x]$ be a polynomial. Then $p(\alpha) = 0$ if and only if $(x - \alpha) \mid p$.*

Proof. If $p(\alpha) = 0$, then by the remainder theorem, we get that $p(x) = (x - \alpha)s(x)$.

Conversely, if $(x - \alpha) \mid p$, then $p(x) = (x - \alpha)s(x)$ and so $p(\alpha) = 0$. \square

This allows us to prove various following fundamental facts about polynomials. But first we will need to generalise it slightly. If α is a root of p , then by the factor theorem, $(x - \alpha) \mid p$, and so $p/(x - \alpha)$ is a polynomial. Now if α is a root of this polynomial, then applying the factor theorem again gives us that $(x - \alpha) \mid (p/(x - \alpha))$, or, $(x - \alpha)^2 \mid p$. But this in turn implies that $p/(x - \alpha)^2$ is a polynomial, and we can ask again whether α is a root of this new polynomial. If this is the case, we will similarly get that $(x - \alpha)^3 \mid p$, and so on. This idea gives rise to the following definition.

Definition 5.25 (Multiplicity). Let $f \in \mathbb{R}[x]$ be a polynomial, and let $\alpha \in \mathbb{R}$ be a real root of f , so that $(x - \alpha) \mid f$ by the factor theorem and so $f/(x - \alpha)$ is a polynomial. Then α is said to be *repeated* if it is also a root of $f/(x - \alpha)$, or equivalently, if $(x - \alpha)^2 \mid f$.

More generally, we say that α is a *root with multiplicity n* if n is the largest integer such that $(x - \alpha)^n \mid f$.

Notice this definition is compatible with the notion of repeated root for quadratics introduced in [theorem 3.12](#). If we say that a polynomial has roots $\alpha_1, \dots, \alpha_n \in \mathbb{R}$, we do not exclude the possibility that some of the α_i are equal to each other, and interpret n occurrences of the same α_i as its multiplicity.

Examples 5.26. The polynomial $x^3 - 1$ has one root, namely $x = 1$ with multiplicity 1, since it factorises as $(x - 1)(x^2 + x + 1)$ and the second factor has discriminant -3 . The polynomial $x^5 + 3x^4 + 4x^3 + 4x^2 + 3x + 1$ has only one root, but it has multiplicity 3. Indeed, its factorisation is $(x - 1)^3(x^2 + 1)$.

Now we can state a generalisation of [theorem 3.16](#).

Theorem 5.27. *Let $p \in \mathbb{R}[x]$ be a non-zero polynomial of degree n with s real roots $\alpha_1, \dots, \alpha_s \in \mathbb{R}$ (possibly repeated). Then*

$$p(x) = (x - \alpha_1) \cdots (x - \alpha_s) q(x).$$

where q is either a polynomial with $\deg(q) = n - s$ or the zero polynomial.

Proof. If p is the zero polynomial, then the result is obvious, we can take any $\alpha_i \in \mathbb{R}$ we want and then set q to be the zero polynomial. So suppose $p \neq 0$. By the factor theorem, $p(\alpha_1) = 0$, so we may express p as $p(x) = (x - \alpha_1)t(x)$. Now if $t(\alpha_1) = 0$ (i.e., α_1 is a repeated root), then we can apply the factor theorem to t and get that $p(x) = (x - \alpha_1)^2 u(x)$. Repeating the process until α_1 is no longer a root, we will obtain $p(x) = (x - \alpha_1)^{m_1} v(x)$, where $v(\alpha_1) \neq 0$, and m_1 denotes the multiplicity of α_1 . Now if there are roots left (i.e., if they weren't all equal to α_1), then there is a root α_2 (let's keep the subscripts simple) so that $\alpha_2 \neq \alpha_1$ and $0 = p(\alpha_2) = (\alpha_1 - \alpha_2)^{m_1} v(\alpha_2)$. Since $(\alpha_1 - \alpha_2)^{m_1} \neq 0$, then we must have $v(\alpha_2) = 0$, and so $(x - \alpha_2) \mid v$, and we can write $p = (x - \alpha_1)^{m_1} (x - \alpha_2) w(x)$. Continuing similarly, accounting for repeated roots, we get that $p(x) = (x - \alpha_1) \cdots (x - \alpha_s) q(x)$ and $q \neq 0$.

Finally by [theorem 5.8\(i\)](#), we see that $n = \deg(p) = s + \deg(q)$. \square

As an immediate consequence, we have an upper-bound to the number of roots of a polynomial.

Theorem 5.28. *Let $p \in \mathbb{R}[x]$ be a non-zero polynomial of degree n . Then p can have at most n roots (including multiplicity).*

Proof. Suppose p has s roots $\alpha_1, \dots, \alpha_s$. Then $p = (x - \alpha_1) \cdots (x - \alpha_s) q(x)$ with $q \neq 0$, and so

$$\begin{aligned} \deg(p) &= \deg((x - \alpha_1) \cdots (x - \alpha_s) q(x)) \\ &= \deg((x - \alpha_1) \cdots (x - \alpha_s)) + \deg(q(x)) \\ &\geq \deg((x - \alpha_1) \cdots (x - \alpha_s)) = s, \end{aligned}$$

so number of roots is at most the degree, as required. \square

In general, the roots of polynomial equations of degree higher than 2 are not as simple to understand. But what can these theorems tell us about the next type of polynomial, namely, those of degree 3? These are called *cubics*. Well, we know that the cubic can have at most 3 roots by [theorem 5.28](#). In particular, it can have zero, one or three real roots (including multiplicity), since if it has one root, it will be equal to

$$(x - \alpha_1) q(x)$$

where $q(x)$ has degree two, but if it has two roots, it will equal

$$(x - \alpha_1)(x - \alpha_2) q(x)$$

and $q(x)$ will be linear, i.e., $q(x) = a(x - \alpha_3)$, which introduces a third root. So a cubic cannot have precisely two roots. Moreover, we will later see that, unlike a quadratic, a cubic $ax^3 + bx^2 + cx + d$ cannot have zero roots. The intuitive reason for this is that when x is very large in size (think of $x = 10\,000$), then x^3 is much larger than the remaining terms, and the value of the polynomial at x is approximately ax^3 . Thus assuming $a > 0$, if x is large positive, the value of the polynomial at x is large and positive, and similarly if x is large and negative, then the value of the polynomial at x is large and negative. (If $a < 0$, then things are the other way around). Either way, we have that at some point, the polynomial is positive, and at another point, the polynomial is negative. Because polynomials behave “nicely” (they are continuous, as we will discuss later), we will see that they must take on all values in between these extremes, and in particular, the cubic must take on the value zero for some x between these two “large” inputs. Thus, a cubic has at least one root.

In conclusion, a cubic always has either 1 or 3 real roots.

But this is not very helpful, since the roots are rarely easy to obtain unless the polynomial is hand-picked. (i.e., if I give you the cubic $(x - 1)(x - 2)(x - 3)$, then clearly its roots are simple, but if I randomly pick coefficients for x^3 , x^2 , x and 1, even if they are all integers, then the roots can be complicated to express.) Take the innocent looking $x^3 + 4x - 1$. Then this cubic only has one real root, and it is given by

$$4\sqrt[3]{\frac{2}{3(-9 + \sqrt{849})}} - 4\sqrt[3]{\frac{2}{3(9 + \sqrt{849})}},$$

and the reasoning to obtain such an expression can sometimes involve non-trivial algebraic difficulties. This was not a specially picked polynomial whose root is particularly ugly, these were literally the first three random numbers I picked as coefficients. This is what “normal” cubic roots look like. The picture gets a lot worse for polynomials of higher degree. It turns out that if a fourth degree polynomial has roots, then they will be expressible (usually as some horrible humongous expression) involving square ($\sqrt{}$), cube ($\sqrt[3]{}$) and fourth ($\sqrt[4]{}$) roots. But for degree 5 and higher, most roots cannot be written down using any combination of n th roots, for n as large as you like, and we can only speak of their existence and approximate them numerically as decimals. The very profound and elegant theory behind these facts is called Galois theory, which was developed by the French mathematician Évariste Galois in the 19th century. He died at the age of 20 in a pistol duel

(allegedly over a woman), and he was so convinced of his impending death that he stayed up all night writing letters to his Republican friends and composing what would become his mathematical testament, the famous letter to Auguste Chevalier outlining his ideas, and three attached manuscripts.

Therefore, when it comes to polynomials of degree higher than 2, we will restrict our interests to roots which are rational. In particular, we have the following condition for the existence of rational roots which we will find useful.

Theorem 5.29 (Rational roots theorem). *Let $p \in \mathbb{Z}[x]$ be a polynomial*

$$p(x) = a_n x^n + \cdots + a_0$$

with integer coefficients. Then if $x = c/d$ is a root, $c \mid a_0$ and $d \mid a_n$.

Proof. We can assume that c and d share no common factors (i.e., the fraction is in its lowest form). If $p(c/d) = 0$, then

$$\begin{aligned} a_n \left(\frac{c}{d}\right)^n + a_{n-1} \left(\frac{c}{d}\right)^{n-1} + \cdots + a_1 \left(\frac{c}{d}\right) + a_0 &= 0 \quad (\times d^n) \\ \implies c(a_n c^{n-1} + a_{n-1} c^{n-2} d + \cdots + a_1 d^{n-1}) &= -a_0 d^n, \end{aligned}$$

since both sides are integers, we get that c divides $-a_0 d^n$. Moreover, since c and d share no factors, it follows that $c \mid a_0$. On the other hand, we can rearrange the last equation to get

$$d(a_n c^{n-1} + \cdots + a_1 c d^{n-2} + a_0 d^{n-1}) = -a_n c^n,$$

and by similar reasoning, $d \mid a_n$. □

Example 5.30. The polynomial $2x^3 + 7x^2 + 16x + 15$ has $x = -3/2$ as a root. Indeed, $3 \mid 15$ (the constant coefficient), and $2 \mid 2$ (the leading coefficient). Notice that this is a *necessary* but *not sufficient* condition for the existence of a rational root. For instance, for the same polynomial, we have $5 \mid 15$ and $1 \mid 2$, but $5 = 5/1$ is not a root.

Therefore in general, given an n th degree polynomial

$$a_n x^n + \cdots + a_0,$$

with integer coefficients, we have a method to obtain all possible rational roots/factors. If c_0, \dots, c_k are all the positive divisors of a_0 and d_0, \dots, d_ℓ are all the positive divisors of a_n , then we try substituting

$$x = \pm \frac{c_i}{d_j}$$

for all $1 \leq i \leq k$ and $1 \leq j \leq \ell$. By [theorem 5.29](#), this will exhaust all possible rational roots.

Before we give an example of the method, we will give this useful proposition.

Proposition 5.31 (Comparing coefficients). *Let $f, g \in \mathbb{R}[x]$ be two polynomials of degree n . If $f(x)$ and $g(x)$ agree on $n + 1$ values, then $f = g$ and moreover, f and g have the same coefficients.*

Proof. If $f(x) = g(x)$ for $n + 1$ different values of x , then $f(x) - g(x)$ has $n + 1$ roots. But $\deg(f - g) \leq n$, so by [theorem 5.28](#), $f - g$ is the zero polynomial, i.e., $f(x) = g(x)$ for all values of x , so $f = g$.

Now for the coefficients, notice that the constant term is given by $f(0) = g(0)$, so they have the same constant term, say a_0 . Define a new polynomial f_1 by $f_1(x) = (f(x) - a_0)/x$ and similarly $g_1(x) = (g(x) - a_0)/x$. These are polynomials since we can factor x out of both numerators. Now we have $f_1(0) = g_1(0)$ since these depend only on f and g which are equal for all x . But $f_1(0)$ is the coefficient of x in f and $g_1(0)$ is the coefficient of x in g , so their x -coefficients are equal, say to a_1 . Now define $f_2(x) = (f_1(x) - a_1)/x$ and $g_2(x) = (g_1(x) - a_1)/x$. Continuing this way up to f_n and g_n , we get that all coefficients are equal. \square

Thus from the proposition, we know that, for example, if $x^2 + 1 = ax^2 + bx + c$ for 3 different values of x , then we must have $a = 1$, $b = 0$ and $c = 1$. Now let us give an example of our general method for finding rational roots.

Example 5.32. Say we want to factorise the polynomial

$$p(x) = 4x^4 - 4x^3 + 13x^2 - 12x + 3.$$

The divisors of 3 are 1, 3 and the divisors of 4 are 1, 2, 4. Thus we need to try

$$x = \pm \frac{1}{1}, \pm \frac{1}{2}, \pm \frac{1}{4}, \pm \frac{3}{1}, \pm \frac{3}{2}, \pm \frac{3}{4}.$$

If we do this, we get that only $p(1/2) = 0$, and so $p(x) = (2x - 1)q(x)$ for some cubic q (notice this is equivalent to the factor $(x - 1/2)$). Now we could determine q using long division since $q = p/(2x - 1)$. But a shorter way is possible. Since q is cubic, we have

$$p(x) = (2x - 1)(ax^3 + bx^2 + cx + d).$$

Moreover, it's easy to see that when we expand this, the constant term is $-d$ and the leading coefficient is $2a$. By [proposition 5.31](#), these must be equal to

the coefficients 3 and 4 of p (since we want equality for all $x \in \mathbb{R}$, let alone $n + 1$ values!). Thus we get

$$p(x) = (2x - 1)(2x^3 + bx^2 + cx - 3).$$

Now to determine b and c , we can think about what the other coefficients are when we expand the brackets. The coefficient of x^3 is going to be $2b - 2$, and this should equal -4 , so $b = -1$. Similarly the coefficient of x will be $-c - 6$, and this should equal -12 , so $c = 6$. Therefore

$$p(x) = (2x - 1)(2x^3 - x^2 + 6x - 3).$$

The remaining coefficient, that of x^2 , can be used to check that we've done things correctly. Indeed, this should equal $-b + 2c = 1 + 12 = 13$, which agrees with p .

Now we need to check if we can factorise $2x^3 - x^2 + 6x - 3$ further. Clearly if this has a rational root, then it would also be a root of p , so we would have found it in the initial stage where we computed all possible rational roots. So this definitely can't have any "new" factors, but it might have another factor of $(2x - 1)$, which corresponds to $x = 1/2$ having multiplicity 2. Indeed, if we plug in $x = 1/2$, we get that it equals zero again. Thus

$$2x^3 - x^2 + 6x - 3 = (2x - 1)(ax^2 + bx + c)$$

for some quadratic $ax^2 + bx + c$. Again we can reason about the first and last coefficients upon expansion to get that

$$2x^3 - x^2 + 6x - 3 = (2x - 1)(x^2 + bx + 3),$$

and for b , consider the coefficient of x^2 . Upon expansion of the RHS, this is $2b - 1$, and this should equal -1 , so we get that $b = 0$. It follows that

$$p(x) = (2x - 1)^2(x^2 + 3).$$

This quadratic factor is not zero when $x = 1/2$, so this root has multiplicity 2. Moreover, it has no real roots at all since its discriminant is -12 . Therefore the solutions of $p(x) = 0$ are $x = 1/2$ (twice).

Let's give another example.

Example 5.33. Say we want to solve $x^4 + 12x^2 + 2 = 6x^3 + 9x$. First we rearrange it into a question of finding zeros, namely, the zeros of

$$x^4 - 6x^3 + 12x^2 - 9x + 2.$$

The only possible rational roots are $x = \pm 1, \pm 2$ by the rational roots theorem (5.29). Indeed, if we try these, we get that $(x-1)$ and $(x-2)$ are both factors. Hence

$$x^4 - 6x^3 + 12x^2 - 9x + 2 = (x-1)(x-2)(x^2 + bx + 1)$$

where the constant and leading term of the remaining factor were determined by thinking about expansion, as in the last example. Finally for b , notice that the coefficient of x^3 will be $b-1-2$ upon expansion, which should equal -6 , so $b = -3$. Thus the equation becomes

$$\begin{aligned} (x-1)(x-2)(x^2 - 3x + 1) &= 0 \\ \implies x = 1 \quad \text{or} \quad x = 2 \quad \text{or} \quad x^2 - 3x + 1 &= 0. \end{aligned}$$

Solving this remaining quadratic by completing the square, we get that the solutions of the equation are $x = 1, 2, \frac{1}{2}(3 \pm \sqrt{5})$.

Exercise 5.34. 1. The polynomial $ax^3 - x^2 + bx - 6$ leaves a remainder of 54 when divided by $(x-4)$, whereas $(x-3)$ is a factor of the expression. Determine the values of a and b , and hence; by comparing coefficients or otherwise, express the given expression as a product of three linear factors.

2. Solve the following equations by factorising.

- a) $x^3 - 4x^2 + 10 = 3x - 8$ b) $3x^3 - 10x^2 - 71x = 42$
- c) $0 = 6 + 7x - 9x^2 + 2x^3$ d) $x^3 - 2x^2 - 36x + 7 = 0$
- e) $x^2(x^2 + 6x + 7) = 6x + 8$ f) $x^4 + 16 = 8x^2$
- g) $24x^3 + 26x^2 + 9x + 1 = 0$ h) $x^3 - 6x^2 + 10x = 3$
- i) $x^3 + 3a = ax^2 + 3x$

3. Let $p \in \mathbb{R}[x]$ be defined by

$$p(x) = 3x^4 - 26x^3 + 39x^2 + 4x - 4.$$

- a) Determine all the rational roots of p .
- b) Find the remaining roots of p *without* performing long division.
- c) What is the remainder when dividing p by $(x-3)$?

4. Solve the following cubic equations.

a) $2x^3 - 15x^2 + 22x + 15 = 0$ b) $3x^3 - 5x^2 + x + 1 = 0$

c) $2x^3 + 7 = x(11x + 9)$ d) $2x^3 - 11x^2 + 19x - 7 = 0$

5. Suppose $x = 3/5$ is a root of the polynomial $a_n x^n + \cdots + a_0$ where $a_0, \dots, a_n \in \mathbb{Z}$. Prove, *without using the rational roots theorem*, that $3 \mid a_0$ and that $5 \mid a_n$.

6. In this question, we will extend the theory of Viète's formulæ (theorem 3.18) to cubics. Suppose a cubic

$$p(x) = ax^3 + bx^2 + cx + d$$

has roots $\alpha, \beta, \gamma \in \mathbb{R}$.

a) Show that $p(x) = a(x - \alpha)(x - \beta)(x - \gamma)$.

b) Let $\Sigma = \alpha + \beta + \gamma$, $\Pi = \alpha\beta\gamma$ and $\Xi = \alpha\beta + \beta\gamma + \gamma\alpha$. Show that

$$p(x) = a(x^3 - \Sigma x^2 + \Xi x - \Pi).$$

c) Show that

$$\alpha^2 + \beta^2 + \gamma^2 = \Sigma^2 - 2\Xi$$

and that

$$\frac{1}{\alpha^2} + \frac{1}{\beta^2} + \frac{1}{\gamma^2} = \frac{\Xi^2 - 2\Sigma\Pi}{\Pi^2}.$$

Hence, given that the cubic $3x^3 - 5x + 1$ has roots α, β, γ , determine a cubic with roots $\alpha/\beta\gamma$, $\beta/\alpha\gamma$ and $\gamma/\alpha\beta$.

7. a) By considering the polynomial $x^2 - 2$, use the rational roots theorem to deduce that it has no rational roots. Conclude that $\sqrt{2}$ is irrational.
- b) Construct a polynomial which has $\sqrt{2 + \sqrt{3}}$ as a root. Use the rational roots theorem similarly to part (a) to conclude that it is irrational.
- c) Construct a quadratic polynomial which has $\sqrt{4 + 2\sqrt{3}} - \sqrt{3}$ as a root. Deduce that it is rational, and write it in the form a/b with $a, b \in \mathbb{Z}$.

5.3 Partial Fractions

It is simple to verify that, for example,

$$\frac{2}{x+1} - \frac{1}{x-2} = \frac{x-5}{(x+1)(x-2)}.$$

But can we somehow reverse this process? In other words, given

$$\frac{x-5}{(x+1)(x-2)},$$

can we decompose it as a sum of two rational functions over each linear denominator? First of all, observe that this is a proper rational function, and that its decomposition is a sum of proper rational functions. Indeed, if p_1, q_1, p_2, q_2 are polynomials with $\deg(p_1) < \deg(q_1)$ and $\deg(p_2) < \deg(q_2)$, then

$$\frac{p_1}{q_1} + \frac{p_2}{q_2} = \frac{p_1 q_2 + p_2 q_1}{q_1 q_2}$$

is necessarily proper, since

$$\begin{aligned} \deg(p_1 q_2 + p_2 q_1) &\leq \max\{\deg(p_1 q_2), \deg(p_2 q_1)\} \\ &= \max\{\deg(p_1) + \deg(q_2), \deg(p_2) + \deg(q_1)\} \\ &< \max\{\deg(q_1) + \deg(q_2), \deg(q_2) + \deg(q_1)\} \\ &= \deg(q_1) + \deg(q_2) = \deg(q_1 q_2), \end{aligned}$$

where $\max\{a, b\}$ denotes the larger number of a and b .

But why would it be desirable to reverse this process? In later chapters, we are going to be performing operations on rational functions which are *additive*. An operation O is additive if

$$O(f + g) = O(f) + O(g).$$

Therefore, if we can decompose a rational function p/q into a sum of simpler rational functions $p_1/q_1 + \cdots + p_n/q_n$, it might turn out to be simpler to work out $O(p_1/q_1), \dots, O(p_n/q_n)$ separately and add them up, rather than to compute $O(p/q)$ directly. These will be the same if O is additive. (For those who are curious, additive operations include limits, summation, differentiation and integration). For now we will not worry about the applications, but suffice to say that what we are doing will actually prove useful!

First we will consider rational functions of the form

$$\frac{f}{p_1 \cdots p_n}$$

where each p_i is linear (i.e., $\deg(p_i) = 1$ for $1 \leq i \leq n$), $\deg(f) < n$, so that the rational function proper, and they are *all distinct*, i.e., $p_i \neq p_j$ for $i \neq j$. Indeed, write each $p_i(x) = a_i x + b_i$, so we have

$$\frac{f(x)}{(a_1 x + b_1) \cdots (a_n x + b_n)}.$$

Now we might have that some $(a_1 x + b_1)$ and $(a_2 x + b_2)$ are distinct, but still scalar multiples of each other (e.g. $(x + 1)$ and $(2x + 2)$). We do not want to count these as “distinct” for our purposes, since we can factor out the multiple of 2 and get two $(x + 1)$ ’s. So rather than $p_i \neq p_j$, we shall say that $\text{hcf}(p_i, p_j) = 1$ for $i \neq j$. (Make sure you understand why this captures what we want.)

Then we have the following.

Theorem 5.35 (Heaviside’s cover-up method). *Let $f \in \mathbb{R}[x]$ with $\deg(f) < n$, and let $(a_1 x + b_1), \dots, (a_n x + b_n) \in \mathbb{R}[x]$ with $\text{hcf}(a_i x + b_i, a_j x + b_j) = 1$ for $i \neq j$. For each $1 \leq i \leq n$, let*

$$f_i(x) = \frac{f(x)}{(a_1 x + b_1) \cdots (a_{i-1} x + b_{i-1})(a_{i+1} x + b_{i+1}) \cdots (a_n x + b_n)},$$

i.e., $f_i(x)$ is the rational function excluding the bracket $(a_i x + b_i)$ from the denominator. Then

$$\frac{f(x)}{(a_1 x + b_1) \cdots (a_n x + b_n)} = \frac{f_1(-b_1/a_1)}{a_1 x + b_1} + \cdots + \frac{f_n(-b_n/a_n)}{a_n x + b_n}.$$

Before we prove the result, let us give an example to make sure we understand what it’s saying. Indeed, take the example we started with,

$$\frac{x - 5}{(x + 1)(x - 2)}.$$

We want to express this as

$$\frac{x - 5}{(x + 1)(x - 2)} = \frac{A}{x + 1} + \frac{B}{x - 2},$$

where A and B are constants (since the corresponding fractions must be proper). Now theorem tells us that f_i is the rational function on the LHS with the i th bracket removed (or “covered up”), i.e., in our case,

$$f_1(x) = \frac{x - 5}{\boxed{(x + 1)}(x - 2)} = \frac{x - 5}{x - 2} \quad \text{and} \quad f_2(x) = \frac{x - 5}{(x + 1)\boxed{(x - 2)}} = \frac{x - 5}{x + 1},$$

and that the constant above the bracket $(a_i x + b_i)$ is $f_i(-b_i/a_i)$, in other words, f_i evaluated at the root of $a_i x + b_i$. So in our case, A is above $x + 1$, so we evaluate f_1 at -1 (which is the root of $x + 1$) to get

$$A = f_1(-1) = \frac{(-1) - 5}{(-1) - 2} = 2$$

and since B is above $x - 2$, we put 2 in f_2 to get

$$B = f_2(2) = \frac{(2) - 5}{(2) + 1} = -1,$$

which gives us our original decomposition

$$\frac{x - 5}{(x + 1)(x - 2)} = \frac{2}{x + 1} - \frac{1}{x - 2}.$$

Let's do one more example before we give the proof. Say we have

$$\frac{5(x^2 - 4)}{(x + 3)(2x + 1)(3x + 4)}.$$

First we observe that this is indeed proper, otherwise the theorem doesn't apply. Thus by the theorem, we know that there exists a way to write

$$\frac{5(x^2 - 4)}{(x + 3)(2x + 1)(3x + 4)} = \frac{A}{x + 3} + \frac{B}{2x + 1} + \frac{C}{3x + 4}$$

where A, B, C are polynomials of degree zero, i.e., constants. Now to find A , we "cover-up" its corresponding bracket, and evaluate the function at the root of $x + 3$, i.e., $x = -3$:

$$A = \frac{5(x^2 - 4)}{\cancel{(x + 3)}(2x + 1)(3x + 4)} \Big|_{x=-3} = \frac{5((-3)^2 - 4)}{(2(-3) + 1)(3(-3) + 4)} = 1,$$

similarly for B we cover up $(2x + 1)$ and plug in its root, $x = -1/2$:

$$B = \frac{5(x^2 - 4)}{(x + 3)\cancel{(2x + 1)}(3x + 4)} \Big|_{x=-1/2} = \frac{5((-1/2)^2 - 4)}{(-1/2 + 3)(3(-1/2) + 4)} = -3,$$

and finally for C we cover up $(3x + 4)$ and put $x = -4/3$:

$$C = \frac{5(x^2 - 4)}{(x + 3)(2x + 1)\cancel{(3x + 4)}} \Big|_{x=-4/3} = \frac{5((-4/3)^2 - 4)}{(-4/3 + 3)(2(-1/2) + 1)} = 4,$$

which gives us the desired decomposition

$$\frac{5(x^2 - 4)}{(x + 3)(2x + 1)(3x + 4)} = \frac{1}{x + 3} - \frac{3}{2x + 1} + \frac{4}{3x + 4},$$

which can be verified by combining the RHS back into a single rational function.

Now let's prove the theorem to see *why* it works.

Proof of Theorem 5.35. First of all, notice that by [theorem 5.20](#), if we have a product of linear factors $q = (a_1x + b_1) \cdots (a_nx + b_n)$, such that each pair of distinct factors have $\text{hcf}(a_ix + b_i, a_jx + b_j) = 1$, then there exist $s, t \in \mathbb{R}[x]$ such that $s(x)(a_1x + b_1) + t(x)(a_2x + b_2) \cdots (a_nx + b_n) = 1$, where $\deg(s) < n - 1$ and $\deg(t) = 0$ (i.e., t is some constant A_1). Thus

$$\begin{aligned} \frac{f}{q} &= \frac{f(x)(s(x)(a_1x + b_1) + A_1(a_2x + b_2) \cdots (a_nx + b_n))}{(a_1x + b_1) \cdots (a_nx + b_n)} \\ &= \frac{A_1}{a_1x + b_1} + \frac{s(x)}{(a_2x + b_2) \cdots (a_nx + b_n)}. \end{aligned}$$

Applying this procedure on the remaining term with non-linear denominator, and repeating until all denominators are linear, we establish the existence of a way to write

$$\frac{f}{q} = \frac{A_1}{a_1x + b_1} + \cdots + \frac{A_n}{a_nx + b_n}$$

where each A_i ($1 \leq i \leq n$) is constant. Now all we have to show is that each $A_i = f_i(-b_i/a_i)$. Indeed, if we multiply the above by $(a_1x + b_1)$, then we get

$$f_1(x) = A_1 + \frac{A_2(a_1x + b_1)}{a_2x + b_2} + \cdots + \frac{A_n(a_1x + b_1)}{a_nx + b_n},$$

and putting $x = -b_1/a_1$, we get

$$f_1(-b_1/a_1) = A_1 + 0 + \cdots + 0,$$

and notice that none of the denominators vanish since they cannot have the same roots (because $\text{hcf} = 1$.) This shows that $A_1 = f_1(-b_1/a_1)$, which can be easily adapted for the other i . \square

Now, before we discuss more general rational functions, let us discuss another (perhaps more intuitive) method to determine the constants A_i . We need the following proposition first.

Proposition 5.36. *Let $f, g, q \in \mathbb{R}[x]$ with $\text{hcf}\{f, q\} = \text{hcf}\{g, q\} = 1$ and $\deg(f) = \deg(g) = n$, and suppose the rational functions f/q and g/q agree on $n + 1$ values. Then $f = g$.*

Proof. We have $(f/q)(x) = (g/q)(x)$ if and only if $f(x) = g(x)$ and $q(x) \neq 0$. Now apply [proposition 5.31](#). \square

The idea for this more general method is simple, it's basically comparing coefficients in the numerator. Let's treat the first example again. We want to express

$$\frac{x-5}{(x+1)(x-2)} = \frac{A}{x+1} + \frac{B}{x-2}.$$

So why not manipulate the RHS to resemble the LHS as much as possible? Indeed,

$$\frac{A}{x+1} + \frac{B}{x-2} = \frac{A(x-2) + B(x+1)}{(x+1)(x-2)} = \frac{(A+B)x + (B-2A)}{(x+1)(x-2)},$$

and so we want A and B so that

$$\frac{x-5}{(x+1)(x-2)} = \frac{(A+B)x + (B-2A)}{(x+1)(x-2)}.$$

Now we want this equality to hold for *all* real values of x (apart from the cases where we're dividing by zero), so [proposition 5.36](#) trivially applies. Thus it's clear that the polynomials in the numerator are equal, that is, their coefficients are equal:

$$\begin{cases} x^1 : 1 = A + B \\ x^0 : -5 = B - 2A \end{cases}$$

and indeed, solving this set of equations simultaneously gives $A = 2$ and $B = -1$. Comparing coefficients is not as quick as Heaviside's cover-up method, but it is perhaps a more natural method to come up with. In the cases where Heaviside's method applies, you are encouraged to use it. But this method applies to a wider range of rational functions. Let's take a new example,

$$\frac{2x^2}{(1-x)(x^2+1)}.$$

(TO BE CONTINUED...)

6 The Binomial Theorem

6.1 The Binomial Theorem

6.2 Pascal's Triangle and Recursion

Appendices

A Naïve Set Theory

We start with the notion of a *set*. Informally, a set is a *collection of distinct “objects”*. In particular, the defining characteristic of a set is the idea of *membership*—an object x is either a member of a set S , or not. We write $x \in S$ for “ x is an element of the set S ” (or x is in S), and similarly $y \notin S$ for the negation “ y is not an element of S ”. Sets may be defined by listing their elements between curly brackets, e.g.

$$A = \{1, 2, 3, 4, 5\}$$

defines the set A whose elements are 1, 2, 3, 4 and 5. We have $1 \in A$, but $0 \notin A$ (for example). It is conventional to use capital letters for sets.

Notice that our definition of a set is an imprecise one: we do not clearly state what counts as an “object” in a set, nor which sets we are explicitly allowed to construct; we simply define sets by describing their elements verbally. Can sets contain other sets? Are we allowed to define strange sets such as “the set of all sets which are not members of themselves”? This vagueness leads to fundamental problems in mathematics and philosophy—but we will not concern ourselves with these issues here.⁷

Some of the important sets which we encounter are:

- The **empty set**, denoted by the symbol \emptyset , is the set such that

$$x \notin \emptyset \text{ for all } x.$$

- The set of **natural numbers**, denoted by the symbol \mathbb{N} , is the infinite set containing all positive whole numbers:

$$\mathbb{N} = \{1, 2, 3, 4, \dots\}.$$

- The set of **integers**, denoted by the symbol \mathbb{Z} (for the German *zählen*, meaning *counting*), is the infinite set containing the positive whole numbers, the negative whole numbers and zero:

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

⁷The interested reader is encouraged to look up the graphic novel *Logicomix* to get an idea of the historical significance of these problems, or, to get stuck in to formal (i.e., non-naïve) set theory itself, take a look at the textbook *Introduction to Set Theory* by Hrbáček and Jech or this free pdf textbook: https://www.math.uwaterloo.ca/~randre/1aaset_theory_140613.pdf.

- The set of **rational numbers**, denoted by the symbol \mathbb{Q} (for *quotient*), is the set of all numbers which can be expressed as a ratio of two integers. For example, this set contains the numbers $\frac{1}{2}$, $\frac{22}{7}$, $-\frac{1}{3}$, 0 and 5.
- The set of **real numbers**, denoted by the symbol \mathbb{R} , contains all the rational numbers, together with all the numbers which have infinite decimal expansions. Some of these are rational (e.g. $\frac{1}{3} = 0.333\dots$ and $\frac{1}{7} = 0.142857142\dots$), but others are *irrational*, that is, not rational (e.g. $\sqrt{2} = 1.41421\dots$, $\pi = 3.14159\dots$ and $e = 2.7182818\dots$).

It is not easy to see that some numbers are irrational. The easiest number to prove is irrational is $\sqrt{2}$, and a proof is provided in the following pages.

Optional Reading: The Irrationality of $\sqrt{2}$

It is not easy to convince students that there are irrational numbers. The ancient Greeks, in particular, the Pythagoreans, believed that numbers were either *whole* (that is, integers) or *parts of a whole* (that is, rationals). Pythagoras is famous for his theorem relating the lengths of sides in a right-angled triangle,^a and perhaps the simplest case we can consider is when the legs of the right-angled triangle are both equal to 1.

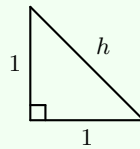


FIGURE 2: Right-angled triangle with legs of unit length

By Pythagoras' theorem, we get that the hypotenuse h must satisfy $h^2 = 1^2 + 1^2$, from which one easily obtains $h = \sqrt{2}$. Naturally, since numbers are either whole or parts of a whole, there must be a way to express

$$\sqrt{2} = \frac{a}{b}$$

for some integers $a, b \in \mathbb{Z}$, right? That's what the Pythagoreans believed.

Let us prove that this is impossible. (If you wish, you can watch a YouTube version of this proof here: <https://youtu.be/LmpAntNjPj0>.) We will do this by contradiction; that is, we will assume that there *exist* integers a and b such that $\sqrt{2} = \frac{a}{b}$, and show that this assumption leads us to an absurd conclusion. Before we proceed with the proof, we need to make two easy observations. An *even*

number is an integer which is divisible by 2, that is, a number of the form $2n$ for some $n \in \mathbb{Z}$, whereas an *odd number* is an integer which has the form $2n + 1$ for some $n \in \mathbb{Z}$. Indeed, 6 is even because $6 = 2(3)$, and -7 is odd because $-7 = 2(-4) + 1$.

Lemma A.1. *Suppose $n \in \mathbb{Z}$. Then n is either odd or even.*

Proof. This seems obvious—but it requires proof: we must show that any $n \in \mathbb{Z}$ can be written either as $2k$ or $2k + 1$ for some other integer k . To prove this, we will use a neat trick which mathematicians use all the time: we will consider a *minimal counterexample*. Indeed, suppose there exists some integer $n \geq 0$ which is neither even nor odd (we aim to conclude that there is no such n), and suppose that n is the smallest such integer. Since n is the smallest integer with this property, then $n - 1$ must be even or odd (otherwise $n - 1$ would be the smallest). But if $n - 1$ is even; i.e., $n - 1 = 2k$ for some k , then we get that $n = 2k + 1$, i.e., that n is odd, contradicting our assumption. Thus the alternative must be true; that is, $n - 1$ must be odd, i.e., $n - 1 = 2k + 1$ for some k . But this gives $n = 2k + 2 = 2(k + 1)$, which means that n is even, also contradicting the assumption. Therefore there is no smallest $n \geq 0$ with this property, and therefore all integers $n \geq 0$ are odd or even. We can identically prove this for negative values by considering a *largest counterexample* and working with $n + 1$, and thus we have that all integers are either odd or even. \square

Lemma A.2. *Suppose $n \in \mathbb{Z}$. If n^2 is even, then n is even.*

Proof. This is the same as saying that if n is not even, then n^2 is not even (contrapositive^b), and since n is either odd or even by the previous lemma, this is therefore equivalent to showing that if n is odd, then n^2 is odd.

Indeed, if n is odd, then $n = 2k + 1$ for some $k \in \mathbb{Z}$, which means that

$$\begin{aligned}
 n^2 &= (2k + 1)^2 = (2k + 1)(2k + 1) \\
 &= t(2k + 1) && \text{(where } t = 2k + 1\text{)} \\
 &= 2kt + t \\
 &= 2k(2k + 1) + 2k + 1 \\
 &= 4k^2 + 2k + 2k + 1 \\
 &= 4k^2 + 4k + 1 \\
 &= 2(2k^2 + 2k) + 1 \\
 &= 2m + 1, && \text{(where } m = 2k^2 + 2k\text{)}
 \end{aligned}$$

and thus n^2 is odd since it is of the required form. \square

Now we are ready to prove that $\sqrt{2}$ is irrational. Indeed, suppose there exist two integers a and b such that $\frac{a}{b} = \sqrt{2}$. We can also assume that a and b share no common divisors, since if they did, we can cancel them out.^c

By definition of $\sqrt{}$, if $\sqrt{2} = a/b$, then

$$\sqrt{2} = \frac{a}{b} \implies 2 = \left(\frac{a}{b}\right)^2 \implies 2 = \frac{a^2}{b^2} \implies a^2 = 2b^2.$$

In particular, this means that a^2 is even, which by [lemma A.2](#), means a is even. But since a is even, then $a = 2n$ for some $n \in \mathbb{Z}$, which means

$$a^2 = 2b^2 \implies (2n)^2 = 2b^2 \implies 4n^2 = 2b^2 \implies 2n^2 = b^2.$$

This similarly gives us that b^2 is even, which again by [lemma A.2](#) means that b is also even. Therefore a and b are both divisible by 2. But we chose a and b so that they have no common divisors! This must mean that our assumption was incorrect, that is, the assumption that “there exist integers a and b with no common divisors such that $\sqrt{2} = a/b$ ”, is incorrect. It follows that $\sqrt{2}$ is irrational, which concludes the proof.

It is said that one of the disciples of Pythagoras, *Hippasos of Metapontion*, presented an argument to Pythagoras that $\sqrt{2}$ is irrational. He was so outraged by this proof that he had Hippasos killed by throwing him to the sea!

Thus we have proved that there is at least one $x \in \mathbb{R}$ where $x \notin \mathbb{Q}$.

^aAlthough there is evidence which suggests that the theorem was known to the Babylonians before Pythagoras.

^bThe *contrapositive* of a statement “If P then Q ” is “If not Q then not P ”. The two statements are logically equivalent, that is, if one is true, so is the other. For example, “If it is raining, then the grass gets wet” is equivalent to “If the grass does not get wet, then it is not raining”. Note that this is not the same as “If it is not raining, the grass does not get wet”, which is not necessarily true!

^cFor example, $\frac{4}{6}$ can be written as $\frac{2}{3}$, since 4 and 6 have 2 as a common divisor, where as 2 and 3 now share no divisors.

Notice that each of the sets we defined (\emptyset , \mathbb{N} , \mathbb{Z} , \mathbb{Q} , \mathbb{R}) contains all the elements of the previous one. When a set B contains all the elements of A , or more formally, if

$$\text{For all } x, \text{ if } x \in A \text{ then } x \in B,$$

we say A is a *subset* of B and write $A \subseteq B$. For example, if $A = \{1, 2, 3\}$, $B = \{1, 2, 3, 4\}$, then $A \subseteq B$. Note that by this definition, every set S is a subset of itself. Also note that it is not necessarily the case that a set is a subset of the other; for example if $C = \{2, 4, 6, 8\}$, we neither have $A \subseteq C$ nor $C \subseteq A$.⁸

⁸Unlike the similar looking relation “ \leq ” for real numbers, where it *must* be the case that $x \leq y$ or $y \leq x$. Because of this, \subseteq is called a *partial order*, and \leq is called a *total order*.

If A contains every element of B , and B contains every element of A , that is, if both $A \subseteq B$ and $B \subseteq A$, we say that A is *equal to* B , written $A = B$. Observe that

$$\emptyset \subseteq \mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$$

but none of these are equal. In particular, by proving that $\sqrt{2} \in \mathbb{R}$ but $\sqrt{2} \notin \mathbb{Q}$, we showed that $\mathbb{Q} \neq \mathbb{R}$.

Notation. An important group of notations we introduce are the subsets of real numbers called the **real intervals**:

- $[a, b]$ is the set of $x \in \mathbb{R}$ such that $a \leq x \leq b$
- $[a, b)$ or $[a, b[$ is the set of $x \in \mathbb{R}$ such that $a \leq x < b$
- $(a, b]$ or $]a, b]$ is the set of $x \in \mathbb{R}$ such that $a < x \leq b$
- (a, b) or $]a, b[$ is the set of $x \in \mathbb{R}$ such that $a < x < b$
- $[a, \infty)$ or $[a, \infty[$ is the set of $x \in \mathbb{R}$ such that $a \leq x$
- (a, ∞) or $]a, \infty[$ is the set of $x \in \mathbb{R}$ such that $a < x$
- $(-\infty, b]$ or $] - \infty, b]$ is the set of $x \in \mathbb{R}$ such that $x \leq b$
- $(-\infty, b)$ or $] - \infty, b[$ is the set of $x \in \mathbb{R}$ such that $x < b$

So for example, if x is a real number such that $1 \leq x \leq 2$, then $x \in [1, 2]$. If moreover, $x \neq 2$, then $x \in [1, 2)$. If y is a positive real number, then $y \in (0, \infty)$, whereas if y is a non-negative real number, then $y \in [0, \infty)$.

Exercise A.3. 1. Consider the sets $A = \{1, 2, 3\}$, $B = \{2, 4, 6, 8\}$, $C = \{-1, 0, 1\}$ and $D = \{\sqrt{2}, e, \pi\}$. For each of the following, say whether they are true and false.

- | | | |
|--------------------------------|-------------------------------------|------------------------------------|
| a) $1 \in A$ | b) $\{1, 2\} \in A$ | c) $4 \notin A$ |
| d) $A \subseteq B$ | e) $A = C$ | f) $C \subseteq C$ |
| g) $D \subseteq \mathbb{Q}$ | h) $C \subseteq \mathbb{Z}$ | i) $\sqrt{2} \subseteq \mathbb{R}$ |
| j) $[-1, 2] \subseteq [-2, 2)$ | k) $(-3, 3) \subseteq [-3, \infty)$ | |

2. (*Optional*) Adapt the proof that $\sqrt{2}$ is irrational to prove that $\sqrt{3}$ is irrational. Why would the proof fail if one tries to show $\sqrt{4}$ is irrational?

Notation (Set Comprehension). Here we introduce an alternative notation to describe sets, instead of explicitly listing their elements. Suppose we want to describe the set of even numbers, E . Since there are infinitely many, in our current notation, we are forced to use ellipses (...) and let the reader deduce what the set contains:

$$E = \{\dots, -4, -2, 0, 2, 4, \dots\}.$$

There is a level of ambiguity with this notation however. Alternatively, using set comprehension, we write this as

$$E = \{2n : n \in \mathbb{Z}\},$$

where the colon is read “*such that*”. The whole expression is read as “ E = the set of all things of the form $2n$, such that $n \in \mathbb{Z}$ ”; in other words, E is the set of even numbers. In general, the notation

$$X = \{x : \Phi(x)\}$$

defines the set of all things “ x ” which satisfy the sentence Φ . Sometimes, we would like to take our elements from a larger set. For example, the set of prime numbers can be written as

$$P = \{n \in \mathbb{N} : n \text{ is prime}\}$$

or as

$$P = \{n : n \in \mathbb{N} \text{ and } n \text{ is prime}\}.$$

In general, there are many ways to express the same set using comprehension.

Examples A.4. We give some examples of set comprehension.

$$\begin{aligned} \{n^2 : n \in \mathbb{N}\} &= \{1, 4, 9, 16, \dots\} \\ \{5n : n \in \mathbb{Z}\} &= \{\dots, -5, 0, 5, 10, \dots\} \\ \{x \in \mathbb{R} : 1 \leq x \leq 2\} &= [1, 2] \\ \{x \in \mathbb{Q} : x + 2 = 1\} &= \{-1\} \\ \{x \in \mathbb{N} : x + 2 = 1\} &= \emptyset \\ \{2x : x \in \mathbb{R}\} &= \mathbb{R} \\ \{x \in \mathbb{R} : x > 0\} &= (0, \infty) \\ \{a/b : a, b \in \mathbb{Z} \text{ and } b \neq 0\} &= \mathbb{Q} \end{aligned}$$

Exercise A.5. 1. Express these sets by listing their elements between curly brackets. For example, $\{2x + 6y : x, y \in \mathbb{N}\}$ can be written as $\{0, 2, 4, 6, 8, \dots\}$.

- | | |
|--|--|
| a) $\{4n + 1 : n \in \mathbb{Z}\}$ | b) $\{7n - 2 : n \in \mathbb{Z}\}$ |
| c) $\{n^2 : n \in \mathbb{Z}\}$ | d) $\{n \in \mathbb{Z} : -5 < n \leq 5\}$ |
| e) $\{n \in \mathbb{N} : -5 \leq n < 5\}$ | f) $\{x \in \mathbb{R} : x^2 = 5\}$ |
| g) $\{x \in \mathbb{Z} : x^2 = 3\}$ | h) $\{x \in \mathbb{R} : x^2 = 3 \text{ or } x^2 = 4\}$ |
| i) $\{q \in \mathbb{Q} : q = \frac{1}{n} \text{ or } n \in \mathbb{N}\}$ | j) $\{(a, b) : a \in \mathbb{N} \text{ and } b \in \mathbb{Z}\}$ |
| k) $\{5a + 2b : a, b \in \mathbb{Z}\}$ | l) $\{\{a, b\} : a \in \mathbb{N} \text{ and } b \in \{0, 1\}\}$ |

2. Write each of the following sets using set comprehension notation.

- | | |
|--|--|
| a) $\{10, 11, 12, 13, 14, 15, 16\}$ | b) $\{3, 5, 7, 9, 11, 13\}$ |
| c) $\{2, 4, 8, 16, 32, 64, \dots\}$ | d) $\{1, 9, 25, 49, 81, 121, \dots\}$ |
| e) $\{\dots, -14, -7, 0, 7, 14, \dots\}$ | f) $\{\dots, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, \dots\}$ |
| g) $\{\dots, -1, 3, 7, 11, 15, \dots\}$ | h) $\{\emptyset, \{1\}, \{1, 2\}, \{1, 2, 3\}, \dots\}$ |
| i) $\{\dots, -\frac{2\pi}{3}, -\frac{\pi}{3}, 0, \frac{\pi}{3}, \frac{2\pi}{3}, \dots\}$ | j) $\{1, 2, 3, 5, 6, 7, 9, 10, 11, \dots\}$ |
| \cup k) $\{1, 1.1, 1.11, 1.111, \dots\}$ | \cup l) $\{3, \{3\}, \{\{3\}\}, \{\{\{3\}\}\}, \dots\}$ |
| \cup m) $\{\emptyset, \{(1, 1)\}, \{(1, 1), (1, 2), (2, 1), (2, 2)\}, \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\}, \dots\}$ | |

Now, let us define some set operations, that is, ways to combine sets to create new sets.

Definitions A.6. Suppose A and B are two sets. Then

- (i) The *union* of A and B , denoted $A \cup B$, is the set defined by the property

$$\text{If } x \in A \text{ OR } x \in B, \text{ then } x \in A \cup B.$$

- (ii) The *intersection of A and B* , denoted $A \cap B$, is the set defined by the property

$$\text{If } x \in A \text{ AND } x \in B, \text{ then } x \in A \cap B.$$

- (iii) The *difference between A and B* , denoted $A \setminus B$, is the set defined by the property

$$\text{If } x \in A \text{ AND } x \notin B, \text{ then } x \in A \setminus B.$$

Examples A.7. If $A = \{1, 2, 3, 4, 5\}$, $B = \{2, 4, 6, 8, 10\}$ and $C = \{-1, 0, 1\}$, then

$$A \cup B = \{1, 2, 3, 4, 5, 6, 8, 10\}$$

$$A \cap B = \{2, 4\}$$

$$A \setminus B = \{1, 3, 5\}$$

$$(A \cup B) \cap C = \{1, 2, 3, 4, 5, 6, 8, 10\} \cap \{-1, 0, 1\} = \{1\}$$

$$A \cup (B \cap C) = \{1, 2, 3, 4, 5\} \cup \emptyset = \{1, 2, 3, 4, 5\} = A$$

The final operation we will introduce here is the Cartesian product $A \times B$ of two sets. We first need to define the idea of an *ordered pair*. First of all, for a finite set A , the number of elements of A is called its *cardinality*, denoted by $|A|$. For example, $|\{-1, 0, 1\}| = 3$.

An *unordered pair* is a set P such that $|P| = 2$. This makes sense of course, since if a set contains two elements, we call it a pair. Why unordered? Well, a set gives no sense of “order”, only membership. For example, $\{1, 2\} = \{2, 1\}$. How do we represent a pair of objects with an idea of which is the *first one*, and which is the *second one*? What we do is the following. We define the notation (a, b) to denote the set

$$(a, b) = \{\{a\}, \{a, b\}\},$$

and take this as our definition of an *ordered pair*. Why this way? Well, it satisfies the property we want it to satisfy, namely, $(a, b) = (c, d)$ if and only if $a = c$ and $b = d$. This is easy to prove by definition of set equality.

We can similarly define the ordered triple (a, b, c) by the pair $(a, (b, c))$, the ordered quadruple (a, b, c, d) by the pair $(a, (b, c, d))$, and so on. In general, we define an ordered k -tuple (a_1, a_2, \dots, a_k) by the pair $(a_1, (a_2, a_3, \dots, a_k))$.

Now we define our final operator.

Definition A.8 (Cartesian Product). Let A and B be two sets. The *Cartesian product of A and B* , denoted $A \times B$, is the set defined by the property

$$\text{If } a \in A \text{ AND } b \in B, \text{ then } (a, b) \in A \times B.$$

If $A = B$, then $A \times B = A \times A$ is denoted by A^2 .

Thus the set $A \times B$ consists of all the ordered pairs (a, b) such that $a \in A$ and $b \in B$. Note that we do not have $A \subseteq A \times B$ nor $B \subseteq A \times B$. Unlike the other operators, the Cartesian product does not contain any of the same objects as A and B themselves.

Example A.9. If $A = \{1, 2, 3, 4\}$ and $B = \{a, b, c\}$, then

$$A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c), \\ (3, a), (3, b), (3, c), (4, a), (4, b), (4, c)\}.$$

Example A.10. The set \mathbb{Q} consisting of all rational numbers can be identified with the set $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$, where the pair (p, q) is interpreted as p/q . There is not a one-to-one correspondence however, since many equivalent representations exist: the pairs $(1, 2)$, $(3, 6)$, $(-5, -10)$ each correspond to the rational number $1/2$.

Example A.11. The enormous set $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ consists of all pairs (x, y) of real numbers. We can identify each element of this set with a point in the xy -plane.

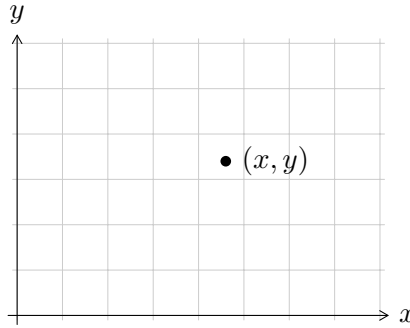


FIGURE 3: The point (x, y) in the plane.

Thus we consider the plane, in some sense, “equivalent” to the set \mathbb{R}^2 ; or rather, a way to visualise its points.

Exercise A.12. 1. Consider the sets $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$, $B = \{2, 4, 6, 8, 10, 12, 14\}$ and $C = \{2, 3, 6, 9\}$. Determine:

- | | | |
|------------------------|--|--------------------|
| a) $A \cup B$ | b) $A \cap B$ | c) $B \cup C$ |
| d) $A \setminus C$ | e) $B \cap C$ | f) $B \setminus A$ |
| g) $A \setminus B$ | h) $A \cap C$ | i) $C \setminus B$ |
| j) $C \cup (B \cap A)$ | k) $(A \setminus B) \cup (B \setminus C) \cup (C \setminus A)$ | |

2. Consider the sets $X = \{4, 7, 2, 1\}$, $Y = \{4, 6, 12, 7, 3\}$ and $Z = \{0, 1, 2\}$. Determine:

- | | |
|--|------------------------|
| a) $X \cup Y$ | b) $X \setminus Y$ |
| c) $(X \setminus Y) \cup (Y \setminus X)$ | d) $X \cap Y \cap Z$ |
| e) $X \cup (Y \cap Z)$ | f) $(X \cup Y) \cap Z$ |
| g) $X \setminus (Y \setminus (Z \setminus X))$ | h) Z^3 |

3. Let $A = \{1, 2, 3, 4\}$, $B = \{a, b\}$, $C = \{0, 1, 2\}$ and $D = \{-1, 1\}$. Find:

- | | |
|--------------------------|-------------------------------------|
| a) $A \times B$ | b) A^2 |
| c) $\emptyset \times B$ | d) $A \times B^2$ |
| e) $B \times A$ | f) B^2 |
| g) B^3 | h) $C \times D$ |
| i) $D \times \emptyset$ | j) $B \times C$ |
| k) $B \times C \times D$ | l) $(A \times C) \cap (C \times D)$ |

B Supplementary Proofs

In this appendix, we present proofs of results which are not essential to the material of the course, but are important if one wants to leave no stone unturned.

B.1 Proof of Corollary 3.14

Recall that [corollary 3.14](#) states the following.

Let $\phi(x) = ax^2 + bx + c$ be a quadratic, where $a, b, c \in \mathbb{Z}$, and let Δ be its discriminant. If $\Delta \in \{n^2 : n \in \mathbb{Z}\}$, then ϕ can be expressed in the form

$$\phi(x) = K(mx - s)(nx - t),$$

where $K, m, n, s, t \in \mathbb{Z}$ and $K, m, n \neq 0$.

Before we give the proof, we need some definitions and easy lemmata.

- Definitions B.1.** (i) Let $a, b \in \mathbb{Z}$. We say that a *divides* b , written $a \mid b$, if there exists $k \in \mathbb{Z}$ such that $b = ak$.
- (ii) Let $a, b \in \mathbb{Z}$. The *greatest common divisor* of a and b , denoted $\gcd\{a, b\}$, is the largest integer $k \in \mathbb{Z}$ such that $k \mid a$ and $k \mid b$.
- (iii) More generally for a finite set $A \subseteq \mathbb{Z}$, the *greatest common divisor* of A , denoted $\gcd A$, is the largest integer $k \in \mathbb{Z}$ such that $k \mid a$ for all $a \in A$.

Examples B.2. We have $\gcd\{15, 20\} = 5$, $\gcd\{24, 36, 90\} = 3$, $\gcd\{1, 25\} = 1$, $\gcd\{0, 23\} = 23$.

Lemma B.3. Let $A \subseteq \mathbb{Z}$ such that $1 \in A$. Then $\gcd A = 1$.

Proof. The largest integer a to divide 1, i.e., to satisfy $1 = ak$ for some $k \in \mathbb{Z}$, is $a = 1$. Thus if $1 \in A$, $\gcd A = 1$. \square

Lemma B.4. Let $a, b, m \in \mathbb{Z}$ and $m \neq 0$. Then

$$\gcd\{ma, mb\} = m \gcd\{a, b\}.$$

Proof. If $c = \gcd\{a, b\}$ and $d = \gcd\{ma, mb\}$, then

$$c \mid a \text{ and } c \mid b \implies mc \mid ma \text{ and } mc \mid mb \implies mc \mid d,$$

so $d = mck$ for some $k \in \mathbb{Z}$. Thus

$$mck \mid ma \text{ and } mck \mid mb \implies ck \mid a \text{ and } ck \mid b \implies ck \mid c \implies k \mid 1,$$

so $k = 1$ by the previous lemma, and therefore $d = mc$. \square

Now we prove the corollary.

Proof of Corollary 3.14. If $\Delta \in \{n^2 : n \in \mathbb{Z}\}$, then $\Delta = k^2$ for some $k \in \mathbb{Z}$, $k \geq 0$, so that $k = \sqrt{\Delta}$. By theorem 3.12, the roots α, β of ϕ are $\frac{-b \pm k}{2a}$.

Now we claim that $\phi(x)$ is equal to

$$\gcd\{a, b, c\} \left(\frac{2a}{\gcd\{-b-k, 2a\}}x - \frac{-b-k}{\gcd\{-b-k, 2a\}} \right) \left(\frac{2a}{\gcd\{-b+k, 2a\}}x - \frac{-b+k}{\gcd\{-b+k, 2a\}} \right).$$

Notice that the fact that the coefficients are all integers is obvious, because each denominator is a divisor of the numerator. Thus we simply need to show that this is in fact equal to $\phi(x)$, and the proof will be done. Indeed, upon expansion, the expression becomes

$$\frac{4a \gcd\{a, b, c\}}{\gcd\{-b-k, 2a\} \gcd\{-b+k, 2a\}} (ax^2 + bx + c),$$

thus all we need to show is that $\frac{4a \gcd\{a, b, c\}}{\gcd\{-b-k, 2a\} \gcd\{-b+k, 2a\}} = 1$. In fact, using theorem 3.18 and lemmata B.3 and B.4, we have

$$\begin{aligned} \frac{4a \gcd\{a, b, c\}}{\gcd\{-b-k, 2a\} \gcd\{-b+k, 2a\}} &= \frac{4a \gcd\{a, -a(\alpha + \beta), a\alpha\beta\}}{\gcd\{2a\alpha, 2a\} \gcd\{2a\beta, 2a\}} \\ &= \frac{4a^2 \gcd\{1, -(\alpha + \beta), \alpha\beta\}}{2a \gcd\{\alpha, 1\} 2a \gcd\{\beta, 1\}} \\ &= \frac{4a^2}{4a^2} = 1, \end{aligned}$$

as required. \square

C Answers to Exercises

1.1: Preliminary Techniques

1. a) 4 b) 4 c) 6 d) 6 e) 48 f) 12 g) 15 h) 40
 i) 1 j) 2 k) -10 l) $1/5$ m) 13 n) 2 o) $5/2$ p) 5
 q) 7

2. a) (3, 6) b) (2, 5) c) (4, 5) d) (5, 3) e) (7, 3) f) (4, 7)
 g) Alice has €146, Bob has €106 h) 45, 75

3. a) $x = y + 3z$ b) $x = \frac{3}{2+y+z-4yz}$
 c) $x = \frac{y+z^2}{y-3z-1}$ d) $x = \frac{wz}{w-z}$
 e) $x = \frac{wyz}{wy-wz-yz}$ f) $x = -\frac{z(1-y^2)}{y(1-z^2)}$

4. The man is looking at a picture of his son. (Think about it!)

5. Ask “*Are you James?*” since:

- John will say *yes*, because he lies,
- James will say *no*, since James lies,
- William will say *no*, since William tells the truth.

Thus a *yes* answer uniquely identifies John, and a *no* answer means that he is certainly not John.

Watch this video of the author of this puzzle explaining the solution to Johnny Carson (go to 6:15): youtu.be/E27v83WWiGo?t=376.

1.5: The Real Numbers

1. Since by distributivity ([theorem 1.2\(XI\)](#)), we have

$$x + x = x \cdot 1 + x \cdot 1 = x \cdot (1 + 1) = x \cdot 2 = 2 \cdot x = 2x.$$

2. A possible way (not the only way):

$$\begin{aligned} 2x + 1 &= 3 \\ \implies (2x + 1) + (-1) &= 3 + (-1) \end{aligned}$$

$$\begin{aligned}
&\implies 2x + (1 + -1) = 2 && \text{(by theorem 1.2(II))} \\
&\implies 2x + 0 = 2 && \text{(by theorem 1.2(IV))} \\
&\implies 2x = 2 && \text{(by theorem 1.2(III))} \\
&\implies \frac{1}{2} \cdot (2x) = \frac{1}{2} \cdot 2 \\
&\implies (\frac{1}{2} \cdot 2)x = 1 && \text{(by theorem 1.2(VII,IX))} \\
&\implies 1 \cdot x = 1 && \text{(by theorem 1.2(IX))} \\
&\implies x = 1 && \text{(by theorem 1.2(VIII)),}
\end{aligned}$$

and so $x = 1$.

3. Working similarly to the previous question, we should get $x = 4$. **Proposition 1.4** should prove useful here.
4. A possible way: denote $(a + b)$ by t for now. So applying **theorem 1.2**, what we have is

$$\begin{aligned}
t(c + d) &= tc + td \\
&= ct + dt \\
&= c(a + b) + d(a + b) \\
&= ca + cb + da + db \\
&= ac + bc + ad + bd,
\end{aligned}$$

as required. □

5. By **proposition 1.3**(ix) and **proposition 1.4**(iii),

$$\frac{-x}{y} = \frac{(-1) \cdot x}{1 \cdot y} = \frac{-1}{1} \cdot \frac{x}{y} = \left(-1 \cdot \frac{1}{1}\right) \cdot \frac{x}{y}.$$

But what is $\frac{1}{1}$? Well, since $1 \cdot 1 = 1$, it follows that $\frac{1}{1} = 1$ (i.e., 1 is the unique inverse of 1 in the sense of **theorem 1.2**(IX)). Thus

$$\left(-1 \cdot \frac{1}{1}\right) \cdot \frac{x}{y} = (-1 \cdot 1) \cdot \frac{x}{y} = -1 \cdot \frac{x}{y} = -\frac{x}{y}$$

by **proposition 1.3**(ix). □

The other equality $\frac{x}{y} = \frac{x}{-y}$ follows by applying a similar argument.

6. By **theorem 1.2**(XIV), $x \leq y$ or $y \leq x$ for any $x, y \in \mathbb{R}$. If we put $y = x$, we get that $x \leq x$ or $x \leq x$, i.e., that $x \leq x$.
7. For \geq , we have:

XII'. If $x \geq y$ and $y \geq x$, then $x = y$

XIII'. If $x \geq y$ and $y \geq z$, then $x \geq z$

XIV'. $x \geq y$ or $y \geq x$

XV'. If $x \geq y$, then $x + z \geq y + z$

XVI'. If $0 \geq x$ and $0 \geq y$, then $x \cdot y \geq 0$

Notice that the only substantially different one is XVI'. To prove, say, XII, we simply use the definition of \geq :

$$x \geq y \quad \text{and} \quad y \geq x \implies y \leq x \quad \text{and} \quad x \leq y \implies y = x,$$

by [theorem 1.2\(XII\)](#). Indeed, for XII'–XV', simply switching \geq to the corresponding \leq statement and applying [theorem 1.2](#) will complete the proof. But for XVI', a more subtle reasoning is needed.

If $0 \geq x$ and $0 \geq y$, we translate these to $x \leq 0$ and $y \leq 0$. Then by [theorem 1.2\(XV\)](#) we can get $x - x \leq 0 - x$ and $y - y \leq 0 - y$, i.e., $0 \leq -x$ and $0 \leq -y$. Finally by [theorem 1.2\(XVI\)](#), we get $0 \leq (-x) \cdot (-y) = x \cdot y$ by [proposition 1.3\(viii\)](#), in other words, $x \cdot y \geq 0$.

Next for $<$, the properties become:

XII". $x < y$ and $y < x$ is impossible

XIII". If $x < y$ and $y < z$, then $x < z$

XIV". $x < y$ or $y < x$ or $x = y$

XV". If $x < y$, then $x + z < y + z$

XVI". If $0 < x$ and $0 < y$, then $x \cdot y < 0$

To prove XII", we again translate into \leq :

$$\begin{aligned} & x < y \quad \text{and} \quad y < x \\ \implies & x \leq y \quad \text{and} \quad x \neq y \quad \text{and} \quad y \leq x \quad \text{and} \quad y \neq x. \end{aligned}$$

In particular, $x \leq y$ and $y \leq x$ imply that $x = y$ by [theorem 1.2\(XII\)](#)—but this contradicts that $x \neq y$.

For XIII", again we simply translate: having $x < y$ and $y < z$ means that $x \leq y$ and $x \neq y$ and $y \leq z$ and $y \neq z$. Consequently by [theorem 1.2\(XIII\)](#), we get that $x \leq z$. Now for $<$, we also need that

$x \neq z$. Can $x = z$? If $x = z$, then $x < y$ means that $z < y$. But we already have that $y < z$, and by XII', having both is impossible—therefore $x \neq z$, so we conclude that $x < z$.

For XIV'', we from [theorem 1.2](#)(XIV) that $x \leq y$ or $y \leq x$. Clearly we also have that either $x = y$ or $x \neq y$. Using some logic:

$$\begin{aligned}
 & (x = y \text{ or } x \neq y) \text{ and } (x \leq y \text{ or } y \leq x) \\
 \iff & [x = y \text{ and } (x \leq y \text{ or } y \leq x)] \text{ or } \\
 & [x \neq y \text{ and } (x \leq y \text{ or } y \leq x)] \\
 \iff & [x = y \text{ and true}] \text{ or } \\
 & [(x \neq y \text{ and } x \leq y) \text{ or } (x \neq y \text{ and } y \leq x)] \\
 \iff & x = y \text{ or } x < y \text{ or } y < x,
 \end{aligned}$$

as required.

Now for XV'', if $x < y$, then $x \leq y$ and $x \neq y$. Thus by [theorem 1.2](#)(XV), $x + z \leq y + z$ for any $z \in \mathbb{R}$. Now if $x + z = y + z$, we can do $x + z + (-z) = y + z + (-z)$, so that $x = y$. Consequently, since $x \neq y$, we have that $x + z \neq y + z$. Therefore $x + z < y + z$.

Finally for XVI'', if $0 < x$ and $0 < y$, we have that $0 \leq x$ and $0 \neq x$ and $0 \leq y$ and $0 \neq y$. We can use [theorem 1.2](#)(XVI) to give that $0 \leq x \cdot y$. But if $x \cdot y = 0$, then $x = 0$ or $y = 0$ (see [theorem 2.5](#) and the proof there.) Consequently, we have that $x \cdot y \neq 0$, so we can conclude that $x \cdot y < 0$.

For $>$, we can combine reasoning from the previous two to get

XII'''. $x > y$ and $y > x$ is impossible

XIII'''. If $x > y$ and $y > z$, then $x > z$

XIV'''. $x > y$ or $y > x$ or $x = y$

XV'''. If $x > y$, then $x + z > y + z$

XVI'''. If $0 > x$ and $0 > y$, then $x \cdot y < 0$

The proofs are nearly identical to those of XII''–XVI'', where XVI''' borrows the idea of “negative times negative make a positive” from XVI'.

But can this always be done, for any number of terms in the denominator? It's not immediately obvious, but the answer is *no*. Remember that the reason we multiply $(a + b)$ by $(a - b)$ is that the result is $a^2 - b^2$; if a and b are of the form $p\sqrt{q}$, then the result is an integer.

The analogue of what we did here is

$$(a + b + c)(a + b - c) = \underbrace{a^2 - b^2 - c^2}_{\text{integer}} - \underbrace{2bc}_{\text{maybe not}}$$

but at least the number of non-integral terms is at most one: so after we do this, we can go on to apply the usual method.

Similarly if we started off with a sum of four $p\sqrt{q}$'s:

$$(a + b + c + d)(a + b + c - d) = \underbrace{a^2 + b^2 + c^2 - d^2}_{\text{integer}} + \underbrace{2ab + 2ac + 2bc}_{\text{maybe not}},$$

we went from four to at most three; so we can apply the previous method.

But if we go on to five terms:

$$\begin{aligned} & (a + b + c + d + e)(a + b + c + d - e) \\ &= \underbrace{a^2 + b^2 + c^2 + d^2 - e^2}_{\text{integer}} + \underbrace{2ab + 2ac + 2ad + 2bc + 2bd + 2cd}_{\text{maybe not}} \end{aligned}$$

Here we had an increase! Indeed, the pattern of having less square rooted terms each time does not hold. There still is a pattern here though: it's closely related to the binomial theorem ([section 6](#)), and will be revisited there.

This means that if we try to do, say,

$$\frac{1}{\sqrt{2} + \sqrt{3} + \sqrt{5} + \sqrt{6} + \sqrt{7}},$$

multiplying by $\sqrt{2} + \sqrt{3} + \sqrt{5} + \sqrt{6} - \sqrt{7}$ will *increase* the number of square rooted terms:

$$\begin{aligned} & (\sqrt{2} + \sqrt{3} + \sqrt{5} + \sqrt{6} + \sqrt{7})(\sqrt{2} + \sqrt{3} + \sqrt{5} + \sqrt{6} - \sqrt{7}) \\ &= 9 + 6\sqrt{2} + 4\sqrt{3} + 2\sqrt{6} + 2\sqrt{10} + 2\sqrt{15} + 2\sqrt{30}. \end{aligned}$$

$$6. \ x = -\frac{1}{19}(9\sqrt{2} + 4\sqrt{3}).$$

2.25: Indices

1. a) 8 b) $1/16$ c) 1 d) 25
 e) $1/512$ f) $\sqrt{2}/4$ g) 3 h) 25
 i) $153^2 - 47^2 = (153 + 57)(153 - 47) = 200(106) = 21\,200$
 j) 256 k) $9/7$ l) 14 m) -2
 n) $\sqrt{2}/4$ o) $\sqrt[4]{30}$
2. a) Exactly as in the theorem, show that $\sqrt[3]{a}\sqrt[3]{b}$, when cubed, results in ab . Hence by uniqueness, this must equal $\sqrt[3]{ab}$.
 b) Break it up as $\sqrt[3]{b^3}\sqrt[3]{ac}$, just as in [theorem 2.8](#).
 c) You can simply use the laws of indices. For (a), $(ab)^{1/3} = a^{1/3}b^{1/3}$, and for (b), $(abbb)^{1/3} = (b^3)^{1/3}(ac)^{1/3} = b^1(ac)^{1/3}$.
3. If a/b and ka/kb are two representations of the same rational number, then $x^{a/b} = \sqrt[b]{x^a} = y > 0$ such that $y^b = x^a$ ([definition 2.20](#)). If we raise both sides of this equation to a power of k , we get $y^{kb} = x^{ka}$, so by [theorem 2.21](#) or [2.22](#), we get that $y = \sqrt[kb]{x^{ka}} = x^{ka/kb}$. Thus $x^{a/b} = x^{ka/kb}$. (Notice that it's important that $y > 0$ to ensure that we do not get ambiguities arising from [theorem 2.22](#), e.g., $(-2)^6 = 8^2$, but $-2 \neq \sqrt[6]{8^2}$.)
4. A “cube surd” would be a real number of the form

$$\sqrt[3]{p_1 \cdot p_2 \cdots p_n}$$

where each p_i is prime, but this time no *three* are equal; i.e., $p_i \neq p_j \neq p_k \neq p_i$ for $i \neq j \neq k \neq i$.⁹

Surd form would then be the same: if \mathbb{S}_3 denotes the set of cube surds, then a number is in “cube surd form” if it is written as a linear combination (over \mathbb{Q}) of $\mathbb{S}_3 \cup \{1\}$.

Just as the difference of two squares identity $(a+b)(a-b) = a^2 - b^2$ helped us get rid of square rooted terms in the denominator, the sum of two cubes identity $(a+b)(a^2 - ab + b^2) = a^3 + b^3$ can help us get rid of cube rooted terms. Indeed:

⁹Why do we need to repeat $\neq p_i$ and $\neq i$ at the end of each of these?

$$\frac{1}{\sqrt[3]{2} + \sqrt[3]{3}} \cdot \frac{(\sqrt[3]{2})^2 - \sqrt[3]{2}\sqrt[3]{3} + (\sqrt[3]{3})^2}{(\sqrt[3]{2})^2 - \sqrt[3]{2}\sqrt[3]{3} + (\sqrt[3]{3})^2} = \frac{\sqrt[3]{4} - \sqrt[3]{6} + \sqrt[3]{9}}{5},$$

which is in “cube surd form”.

3.7: Completing the Square

The idea expressed in [figure 1](#) is that the quantity $x^2 + bx$ corresponds to the sum of areas of a square with side length x , and rectangle with side lengths x and b . Splitting the rectangle in two and joining the sides of length x to two sides of the square, we *almost* get a square of area $(x + b/2)^2$. Thus if we add the small missing square with area $(b/2)^2$ and subtract it again, we get the same quantity $x^2 + bx$ expressed as $(x + b/2)^2 - (b/2)^2$.

3.10: Solving QE's

1. a) $x = -4, x = -3$ b) $x = -1, x = 4$ c) $x = -3, x = -2$
 d) $x = -5, x = 3$ e) $x = \pm 4$ f) $x = -2, x = 0$
 g) $x = \pm 1, x = \pm 5$ h) $x = 1$ i) $x = 1$
2. a) $x = -4, x = 12$ b) $x = -1 \pm \sqrt{43}$ c) $x = \frac{1}{5}(5 \pm \sqrt{130})$
 d) $x = \frac{1}{2}(7 \pm 3\sqrt{5})$ e) $x = -\frac{1}{2}(13 \pm \sqrt{109})$
 f) $x = \frac{1}{2}(9 \pm \sqrt{201})$ g) $x = -5, x = -1$ h) $x = -6, x = -\frac{11}{5}$
 i) $x = -4, x = -\frac{8}{3}$
3. 36 m^2
4. $7.29 \text{ m by } 10.29 \text{ m}$
5. $\frac{4}{41}(8 + \sqrt{365}) \approx 10 \text{ hours}$ (Hint: $\text{speed} = \frac{\text{distance}}{\text{time}}$)
6. Hint: write $ax^2 + bx + c$ as $a(x^2 + \frac{b}{a}x + \frac{c}{a})$.
7. a) $4 \times 5 = 20$ dots. Half of them will be black, so 10 black dots.
 b) $n(n+1)$ dots in the n th pattern, $\frac{n}{2}(n+1)$ are black.
 c) $\frac{n}{2}(n+1) = 4950$ gives $n = 99$
 d) $1 + 2 + 3 + 4 + 5 + 6 + 7$
 e) $\frac{1000}{2}(1000 + 1) = 500\,500$
8. $x = -\sqrt{2}$ or $x = -\sqrt{3}$.

3.21: QE Theory

1. a) non-real b) real & repeated c) real & distinct
 d) non-real e) real & distinct f) real & distinct
2. a) $k = \pm 1$
 b) $k = \frac{1}{12}$
 c) $k = 16$ (Note $k = 0$ is wrong since it gives $0 = 4$).
3. Hint: Show that for all $b \in \mathbb{R}$, $\Delta > 0$.
4. a) Hint: Show that $\Delta < 0$.
 b) Hint: Substitute $3 + 2i$ and then $3 - 2i$ for x in ϕ and simplify, replacing any occurring i^2 terms with -1 .
 c) Do the same as part (b), but in general.
5. a) Hint: Simplify the RHS
 b) Hint: Simplify the RHS
6. a) $4x^2 - 61x + 9 = 0$ b) $8x^2 + 469x - 27 = 0$
 c) $3x^2 - 14x - 8 = 0$ d) $9x^2 - 61x + 4 = 0$
 e) $8x^2 + 485x + 450 = 0$ f) $3x^2 - 13x + 8 = 0$
 g) $12x^2 - 469x - 18 = 0$ h) $49x^2 - 49x - 6 = 0$
 i) $4x^2 + 56x + 123 = 0$
7. $4x^2 + 2(2r - 3)x + 1 = 0$
8. $p = -6$
9. Hint: The roots are α and 2α (*no need for β*).
10. $(k - 2)x^2 - 2(4k^3 - 3k^2 + 5k + 2)x - 8k^3 + 7k^2 - 15k + 2 = 0$.
11. a) $x^2 + bx + ac = 0$
 b) $ac^2x^2 + b^2(b^2 - 3ac)x + a^2b^2c = 0$
 c) $c(ac + b + 1)x^2 + (b + 2ac)x + 1 = 0$
12. $x^2 - 4x + 3 = 0$
13. Hint: $\Delta = b^2 - 4ac$

4.10: Logarithms

1. a) $a + b + c$ b) $a - b - c$ c) $4a + 2b$
 d) $a - b + \log(4/3)$ e) $a(a + b)$ f) $a/\log e$
2. a) $x = 5$ b) $x = \log_7 14$ c) $x = 2$
 d) $x = \{-1, 4\}$ e) $x = \{-1, 2\}$ f) $x = \pm 3$
 g) $x = 2$ h) $x = \log_3(6 + \sqrt{33}) - 1$
 i) $x = 10$ j) $x = 10$ k) $x = \{4, 16\}$
 l) $x = 2/25$ m) $x = -1$ n) $x = 3^{3/4}$
 o) $x = \{2, 3\}$ p) $x = 99/100$
3. Hint: Solve the equation as usual, then simplify using laws of logarithms.
4. Note: we use tuple notation (x, y) to write the solutions of simultaneous equations. We also adopt the convention that a constant in front of such a vector is multiplied throughout, i.e., $\alpha(x, y) = (\alpha x, \alpha y)$. It is good to get used to using this notation when presenting solutions to simultaneous equations.
 a) $(x, y) = 2(4, 1)$ b) $(x, y) = 9(2 \pm 1, 2 \mp 1)$
 c) $(x, y) = \frac{3}{4}(3, 1)$ d) $(x, y) = (1, 2)$
 e) $(x, y) = 16(4, 1)$ f) $(x, y) = 4(2, 1)$
5. Solve $1500 \times 1.05^t = 2000$ to give $t \approx 5.89$. Hence $\lceil 5.98 \rceil = 6$ years must pass.
6. Solve $100 \times 2^t = 10^6$ to give $t \approx 13.29$, hence $\lceil 13.29 \times 30 \rceil = 399$ minutes must pass, or 6 hours and 39 minutes.
7. 216 kilometres.
8. Hint: Use laws of logs.
9. Hint: Reduce the right hand side to a single logarithm, and compare their arguments. This should lead to $(a - b)^2 = 0$, i.e., $a = b$.
10. Hint: Use the laws of logs, and switch to index form when necessary.
11. Hint: Prove that $\frac{1}{\log_a x} = \log_x a$.

5.15: Polynomial Division

1. Only (g) is proper.
2. a) $2x + \frac{5}{2} - \frac{11}{2(2x+1)}$ b) $\frac{4}{3} + \frac{7}{3(3t-1)}$
 c) $\frac{4}{3}x - \frac{28}{3x}$ d) $x + \frac{1}{x^2 + x + 1}$
 e) $4x^3 - x^2 + 3x - 2 + \frac{2}{x+1}$ g) $x - 9 + \frac{12(3x+1)}{(x+1)(x+2)}$
 h) $x^2 - x + 1 - \frac{28}{x+1}$ i) $\frac{\pi}{2} + \frac{\pi}{x+\pi}$

5.34: Remainder and Factor Theorems

1. $a = 2$, $b = -13$, the polynomial factorises as $(2x+1)(x+2)(x-3)$.
2. a) $x = -2, 3$ b) $x = -3, -\frac{2}{3}, -7$ c) $x = -\frac{1}{2}, 2, 3$
 d) $x = 7, -\frac{1}{2}(5 \pm \sqrt{29})$ e) $x = -4, -2, -1, 1$ f) $x = \pm 2$
 g) $x = -\frac{1}{2}, -\frac{1}{3}, -\frac{1}{4}$ h) $x = 3, \frac{1}{2}(3 \pm \sqrt{5})$ i) $x = a, \pm\sqrt{3}$
3. a) $2, -1/3$

Hint: Try putting $x = s/t$ with $s = \pm 1, \pm 2, \pm 4$ and $t = \pm 1, \pm 3$.

b) $\frac{1}{2}(7 \pm \sqrt{41})$

Hint: Let the remaining two roots be α, β . By Viète's formulæ, $2^{-1/3} + \alpha + \beta = 2^{6/3}$ and $2^{(1/3)}\alpha\beta = -4/3$. Solving simultaneously yields α and β .

c) -100

Hint: Evaluate $p(3)$ and apply the remainder theorem.

4. a) $-1/2, 3, 5$ b) $-1/3, 1$ (repeated)
 c) $1/2, 1/2(5 \pm \sqrt{53})$ d) $1/2$
5. Hint: reproduce the proof of the rational roots theorem (5.29) with $c = 3$ and $d = 5$.

6. a) Hint: use [theorem 5.28](#) and deduce that $q(x) = a$ using the degree and the fact that the leading coefficient is a (comparing coefficients).
- b) Hint: Expand the brackets of the expression in (a) and compare coefficients.
- c) Hint: Use basic algebra for the identities. For the new cubic, adapt the method of [example 3.20](#) to find Σ_N , Π_N and Ξ_N of the new roots. These should work out to be $(\alpha^2 + \beta^2 + \gamma^2)/\Pi$, $1/\Pi$ and $1/\alpha^2 + 1/\beta^2 + 1/\gamma^2$ respectively.

The resulting cubic is $x^3 + 10x^2 + 25x + 3$.

Appreciate how efficient this is compared to what a Naïve method would look like!

7. a) By the rational roots theorem, the only possible rational roots of $x^2 - 2$ are $\pm 1, \pm 2$. None of these are roots though, so $\sqrt{2}$ which is, by definition, a root of $x^2 - 2$, cannot be rational.
- b) If we let $x = \sqrt{2 + \sqrt{3}}$, then $x^2 = 2 + \sqrt{3}$, so $(x^2 - 2)^2 = 3$ and the desired polynomial is therefore $(x^2 - 2)^2 - 3 = x^4 - 4x^2 + 1$. The only possible rational roots of this polynomial are ± 1 by the rational roots theorem, none of which result in $2 + \sqrt{3}$ when squared (so they are $\neq \sqrt{2 + \sqrt{3}}$). Hence the root $\sqrt{2 + \sqrt{3}}$ of $x^4 - 4x^2 + 1$ cannot be rational.
- c) If we let $x = \sqrt{4 + 2\sqrt{3}} - \sqrt{3}$, then $(x + \sqrt{3})^2 = 4 + 2\sqrt{3}$, i.e., $x^2 + 2\sqrt{3} + 3 = 4 + 2\sqrt{3}$, i.e., $x^2 - 1 = 0$. Thus $\sqrt{4 + 2\sqrt{3}} - \sqrt{3}$ is a root of $x^2 - 1$. But the roots of this polynomial are ± 1 , so in fact this equals ± 1 . To see which, we can observe that by reversing some of our working, $x^2 + 2\sqrt{3} + 3 = (x + \sqrt{3})^2$ for any x . In particular, putting $x = 1$, we see that

$$\begin{aligned}\sqrt{4 + 2\sqrt{3}} - \sqrt{3} &= \sqrt{1^2 + 2\sqrt{3} + 3} \\ &= \sqrt{(1 + \sqrt{3})^2} - \sqrt{3} = 1 + \sqrt{3} - \sqrt{3} = 1.\end{aligned}$$

2. There are various different ways one can express the same set using set comprehension. Here only one way is given.

- | | |
|---|---|
| a) $\{n \in \mathbb{N} : 10 \leq n \leq 16\}$ | b) $\{2n + 1 : n \in \mathbb{N} \text{ and } n \leq 6\}$ |
| c) $\{2^n : n \in \mathbb{N}\}$ | d) $\{m^2 : m = 2n - 1 \text{ and } n \in \mathbb{N}\}$ |
| e) $\{7n : n \in \mathbb{Z}\}$ | f) $\{2^n : n \in \mathbb{Z}\}$ |
| g) $\{4n + 3 : n \in \mathbb{Z}\}$ | h) $\{\{m \in \mathbb{N} : m \leq n\} : n \in \mathbb{Z}\}$ |
| i) $\{\frac{\pi n}{3} : n \in \mathbb{Z}\}$ | j) $\{m \in \mathbb{N} : m/4 \notin \mathbb{N}\}$ |
| k) $\{\frac{10}{9}(1 - 10^{-n}) : n \in \mathbb{N}\}$ | |

Explanation: 10^n is the number 1 followed by n zeros. Subtracting 1, we get $10^n - 1$ which is then the number made up of n nines. Dividing this number by 9 to get $\frac{1}{9}(10^n - 1)$, we obtain the number made up of n ones. Now for this number to be in our set, we want a decimal point to appear after the first digit. Thus we must divide by 10, $n - 1$ times, to get the number $\frac{1}{10^{n-1}} \times \frac{1}{9}(10^n - 1)$, which simplifies to $\frac{10}{9}(1 - 10^{-n})$.

- 1) Define the function $f(n)$ in the following way:

$$\begin{aligned} f(1) &= 3 \\ f(n) &= \{f(n-1)\}. \end{aligned}$$

This is what we call a *recursive* definition, where we use the definition over and over again until we end up with $f(1)$, which is called the *base case*.

Let us work out the first few instances of $f(n)$ to illustrate:

$$\begin{aligned} f(1) &= 3 \\ f(2) &= \{f(1)\} = \{3\} \\ f(3) &= \{f(2)\} = \{\{f(1)\}\} = \{\{3\}\}, \end{aligned}$$

and so on. Thus the set is given by $\{f(n) : n \in \mathbb{N}\}$. Honestly, doing it this way feels a bit like cheating. There is another way, but it's a bit harder to parse:

$$\{x : \text{for all sets } H, \text{ if } 3 \in H \text{ and for every } z \in H \text{ we have } \{z\} \in H, \text{ then } x \in H\}.$$

In logical symbols,

$$\{x : \forall H((3 \in H \wedge \forall z(z \in H \Rightarrow \{z\} \in H)) \Rightarrow x \in H)\}.$$

Let's break it down. Let's say a set H is “3-hungry” if it contains 3, and if for each $z \in H$, we have $\{z\} \in H$ too. Since a 3-hungry set contains 3, it will therefore contain $\{3\}$, and consequently also $\{\{3\}\}$, and so on. So any 3-hungry set will be a superset of the set we want to express (let's call it T). Now define

$$S = \{x : x \text{ is in every 3-hungry set}\}.$$

Clearly T is 3-hungry by definition, so $S \subseteq T$. But also every element of T is contained in every 3-hungry set, so $T \subseteq S$. Thus $S = T$, and notice that S is the same set which we have defined above (with less scary notation).

- m) $\{\{m \in \mathbb{N} : m \leq n\}^2 : n \in \mathbb{Z}\}$
or $\{(k, \ell) : k, \ell \in \mathbb{N} \text{ and } k, \ell \leq n\} : n \in \mathbb{Z}\}.$

