MT181 Number Systems

Mark Wildon, mark.wildon@rhul.ac.uk

Administration:

- Workshops begin next week.
- Sign-in sheet. **Please return to the lecturer after each lecture.**
- Make sure you get the Section 1 Notes, Problem Sheet 1, and the sheet of Challenge Problems when they are passed around. **Always pass everything to the back, even if you the person you are passing to already has a copy.**
- All handouts will be put on Moodle.

MT181 Number Systems

Mark Wildon, mark.wildon@rhul.ac.uk

Administration:

- Workshops begin next week.
- Sign-in sheet. **Please return to the lecturer after each lecture.**
- Make sure you get the Section 1 Notes, Problem Sheet 1, and the sheet of Challenge Problems when they are passed around. **Always pass everything to the back, even if you the person you are passing to already has a copy.**
- All handouts will be put on Moodle.
- **Lectures in BLT1:** Tuesday 1pm, Thursday 9am and Friday 2pm.
- **Office hours in McCrea 240:** Monday 4pm, Wednesday 10am and Friday 4pm.

Recommended Reading and Other Resources

[1] *How to think like a mathematician*. Kevin Houston, Cambridge University Press, 2009.

[2] *A concise introduction to pure mathematics*. Martin Liebeck, Chapman and Hall, 2000.

[3] *Discrete Mathematics*. Norman L. Biggs, Oxford University Press, 2002.

- Printed notes. (But you should also make your own notes.)
- These slides are available from Moodle.
- Problem sheets. Each of the eight marked problem sheets is worth 1.25% of your overall grade. This mark is awarded for any reasonable attempt.
- Discuss questions with your colleagues.
- Go to the solutions classes.
- Web: `planetmath.org`, `http://math.stackexchange.com`.
- Check your answers to computational problems with computer algebra packages such as Mathematica.

Part A: Sets, Functions and Complex Numbers

§1 Introduction: Sets of Numbers

One of the unifying ideas in this course is solving equations. I hope we can all agree this is an useful and interesting thing to do. For example, consider the equation

$$x^2 + y^2 = 25.$$

How many solutions are there?

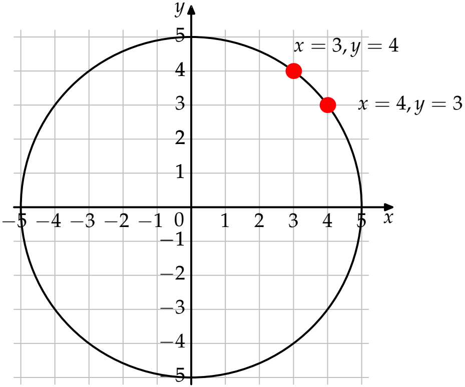
Part A: Sets, Functions and Complex Numbers

§1 Introduction: Sets of Numbers

One of the unifying ideas in this course is solving equations. I hope we can all agree this is an useful and interesting thing to do. For example, consider the equation

$$x^2 + y^2 = 25.$$

How many solutions are there?

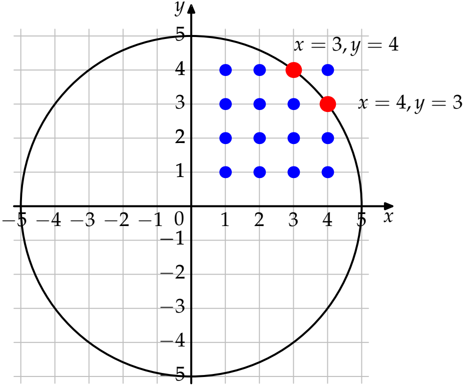


§1 Introduction: Sets of Numbers

One of the unifying ideas in this course is solving equations. I hope we can all agree this is an useful and interesting thing to do. For example, consider the equation

$$x^2 + y^2 = 25.$$

How many solutions are there?



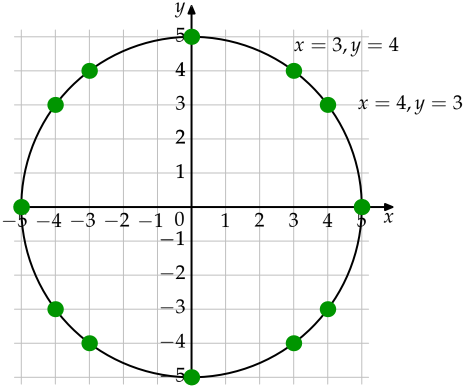
Part A: Sets, Functions and Complex Numbers

§1 Introduction: Sets of Numbers

One of the unifying ideas in this course is solving equations. I hope we can all agree this is an useful and interesting thing to do. For example, consider the equation

$$x^2 + y^2 = 25.$$

How many solutions are there?



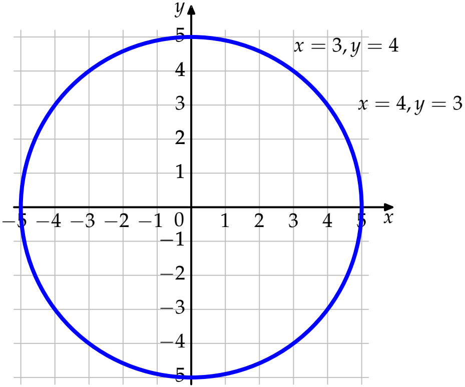
Part A: Sets, Functions and Complex Numbers

§1 Introduction: Sets of Numbers

One of the unifying ideas in this course is solving equations. I hope we can all agree this is an useful and interesting thing to do. For example, consider the equation

$$x^2 + y^2 = 25.$$

How many solutions are there?



Sets

A *set* is any collection of objects. These objects are called the *members* or *elements* of the set.

If X is a set and x is an element of X then we write $x \in X$. (This can be read as 'x is in X', or 'X contains x'.) If y is not an element of X then we write $y \notin X$. For example, $7 \in \{2, 3, 5, 7, 11, 13\}$ and $8 \notin \{2, 3, 5, 7, 11, 13\}$.

Exercise 1.2

True or false?

(i) 29 is a member of the set of prime numbers;

(ii) 87 is a member of the set of prime numbers;

(iii) $\{2, 3, 5, 7, 11\} = \{5, 7, 11, 2, 3\}$.

Sets

A *set* is any collection of objects. These objects are called the *members* or *elements* of the set.

If X is a set and x is an element of X then we write $x \in X$. (This can be read as 'x is in X', or 'X contains x'.) If y is not an element of X then we write $y \notin X$. For example, $7 \in \{2, 3, 5, 7, 11, 13\}$ and $8 \notin \{2, 3, 5, 7, 11, 13\}$.

Exercise 1.2

True or false?

(i) 29 is a member of the set of prime numbers; True

(ii) 87 is a member of the set of prime numbers;

(iii) $\{2, 3, 5, 7, 11\} = \{5, 7, 11, 2, 3\}$.

Sets

A *set* is any collection of objects. These objects are called the *members* or *elements* of the set.

If X is a set and x is an element of X then we write $x \in X$. (This can be read as 'x is in X', or 'X contains x'.) If y is not an element of X then we write $y \notin X$. For example, $7 \in \{2, 3, 5, 7, 11, 13\}$ and $8 \notin \{2, 3, 5, 7, 11, 13\}$.

Exercise 1.2

True or false?

(i) 29 is a member of the set of prime numbers; True

(ii) 87 is a member of the set of prime numbers; False

(iii) $\{2, 3, 5, 7, 11\} = \{5, 7, 11, 2, 3\}$.

Sets

A *set* is any collection of objects. These objects are called the *members* or *elements* of the set.

If X is a set and x is an element of X then we write $x \in X$. (This can be read as 'x is in X', or 'X contains x'.) If y is not an element of X then we write $y \notin X$. For example, $7 \in \{2, 3, 5, 7, 11, 13\}$ and $8 \notin \{2, 3, 5, 7, 11, 13\}$.

Exercise 1.2

True or false?

(i) 29 is a member of the set of prime numbers; True

(ii) 87 is a member of the set of prime numbers; False

(iii) $\{2, 3, 5, 7, 11\} = \{5, 7, 11, 2, 3\}$. True

Sets of Numbers

We write $\mathbb{N}$ for the set of natural numbers:

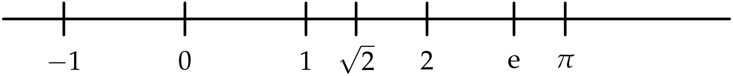
$$\mathbb{N} = \{1, 2, 3, 4, \ldots\}.$$

We write $\mathbb{Z}$ for the set of integers:

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

A number r/s with $r \in \mathbb{Z}$, $s \in \mathbb{Z}$ and $s \neq 0$ is said to be *rational*. We write $\mathbb{Q}$ for the set of rational numbers. Finally we write $\mathbb{R}$ for the set of real numbers.

Some important real numbers are marked below.



Rational and Irrational Numbers

It is an important fact that there are real numbers that are not rational numbers. For example $\sqrt{2} \notin \mathbb{Q}$. We say that such numbers are *irrational*. So what sort of numbers are rational?

Example 1.3 (See board)

Rational and Irrational Numbers

It is an important fact that there are real numbers that are not rational numbers. For example $\sqrt{2} \notin \mathbb{Q}$. We say that such numbers are *irrational*. So what sort of numbers are rational?

Example 1.3 (See board)

Note that ‘ $\implies$ ’ means ‘implies’. If A and B are mathematical statements then

$$A \implies B$$

means ‘A implies B’ or equivalently

‘if A is true, then B is true’.

Using implies signs (and more importantly, words!) will help to clarify the structure of your arguments.

Rational and Irrational Numbers

It is an important fact that there are real numbers that are not rational numbers. For example $\sqrt{2} \notin \mathbb{Q}$. We say that such numbers are *irrational*. So what sort of numbers are rational?

Example 1.3 (See board)

Note that ' $\implies$ ' means 'implies'. If A and B are mathematical statements then

$$A \implies B$$

means 'A implies B' or equivalently

'if A is true, then B is true'.

Using implies signs (and more importantly, words!) will help to clarify the structure of your arguments.

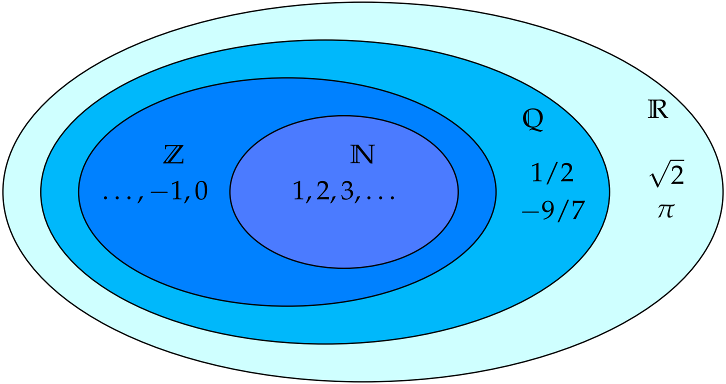
Exercise 1.4

Find a simple expression for $0.99999\ldots$. Are you happy with the answer?

Number Systems Seen So Far

In this diagram, sets are drawn as regions in the plane.

Note that a set contains all the numbers in the sets drawn inside it. For example, It is therefore entirely correct to say that 1 is a real number, or that -1 is a rational number.



Pre-lecture Quiz (Thursday 3 October)

True or False:

(a) $\sqrt{2}$ is a real number

(b) $\sqrt{2}$ is a rational number

(c) $0.123456789\,123456789\ldots$ is a rational number

(d) 3.141592 is a rational number

(e) 1 is a real number

Pre-lecture Quiz (Thursday 3 October)

True or False:

(a) $\sqrt{2}$ is a real number — True

(b) $\sqrt{2}$ is a rational number

(c) $0.123456789\,123456789\ldots$ is a rational number

(d) 3.141592 is a rational number

(e) 1 is a real number

Pre-lecture Quiz (Thursday 3 October)

True or False:

(a) $\sqrt{2}$ is a real number True

(b) $\sqrt{2}$ is a rational number False

(c) $0.123456789\,123456789\ldots$ is a rational number

(d) 3.141592 is a rational number

(e) 1 is a real number

Pre-lecture Quiz (Thursday 3 October)

True or False:

(a) $\sqrt{2}$ is a real number True

(b) $\sqrt{2}$ is a rational number False

(c) $0.123456789\,123456789\ldots$ is a rational number True

(d) 3.141592 is a rational number

(e) 1 is a real number

Pre-lecture Quiz (Thursday 3 October)

True or False:

(a) $\sqrt{2}$ is a real number True

(b) $\sqrt{2}$ is a rational number False

(c) $0.123456789\,123456789\ldots$ is a rational number True

(d) 3.141592 is a rational number True

(e) 1 is a real number

For (d): $\dfrac{3\,141\,592}{1\,000\,000} = 3.141592 \neq \pi$. ($\pi = 3.14159265358\ldots$.)

Pre-lecture Quiz (Thursday 3 October)

True or False:

(a) $\sqrt{2}$ is a real number True

(b) $\sqrt{2}$ is a rational number False

(c) $0.123456789\,123456789\ldots$ is a rational number True

(d) 3.141592 is a rational number True

(e) 1 is a real number True

For (d): $\dfrac{3\,141\,592}{1\,000\,000} = 3.141592 \neq \pi$. ($\pi = 3.14159265358\ldots$.)

Pre-lecture Quiz (Thursday 3 October)

True or False:

(a) $\sqrt{2}$ is a real number True

(b) $\sqrt{2}$ is a rational number False

(c) $0.123456789\,123456789\ldots$ is a rational number True

(d) 3.141592 is a rational number True

(e) 1 is a real number True

For (d): $\dfrac{3\,141\,592}{1\,000\,000} = 3.141592 \neq \pi$. $(\pi = 3.14159265358\ldots.)$

For (e): 1 is a natural number, and every natural number is also a real number.

Closure and Equation Solving

One important property of the natural numbers, which I hope you will agree is obviously true, is that if $m, n \in \mathbb{N}$ then $m + n \in \mathbb{N}$ and $mn \in \mathbb{N}$.

Definition 1.5

Let X be a set of numbers. We say that X is

- *closed under addition* if $x + y \in X$ whenever $x \in X$ and $y \in X$;
- *closed under multiplication* if $xy \in X$ whenever $x \in X$ and $y \in X$;
- *closed under subtraction* if $x - y \in X$ whenever $x \in X$ and $y \in X$;
- *closed under division* if $x/y \in X$ whenever $x \in X$, $y \in X$ and $y \neq 0$.

Exercise 1.6

- Is $\mathbb{N}$ closed under division?
- Is $\mathbb{Z}$ closed under division?
- Is $\mathbb{Q}$ closed under addition?

Closure and Equation Solving

One important property of the natural numbers, which I hope you will agree is obviously true, is that if $m, n \in \mathbb{N}$ then $m + n \in \mathbb{N}$ and $mn \in \mathbb{N}$.

Definition 1.5

Let X be a set of numbers. We say that X is

- *closed under addition* if $x + y \in X$ whenever $x \in X$ and $y \in X$;
- *closed under multiplication* if $xy \in X$ whenever $x \in X$ and $y \in X$;
- *closed under subtraction* if $x - y \in X$ whenever $x \in X$ and $y \in X$;
- *closed under division* if $x/y \in X$ whenever $x \in X$, $y \in X$ and $y \neq 0$.

Exercise 1.6

- Is $\mathbb{N}$ closed under division? No: $1/2 \notin \mathbb{N}$
- Is $\mathbb{Z}$ closed under division?
- Is $\mathbb{Q}$ closed under addition?

Closure and Equation Solving

One important property of the natural numbers, which I hope you will agree is obviously true, is that if $m, n \in \mathbb{N}$ then $m + n \in \mathbb{N}$ and $mn \in \mathbb{N}$.

Definition 1.5

Let X be a set of numbers. We say that X is

- *closed under addition* if $x + y \in X$ whenever $x \in X$ and $y \in X$;
- *closed under multiplication* if $xy \in X$ whenever $x \in X$ and $y \in X$;
- *closed under subtraction* if $x - y \in X$ whenever $x \in X$ and $y \in X$;
- *closed under division* if $x/y \in X$ whenever $x \in X$, $y \in X$ and $y \neq 0$.

Exercise 1.6

- Is $\mathbb{N}$ closed under division? No: $1/2 \notin \mathbb{N}$
- Is $\mathbb{Z}$ closed under division? No: $1/2 \notin \mathbb{Z}$.
- Is $\mathbb{Q}$ closed under addition?

Closure and Equation Solving

One important property of the natural numbers, which I hope you will agree is obviously true, is that if $m, n \in \mathbb{N}$ then $m + n \in \mathbb{N}$ and $mn \in \mathbb{N}$.

Definition 1.5

Let X be a set of numbers. We say that X is

- *closed under addition* if $x + y \in X$ whenever $x \in X$ and $y \in X$;
- *closed under multiplication* if $xy \in X$ whenever $x \in X$ and $y \in X$;
- *closed under subtraction* if $x - y \in X$ whenever $x \in X$ and $y \in X$;
- *closed under division* if $x/y \in X$ whenever $x \in X$, $y \in X$ and $y \neq 0$.

Exercise 1.6

- Is $\mathbb{N}$ closed under division? No: $1/2 \notin \mathbb{N}$
- Is $\mathbb{Z}$ closed under division? No: $1/2 \notin \mathbb{Z}$.
- Is $\mathbb{Q}$ closed under addition? Yes: But one example is not enough to prove this.

Closure and Equation Solving

One important property of the natural numbers, which I hope you will agree is obviously true, is that if $m, n \in \mathbb{N}$ then $m + n \in \mathbb{N}$ and $mn \in \mathbb{N}$.

Definition 1.5

Let X be a set of numbers. We say that X is

- *closed under addition* if $x + y \in X$ whenever $x \in X$ and $y \in X$;
- *closed under multiplication* if $xy \in X$ whenever $x \in X$ and $y \in X$;
- *closed under subtraction* if $x - y \in X$ whenever $x \in X$ and $y \in X$;
- *closed under division* if $x/y \in X$ whenever $x \in X$, $y \in X$ and $y \neq 0$.

Exercise 1.6

- Is $\mathbb{N}$ closed under division? No: $1/2 \notin \mathbb{N}$
- Is $\mathbb{Z}$ closed under division? No: $1/2 \notin \mathbb{Z}$.
- Is $\mathbb{Q}$ closed under addition? Yes: But one example is not enough to prove this.

Closure properties of a set X are closely related to the equations that can be solved using numbers from X.

Proof that $\mathbb{Q}$ is Closed Under Addition

Let $x \in \mathbb{Q}$ and $y \in \mathbb{Q}$. Since $x \in \mathbb{Q}$ there exist $r, s \in \mathbb{Z}$ such that $s \neq 0$ and $x = r/s$. Since $y \in \mathbb{Q}$ there exist $t, u \in \mathbb{Z}$ such that $u \neq 0$ and $y = t/u$. Now

$$x + y = \frac{r}{s} + \frac{t}{u} = \frac{ru + st}{su}.$$

Hence $x + y = m/n$ where $m = ru + st$ and $n = su$. Since the integers are closed under addition and multiplication, we have $m \in \mathbb{Z}$ and $n \in \mathbb{Z}$. Therefore $x + y$ is rational. □

Exercise 1.7

At the end this proof has one (easily fixed) gap. You might also object to it for other reasons. Come up with at least one objection.

Proof that $\mathbb{Q}$ is Closed Under Addition

Let $x \in \mathbb{Q}$ and $y \in \mathbb{Q}$. Since $x \in \mathbb{Q}$ there exist $r, s \in \mathbb{Z}$ such that $s \neq 0$ and $x = r/s$. Since $y \in \mathbb{Q}$ there exist $t, u \in \mathbb{Z}$ such that $u \neq 0$ and $y = t/u$. Now

$$x + y = \frac{r}{s} + \frac{t}{u} = \frac{ru + st}{su}.$$

Hence $x + y = m/n$ where $m = ru + st$ and $n = su$. Since the integers are closed under addition and multiplication, we have $m \in \mathbb{Z}$ and $n \in \mathbb{Z}$. Therefore $x + y$ is rational. □

Exercise 1.7

At the end this proof has one (easily fixed) gap. You might also object to it for other reasons. Come up with at least one objection.

Mathematical gap: At the end we claimed that $x + y = m/n$ where $n = su$. But it is illegal to divide by 0. A careful mathematician would explain that su is non-zero, and so we are allowed to divide by it.

Replies to Some Other Objections

- ‘Why so many words? I thought we were here to do mathematics.’ Reply: We are, and we did.

Replies to Some Other Objections

- 'Why so many words? I thought we were here to do mathematics.' Reply: We are, and we did. That said, the proof could be given almost entirely using symbols:

$$
\begin{aligned}
&x \in \mathbb{Q} \implies x = r/s,\ r \in \mathbb{Z},\ s \in \mathbb{Z}\\
&y \in \mathbb{Q} \implies y = t/u,\ t \in \mathbb{Z},\ u \in \mathbb{Z}\\
&\quad \implies x + y = \frac{r}{s} + \frac{t}{u} = \frac{ru + st}{su}\\
&\quad \implies x + y = m/n \quad m = ru + st \in \mathbb{Z},\ n = su \in \mathbb{Z}\\
&\qquad\qquad\qquad\qquad\quad su \neq 0 \text{ since } s \neq 0,\ u \neq 0.
\end{aligned}
$$

Replies to Some Other Objections

- ‘Why so many words? I thought we were here to do mathematics.’ Reply: We are, and we did. That said, the proof could be given almost entirely using symbols:

$$\begin{aligned}
&x \in \mathbb{Q} \implies x = r/s,\ r \in \mathbb{Z},\ s \in \mathbb{Z} \\
&y \in \mathbb{Q} \implies y = t/u,\ t \in \mathbb{Z},\ u \in \mathbb{Z} \\
&\implies x + y = \frac{r}{s} + \frac{t}{u} = \frac{ru + st}{su} \\
&\implies x + y = m/n \quad m = ru + st \in \mathbb{Z},\ n = su \in \mathbb{Z} \\
&\qquad\qquad\qquad\qquad\quad su \neq 0 \text{ since } s \neq 0,\ u \neq 0.
\end{aligned}$$

  Comments

  - No explanation is given for why m and n are integers.
  - The reason why r, s, t, u exist is compressed into the implies signs after $x \in \mathbb{Q}$ and $y \in Q$.
  - A ‘where’ before the m in $m = ru + st$ would be good style.
  - The first and second lines should probably say that $s \neq 0$ and $t \neq 0$.
  - There is no statement at any point of what is being proved.

Symbolic Proofs: What To Avoid

One problem with relying heavily on symbols is that a single slip can make an argument impossible to follow. It also makes it harder to put in any explanations. Remember that you will be the reader in a few months when you are revising for exams.

Here is an example of the sort of thing to avoid.

$$x = r/s, \; y = t/u$$

$$x + y = ru + st/su$$

$$\text{Proved}$$

Some of the main problems:

- What are r, s, t, u?
- Second line should be $(ru + st)/su$.
- **What** has been proved? It's hard to tell because the rational numbers are not mentioned at any point!

(Chapter 3 of *How to Think Like a Mathematician* has advice on writing mathematics. You will be asked to read it next week.)

Replies to Some Other Objections [continued]

- ‘All we showed is that the sum of two fractions is a fraction. Isn’t this just obvious?’ Reply: maybe it is.

Replies to Some Other Objections [continued]

- ‘All we showed is that the sum of two fractions is a fraction. Isn’t this just obvious?’ Reply: maybe it is. But many obvious sounding statements have turned out to be false. And we have to start somewhere: it’s best to get practice at writing proofs on results that are fairly easy.

  We will prove some much more interesting results later in the course.

Replies to Some Other Objections [continued]

- 'All we showed is that the sum of two fractions is a fraction. Isn't this just obvious?' Reply: maybe it is. But many obvious sounding statements have turned out to be false. And we have to start somewhere: it's best to get practice at writing proofs on results that are fairly easy.

  We will prove some much more interesting results later in the course.

- 'In the proof you assumed that $\mathbb{Z}$ is closed under addition and multiplication. How do we know this?' Reply: good point.

Replies to Some Other Objections [continued]

- 'All we showed is that the sum of two fractions is a fraction. Isn't this just obvious?' Reply: maybe it is. But many obvious sounding statements have turned out to be false. And we have to start somewhere: it's best to get practice at writing proofs on results that are fairly easy.

  We will prove some much more interesting results later in the course.

- 'In the proof you assumed that $\mathbb{Z}$ is closed under addition and multiplication. How do we know this?' Reply: good point.

  But at least this proof reduces the problem of showing that $\mathbb{Q}$ is closed under adddition to proving that $\mathbb{Z}$ is closed under addition and multiplication. Most people would be prepared to take these properties of $\mathbb{Z}$ for granted.

Subsets

If X and Y are sets and every element of X is an element of Y, then we say that X is a *subset* of Y, and write $X \subseteq Y$. In symbols the condition $X \subseteq Y$ is

$$x \in X \implies x \in Y.$$

For example $\mathbb{N}$ is a subset of $\mathbb{Z}$, $\mathbb{Z}$ is a subset of $\mathbb{Q}$ and $\mathbb{Q}$ is a subset of $\mathbb{R}$. In symbols

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

Subsets

If X and Y are sets and every element of X is an element of Y, then we say that X is a *subset* of Y, and write $X \subseteq Y$. In symbols the condition $X \subseteq Y$ is

$$x \in X \implies x \in Y.$$

For example $\mathbb{N}$ is a subset of $\mathbb{Z}$, $\mathbb{Z}$ is a subset of $\mathbb{Q}$ and $\mathbb{Q}$ is a subset of $\mathbb{R}$. In symbols

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

There is a special notation for defining subsets of a set. For example if Y is the set of prime numbers and

$$X = \{x \in Y : x \leq 13\}$$

then X is the set of prime numbers x such that $x \leq 13$. The set $\mathbb{Q}$ of rational numbers can be defined as

$$\mathbb{Q} = \{r/s : r \in \mathbb{Z}, s \in \mathbb{Z}, s \neq 0\}.$$

Example of Subsets

Example 1.8

Let

$$X = \{x \in \mathbb{R} : x \geq 2 + \sqrt{5}.\}$$
$$Y = \{x \in \mathbb{R} : x^2 - 4x + 1 \geq 2\}$$

We will show that $X \subseteq Y$. Is it true that $X = Y$?

The symbol '$\iff$' will be used in the proof: if A and B are mathematical statements then $A \iff B$ means that A implies B *and* B implies A. So A and B are either both true, or both false.

Example of Subsets

Example 1.8

Let

$$X = \{x \in \mathbb{R} : x \geq 2 + \sqrt{5}.\}$$
$$Y = \{x \in \mathbb{R} : x^2 - 4x + 1 \geq 2\}$$

We will show that $X \subseteq Y$. Is it true that $X = Y$?

The symbol '$\iff$' will be used in the proof: if A and B are mathematical statements then $A \iff B$ means that A implies B *and* B implies A. So A and B are either both true, or both false.

Remark: We say that X is a *proper subset* of Y if X is a subset of Y and $X \neq Y$.

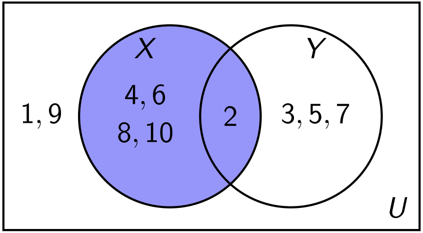
It is correct to write $X \subseteq Y$ even if X is a proper subset of Y. (If this was not allowed, the **only** time it would be correct to write $X \subseteq Y$ would be when $X = Y$. Surely this cannot be a sensible use of notation!)

Venn Diagrams

A *Venn diagram* is a diagram, like the one on page 6, that represents sets by regions of the plane. For example, the sets

$$\begin{aligned} U &= \{1, 2, 3, \ldots, 9, 10\} \\ X &= \{n \in U : n \text{ is even}\} \\ Y &= \{n \in U : n \text{ is a prime number}\} \end{aligned}$$

are shown in the Venn diagram below. The region representing X is shaded.



Intersection, Union, Complement

Let X and Y be sets.

- The *intersection* of X and Y, written $X \cap Y$, is the set of elements that are in both X and Y.
- The *union* of X and Y, written $X \cup Y$, is the set of elements in at least one of X and Y.
- If X is a subset of a set U then we define the *complement of X in U* by $X' = \{y \in U : y \notin X\}$.

Intersection, Union, Complement

Let X and Y be sets.

- The *intersection* of X and Y, written $X \cap Y$, is the set of elements that are in both X and Y.
- The *union* of X and Y, written $X \cup Y$, is the set of elements in at least one of X and Y.
- If X is a subset of a set U then we define the *complement of X in U* by $X' = \{y \in U : y \notin X\}$.

[**Correction:** on Thursday I wrote $X' = \{x \in P : x \text{ is even}\}$ as an example of a subset of the set P of prime numbers. The mark $'$ was intended to distinguish X' from X (the subset of primes ≤ 13). But this clashes badly with the notation for complements. **Please change X' to Z in your notes for Thursday.**]

Exercise 1.9

Draw Venn diagrams representing $X \cap Y$, $X \cup Y$ and X'.

De Morgan's Laws

Claim 1.10 (De Morgan's Laws)

Let X and Y be subsets of a set U. Then

(i) $(X \cup Y)' = X' \cap Y'$,

(ii) $(X \cap Y)' = X' \cup Y'$.

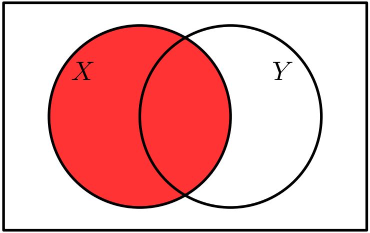
De Morgan's Laws

Claim 1.10 (De Morgan's Laws)

Let X and Y be subsets of a set U. Then

(i) $(X \cup Y)' = X' \cap Y'$,

(ii) $(X \cap Y)' = X' \cup Y'$.



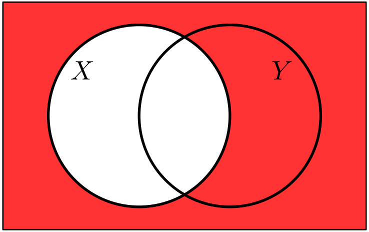
De Morgan's Laws

Claim 1.10 (De Morgan's Laws)

Let X and Y be subsets of a set U. Then

(i) $(X \cup Y)' = X' \cap Y'$,

(ii) $(X \cap Y)' = X' \cup Y'$.



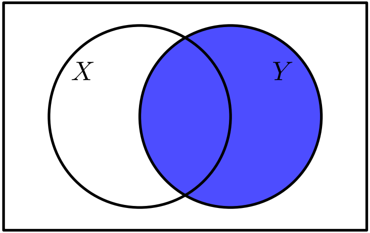
De Morgan's Laws

Claim 1.10 (De Morgan's Laws)

Let X and Y be subsets of a set U. Then

(i) $(X \cup Y)' = X' \cap Y'$,

(ii) $(X \cap Y)' = X' \cup Y'$.



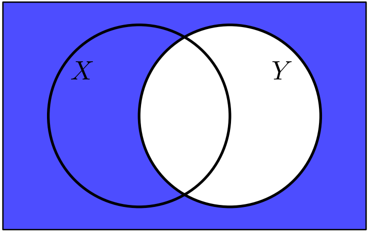
De Morgan's Laws

Claim 1.10 (De Morgan's Laws)

Let X and Y be subsets of a set U. Then

(i) $(X \cup Y)' = X' \cap Y'$,

(ii) $(X \cap Y)' = X' \cup Y'$.



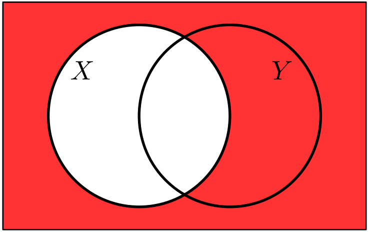
De Morgan's Laws

Claim 1.10 (De Morgan's Laws)

Let X and Y be subsets of a set U. Then

(i) $(X \cup Y)' = X' \cap Y'$,

(ii) $(X \cap Y)' = X' \cup Y'$.



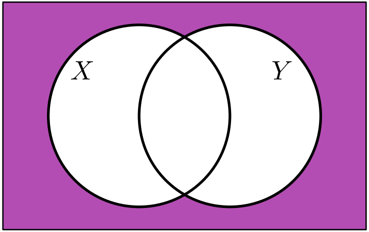
De Morgan's Laws

Claim 1.10 (De Morgan's Laws)

Let X and Y be subsets of a set U. Then

(i) $(X \cup Y)' = X' \cap Y'$,

(ii) $(X \cap Y)' = X' \cup Y'$.



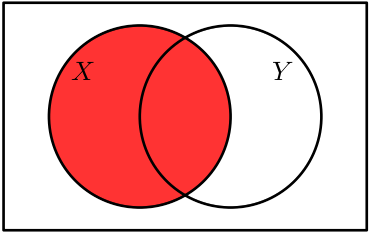
De Morgan's Laws

Claim 1.10 (De Morgan's Laws)

Let X and Y be subsets of a set U. Then

(i) $(X \cup Y)' = X' \cap Y'$,

(ii) $(X \cap Y)' = X' \cup Y'$.



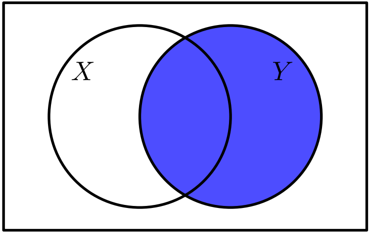
De Morgan's Laws

Claim 1.10 (De Morgan's Laws)

Let X and Y be subsets of a set U. Then

(i) $(X \cup Y)' = X' \cap Y'$,

(ii) $(X \cap Y)' = X' \cup Y'$.



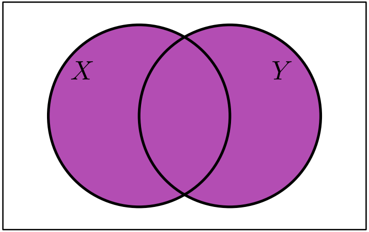
De Morgan's Laws

Claim 1.10 (De Morgan's Laws)

Let X and Y be subsets of a set U. Then

(i) $(X \cup Y)' = X' \cap Y'$,

(ii) $(X \cap Y)' = X' \cup Y'$.



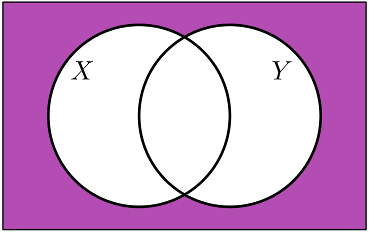
De Morgan's Laws

Claim 1.10 (De Morgan's Laws)

Let X and Y be subsets of a set U. Then

(i) $(X \cup Y)' = X' \cap Y'$,

(ii) $(X \cap Y)' = X' \cup Y'$.



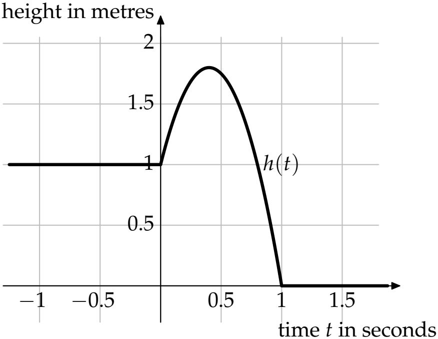
Administration

- Please put your work for Sheet 1 in one of the boxes. Make sure your name and student number is on it. It will be returned in the lecture on Friday.
- Problem Sheet 2 is on Moodle.
- Please take pages 15 to 18 of the handout. (Spare copies of pages 11 to 14 are available.)

§2 Functions

We need an idea of a function that is broad enough to cover everything that might be needed in pure mathematics, applied mathematics, probability and statistics. For example, this should definitely be a function:

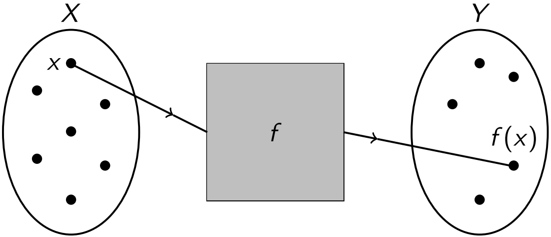
$$h(t) = \begin{cases} 1 & \text{if } t \leq 0 \\ 1 + 4t - 5t^2 & \text{if } 0 \leq t \leq 1 \\ 0 & \text{if } t \geq 1, \end{cases}$$



Definition of Functions

Definition 2.1

Let X and Y be sets. A *function* from X to Y is a black box such that, when an element $x \in X$ is put in, an element $y \in Y$ comes out. If the function is called f, then we write $f : X \to Y$. The output for the input x is written $f(x)$.



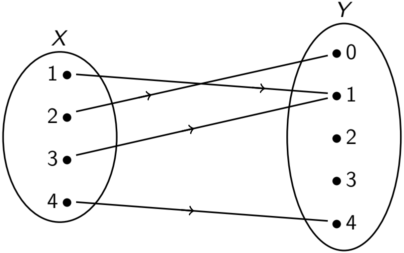
Question: When should two functions be said to be equal?

Example 2.2

Let $f : \{1, 2, 3, 4\} \to \{0, 1, 2, 3, 4\}$ be the function defined by

$$f(1) = 1, \quad f(2) = 0, \quad f(3) = 1, \quad f(4) = 4.$$

Define $g : \{1, 2, 3, 4\} \to \{0, 1, 2, 3, 4\}$ by $g(x) = (x - 2)^2$. Then $f = g$, since $f(x) = g(x)$ for all $x \in \{1, 2, 3, 4\}$.



Definition 2.3

Let $f : X \to Y$ be a function. The set X of allowed inputs to f is called the *domain* of f. The set Y of allowed outputs is called the *codomain* of f. The set $\{f(x) : x \in X\}$ of all outputs that actually appear is called the *range* of f.

[Correction to top of page 13]

Injective, Surjective, Bijective

Definition 2.5

Let X and Y be sets and let $f : X \to Y$ be a function.

(i) We say that f is *injective* if for all $x, x' \in X$,

$$f(x) = f(x') \implies x = x'.$$

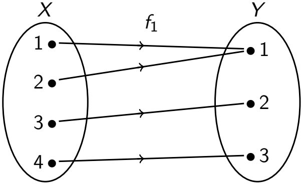
(ii) We say that f is *surjective* if for all $y \in Y$ there exists $x \in X$ such that $f(x) = y$.

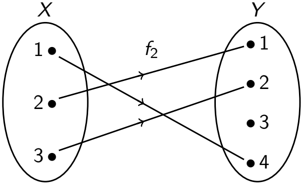
(iii) We say that f is *bijective* if f is injective and surjective.

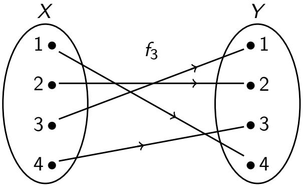
Injective, Surjective, Bijective: Diagrams and Graphs

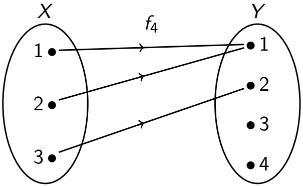
Example 2.6

For each of the functions f_1, f_2, f_3, f_4 drawn as a diagram below, we will determine which combination of the properties injective, surjective, bijective it has. (One function has none of these special properties.)



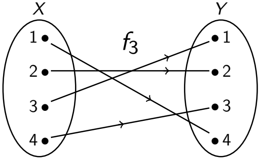


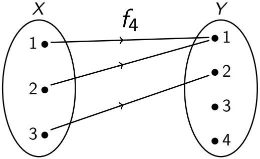


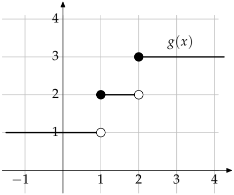


Pre-lecture quiz (Thursday 10th October)

The remaining two functions from Example 2.6, and a further function $g : \mathbb{R} \to \{1, 2, 3\}$ are shown below:







True or False? (Remind yourself of Definition 2.5 first!)

(1) f_3 is bijective

(2) f_4 is injective

(3) f_4 is surjective

(4) The equation $g(x) = y$ has a solution for every y in the codomain of g.

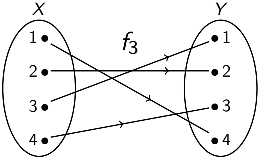
(5) The equation $g(x) = y$ has at most one solution for every y in the codomain of g.

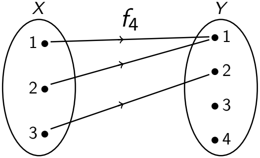
(6) g is surjective

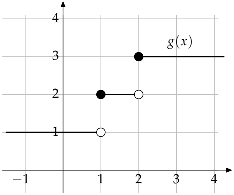
(7) g is injective

Pre-lecture quiz (Thursday 10th October)

The remaining two functions from Example 2.6, and a further function $g : \mathbb{R} \to \{1, 2, 3\}$ are shown below:







True or False? (Remind yourself of Definition 2.5 first!)

(1) f_3 is bijective True: f_3 is injective and surjective

(2) f_4 is injective

(3) f_4 is surjective

(4) The equation $g(x) = y$ has a solution for every y in the codomain of g.

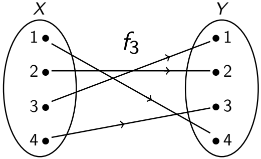
(5) The equation $g(x) = y$ has at most one solution for every y in the codomain of g.

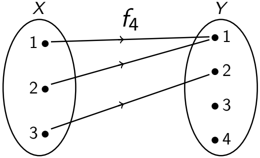
(6) g is surjective

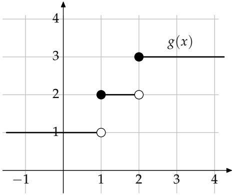
(7) g is injective

Pre-lecture quiz (Thursday 10th October)

The remaining two functions from Example 2.6, and a further function $g : \mathbb{R} \to \{1, 2, 3\}$ are shown below:







True or False? (Remind yourself of Definition 2.5 first!)

(1) f_3 is bijective — True: f_3 is injective and surjective

(2) f_4 is injective — False: $f_4(1) = f_4(2)$

(3) f_4 is surjective

(4) The equation $g(x) = y$ has a solution for every y in the codomain of g.

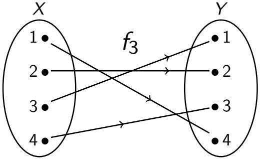
(5) The equation $g(x) = y$ has at most one solution for every y in the codomain of g.

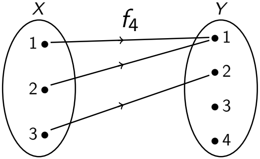
(6) g is surjective

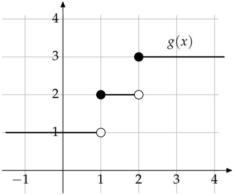
(7) g is injective

Pre-lecture quiz (Thursday 10th October)

The remaining two functions from Example 2.6, and a further function $g : \mathbb{R} \to \{1, 2, 3\}$ are shown below:







True or False? (Remind yourself of Definition 2.5 first!)

(1) f_3 is bijective True: f_3 is injective and surjective

(2) f_4 is injective False: $f_4(1) = f_4(2)$

(3) f_4 is surjective False: $3 \neq f(x)$ for any $x \in \{1, 2, 3, 4\}$

(4) The equation $g(x) = y$ has a solution for every y in the codomain of g.

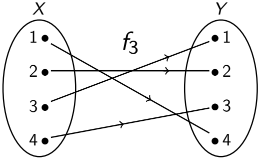
(5) The equation $g(x) = y$ has at most one solution for every y in the codomain of g.

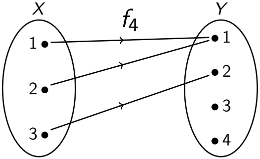
(6) g is surjective

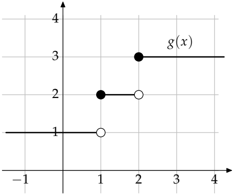
(7) g is injective

Pre-lecture quiz (Thursday 10th October)

The remaining two functions from Example 2.6, and a further function $g : \mathbb{R} \to \{1, 2, 3\}$ are shown below:







True or False? (Remind yourself of Definition 2.5 first!)

(1) f_3 is bijective — True: f_3 is injective and surjective

(2) f_4 is injective — False: $f_4(1) = f_4(2)$

(3) f_4 is surjective — False: $3 \neq f(x)$ for any $x \in \{1, 2, 3, 4\}$

(4) The equation $g(x) = y$ has a solution for every y in the codomain of g. — True (codomain is $\{1, 2, 3\}$)

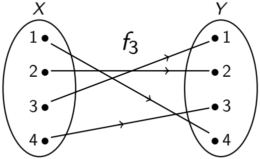
(5) The equation $g(x) = y$ has at most one solution for every y in the codomain of g.

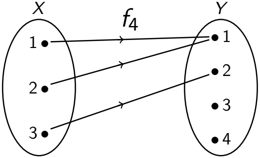
(6) g is surjective

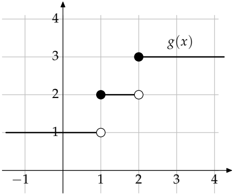
(7) g is injective

Pre-lecture quiz (Thursday 10th October)

The remaining two functions from Example 2.6, and a further function $g : \mathbb{R} \to \{1, 2, 3\}$ are shown below:







True or False? (Remind yourself of Definition 2.5 first!)

(1) f_3 is bijective — True: f_3 is injective and surjective

(2) f_4 is injective — False: $f_4(1) = f_4(2)$

(3) f_4 is surjective — False: $3 \neq f(x)$ for any $x \in \{1, 2, 3, 4\}$

(4) The equation $g(x) = y$ has a solution for every y in the codomain of g. — True (codomain is $\{1, 2, 3\}$)

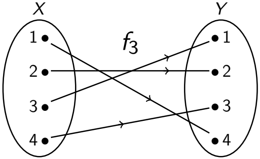
(5) The equation $g(x) = y$ has at most one solution for every y in the codomain of g. — False $g(1) = g(3/2) = 2$

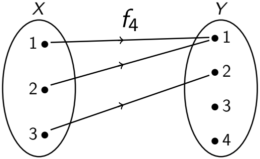
(6) g is surjective

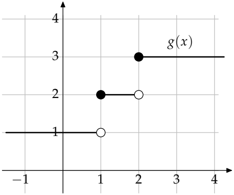
(7) g is injective

Pre-lecture quiz (Thursday 10th October)

The remaining two functions from Example 2.6, and a further function $g : \mathbb{R} \to \{1, 2, 3\}$ are shown below:







True or False? (Remind yourself of Definition 2.5 first!)

(1) f_3 is bijective — True: f_3 is injective and surjective

(2) f_4 is injective — False: $f_4(1) = f_4(2)$

(3) f_4 is surjective — False: $3 \neq f(x)$ for any $x \in \{1, 2, 3, 4\}$

(4) The equation $g(x) = y$ has a solution for every y in the codomain of g. — True (codomain is $\{1, 2, 3\}$)

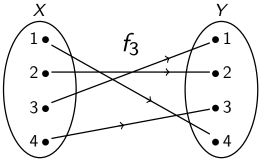
(5) The equation $g(x) = y$ has at most one solution for every y in the codomain of g. — False $g(1) = g(3/2) = 2$

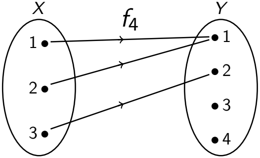
(6) g is surjective — True: exactly the same as (4)

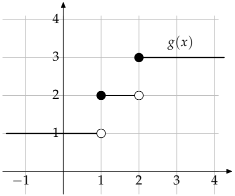
(7) g is injective

Pre-lecture quiz (Thursday 10th October)

The remaining two functions from Example 2.6, and a further function $g : \mathbb{R} \to \{1, 2, 3\}$ are shown below:







True or False? (Remind yourself of Definition 2.5 first!)

(1) f_3 is bijective — True: f_3 is injective and surjective

(2) f_4 is injective — False: $f_4(1) = f_4(2)$

(3) f_4 is surjective — False: $3 \neq f(x)$ for any $x \in \{1, 2, 3, 4\}$

(4) The equation $g(x) = y$ has a solution for every y in the codomain of g. — True (codomain is $\{1, 2, 3\}$)

(5) The equation $g(x) = y$ has at most one solution for every y in the codomain of g. — False $g(1) = g(3/2) = 2$

(6) g is surjective — True: exactly the same as (4)

(7) g is injective — False: exactly the same as (5)

Proving that a Function is Injective

Example 2.8

The function $f : \mathbb{R} \to \mathbb{R}$, defined by $f(x) = x^2 - 4x + 1$ is neither injective nor surjective. Let $X = \{x \in \mathbb{R} : x \geq 2\}$. If we define $g : X \to \mathbb{R}$ by $g(x) = x^2 - 4x + 1$ then g is injective.

Proving that a Function is Injective

Example 2.8

The function $f : \mathbb{R} \to \mathbb{R}$, defined by $f(x) = x^2 - 4x + 1$ is neither injective nor surjective. Let $X = \{x \in \mathbb{R} : x \geq 2\}$. If we define $g : X \to \mathbb{R}$ by $g(x) = x^2 - 4x + 1$ then g is injective.

In the proof we started by supposing that $f(x) = f(x')$ and finished by deducing that $x = x'$. This fits exactly with the definition of injective. (You can if you prefer, use one of the equivalent definitions seen earlier, **but this way often gives the shortest proofs**.)

Proving that a Function is Injective

Example 2.8

The function $f : \mathbb{R} \to \mathbb{R}$, defined by $f(x) = x^2 - 4x + 1$ is neither injective nor surjective. Let $X = \{x \in \mathbb{R} : x \geq 2\}$. If we define $g : X \to \mathbb{R}$ by $g(x) = x^2 - 4x + 1$ then g is injective.

In the proof we started by supposing that $f(x) = f(x')$ and finished by deducing that $x = x'$. This fits exactly with the definition of injective. (You can if you prefer, use one of the equivalent definitions seen earlier, **but this way often gives the shortest proofs**.)

A bijective function is also called a *bijection*.

Exercise 2.9

Let $X = \{x \in \mathbb{R} : x \geq 2\}$. What subset Y of $\mathbb{R}$ should you choose so that the function $h : X \to Y$ defined by $h(x) = x^2 - 4x + 1$ is a bijection?

Inverse Functions

Suppose that $f : X \to Y$ is a bijection. As remarked at the top of page 14, for each $y \in Y$ there exists a unique $x \in X$ such that $f(x) = y$.

We define the *inverse function to f* to be the function $f^{-1} : Y \to X$ which sends $y \in Y$ to the unique $x \in X$ such that $f(x) = y$. In symbols

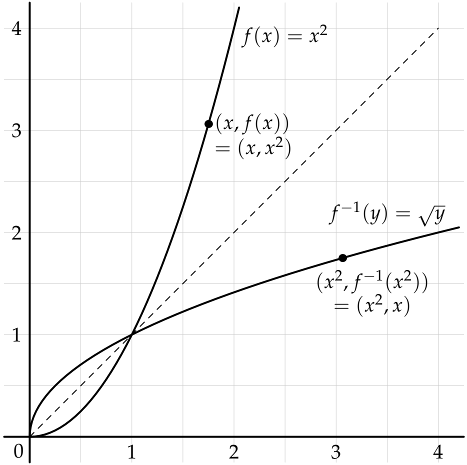
$$f^{-1}(y) = x \iff f(x) = y.$$

Exercise 2.10

Suppose that $f : X \to Y$ is represented by a diagram, as in Example 2.6. How can you obtain the diagram representing the inverse function $f^{-1} : Y \to X$? [*Hint: a complete answer can be given in four words.*]

Graph of a Bijective Function and its Inverse

Let $\mathbb{R}_{\geq 0} = \{x \in \mathbb{R} : x \geq 0\}$. The graph below shows the function $f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ defined by $f(x) = x^2$. The inverse function to f is $f^{-1}(y) = \sqrt{y}$.



Further Examples of Inverse Functions

Example 2.11

Let $Y = \{y \in \mathbb{R} : 0 \leq y < 2\}$. Let $f : \mathbb{R}_{\geq 0} \to Y$ be the function defined by $h(x) = 2x/(1+x)$. For $y \in Y$ we have

$$\frac{2x}{1+x} = y \iff y + xy = 2x \iff y = x(2-y) \iff \frac{y}{2-y} = x.$$

Hence $f(x) = y \iff x = y/(2-y)$. Since $y \geq 0$ and $2 - y > 0$, the solution $x = y/(2-y)$ is in the domain $\mathbb{R}_{\geq 0}$ of h.

Therefore f is a bijection with inverse $f^{-1}(y) = y/(2-y)$.

Further Examples of Inverse Functions

Example 2.11

Let $Y = \{y \in \mathbb{R} : 0 \leq y < 2\}$. Let $f : \mathbb{R}_{\geq 0} \to Y$ be the function defined by $h(x) = 2x/(1+x)$. For $y \in Y$ we have

$$\frac{2x}{1+x} = y \iff y + xy = 2x \iff y = x(2-y) \iff \frac{y}{2-y} = x.$$

Hence $f(x) = y \iff x = y/(2-y)$. Since $y \geq 0$ and $2 - y > 0$, the solution $x = y/(2-y)$ is in the domain $\mathbb{R}_{\geq 0}$ of h.

Therefore f is a bijection with inverse $f^{-1}(y) = y/(2-y)$.

Example 2.12

Let $Y = \{y \in \mathbb{R} : -1 \leq y \leq 1\}$. Consider $\sin : \mathbb{R} \to Y$. This function is not bijective, because it is not injective. For example, $\sin 0 = \sin 2\pi = 1$. To find an inverse we must first restrict the domain.

Composing Functions

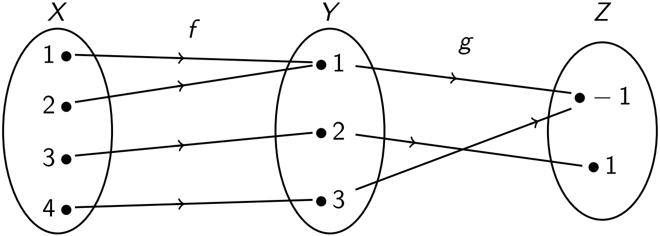
Let $f : X \to Y$ and $g : Y \to Z$ be functions. The *composition of f and g* is the function $gf : X \to Z$, defined by

$$(gf)(x) = g\big(f(x)\big).$$

Note that gf means 'do f, then do g'. One has to get used to reading function compositions from right to left.

Example 2.13

Let $f : \{1,2,3,4\} \to \{1,2,3\}$ be the function f_1 from Example 2.6. Let $g : \{1,2,3\} \to \{-1,1\}$ be defined by $g(x) = (-1)^x$.



Composing Functions

Lemma 2.14 (Examinable)

Let $f : X \to Y$ and $g : Y \to Z$ be functions.

(i) *If f and g are injective then gf is injective.*

(ii) *If f and g are surjective then gf is surjective.*

(iii) *If f and g are bijective then gf is bijective.*

For (ii) see Question 5(a) on Sheet 2.

- Please put your answers to Sheet 2 in the box as it comes around.

- Please take pages 19 to 22 of the printed notes and Sheet 3.

- Your work is marked out of 10, with a further 0/1 mark for 'making a reasonable attempt'. The 0/1 mark is the only one that counts for examination credit. Not all questions will be marked: please see the lecturer after a lecture or in an office hour to go through them.

- Please get copies of any handouts you missed from Moodle. Here is a direct link:

  `http://moodle.rhul.ac.uk/course/view.php?id=407`.

  Even if you are not registered for the course you still have access to this page.

- In future weeks, work will be returned at the Solutions Class on Friday 11am in BLT1.

Inverse of a Composition of Functions

By (c), if $f : X \to Y$ and $g : Y \to Z$ are bijections, then $gf : X \to Z$ is a bijection, and so it has an inverse function. To undo the composition $gf : X \to Z$ we must first undo $g : Y \to Z$, then undo $f : X \to Y$. Hence

$$(gf)^{-1} = f^{-1}g^{-1}.$$

This result can be useful when finding inverse functions.

Example 2.15

Let

$$f(x) = \sqrt{\frac{2x^2}{1+x^2}}.$$

We can write f as a composition: $f = f_3f_2f_1$ where $f_1(x) = x^2$, $f_2(x) = 2x/(1+x)$ and $f_3(x) = \sqrt{x}$. In the lecture we will sort out the domains and codomains of f and f_1, f_2, f_3, and hence find the inverse to f.

Associativity and Identity Functions

The *associative property of composition* states that if $f : X \to Y$, $g : Y \to Z$ and $h : Z \to W$ are any functions then

$$(hg)f = h(gf) : X \to W.$$

This has a one-line proof.

We will see associativity again in §10 of the course on rings.

Associativity and Identity Functions

The *associative property of composition* states that if $f : X \to Y$, $g : Y \to Z$ and $h : Z \to W$ are any functions then

$$(hg)f = h(gf) : X \to W.$$

This has a one-line proof.

We will see associativity again in §10 of the course on rings.

Suppose $f : X \to Y$ is a bijection. We have seen that f has an inverse function $f^{-1} : Y \to X$, with the defining property

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

What happens when we compose f and f^{-1}?

The *identity* function on a set X is the function $\mathrm{id}_X : X \to X$ defined by $\mathrm{id}_X(x) = x$ for all $x \in X$.

§3 Complex Numbers

Definition 3.1

A *complex number* is defined to be a symbol of the form $a + bi$ where $a, b \in \mathbb{R}$. If $z = a + bi$ then we say that a is the *real part* of z, and b is the *imaginary part of z*, and write $\mathrm{Re}\, z = a$, $\mathrm{Im}\, z = b$. We write $\mathbb{C}$ for the set of all complex numbers.

Please interpret the ‘complex’ in complex number as meaning ‘made of more than one part’, rather than ‘difficult’. The word ‘imaginary’ is also standard—please do not be put off by it.

Exercise 3.2

Calculate $(1 + i)^3$.

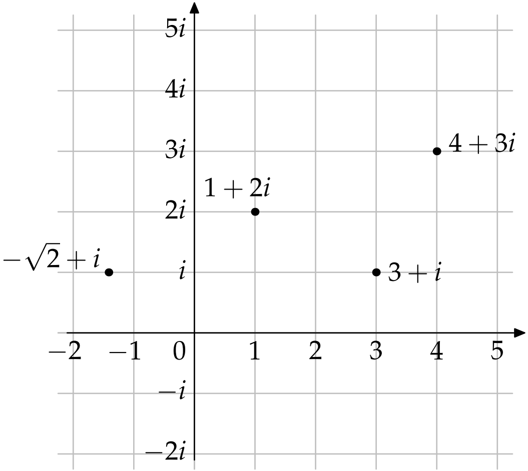
Adding, Subtracting and Multiplying in $\mathbb{C}$

The rules for adding, multiplying and subtracting complex numbers follow from the property that $i^2 = -1$. If $a + bi$ and $c + di \in \mathbb{C}$ are complex numbers in Cartesian form then

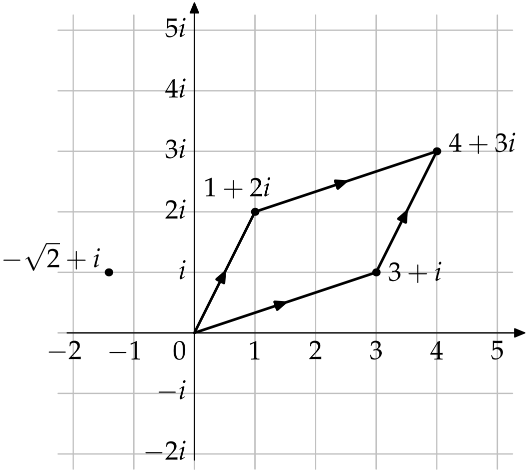
$$\begin{aligned} (a + bi) + (c + di) &= (a + c) + (b + d)i \\ (a + bi) - (c + di) &= (a - c) + (b - d)i \\ (a + bi)(c + di) &= (ac - bd) + (ad + bc)i. \end{aligned}$$

So the set $\mathbb{C}$ of complex numbers is closed under addition, subtraction and multiplication. To see that the complex numbers are also closed under division, it is useful to think about them geometrically.

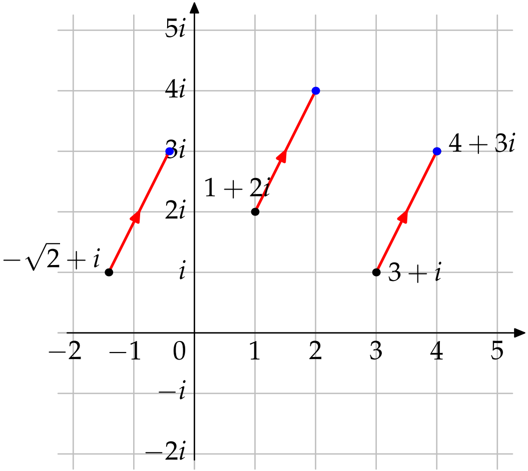
Argand Diagram



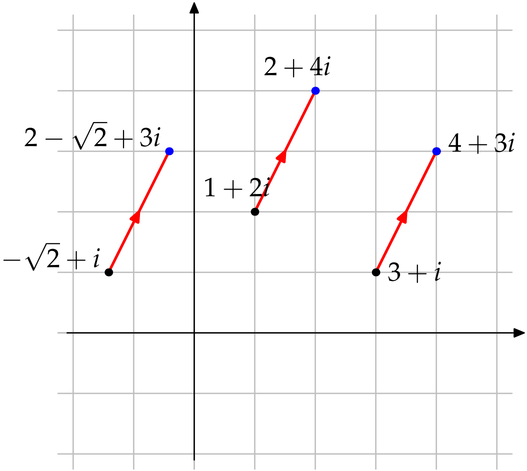
Argand Diagram



Argand Diagram: Adding $1 + 2i$



Argand Diagram: Adding $1 + 2i$



Complex Conjugate and Modulus

We define the *modulus* of z, written $|z|$, to be $\sqrt{a^2 + b^2}$. We define the *complex conjugate* of z, written $\overline{z}$, to be $a - bi$.

We read $|z|$ as 'mod z' and $\overline{z}$ as 'z bar'.

Lemma 3.4 (Examinable)

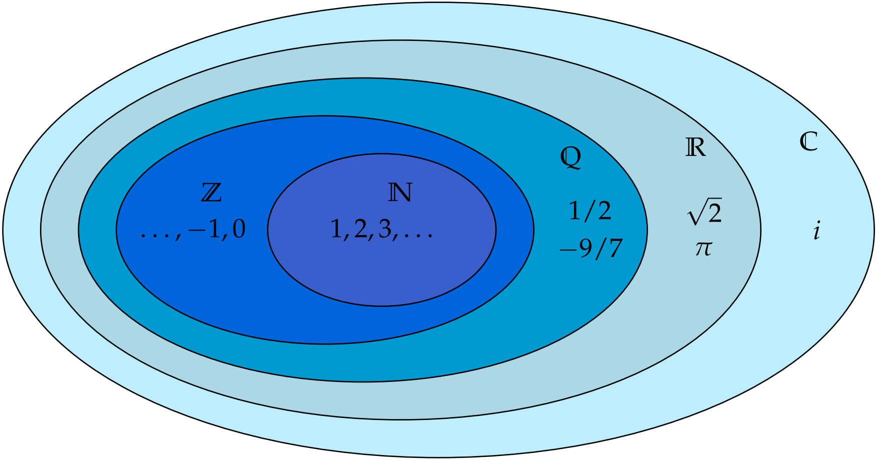
Let $z \in \mathbb{C}$. Then

(a) $|z|^2 = z\overline{z}$.

(b) *If $z \neq 0$ then $1/z = \overline{z}/|z|^2$.*

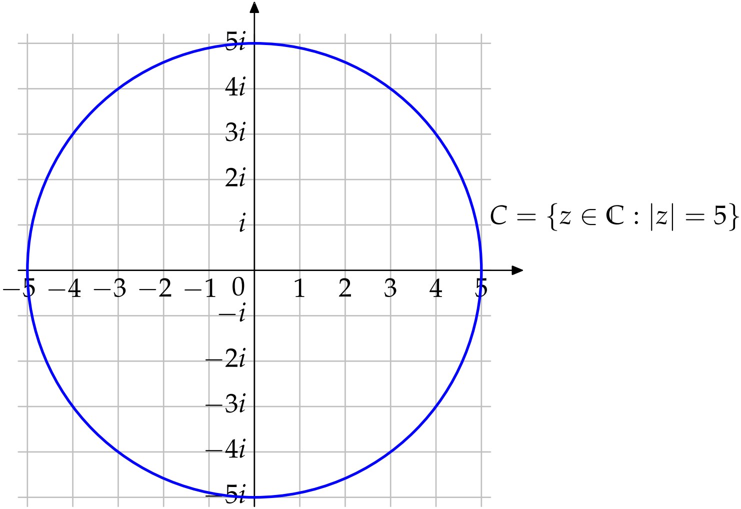
(c) *The set $\mathbb{C}$ of complex numbers is closed under division.*

Number Systems So Far



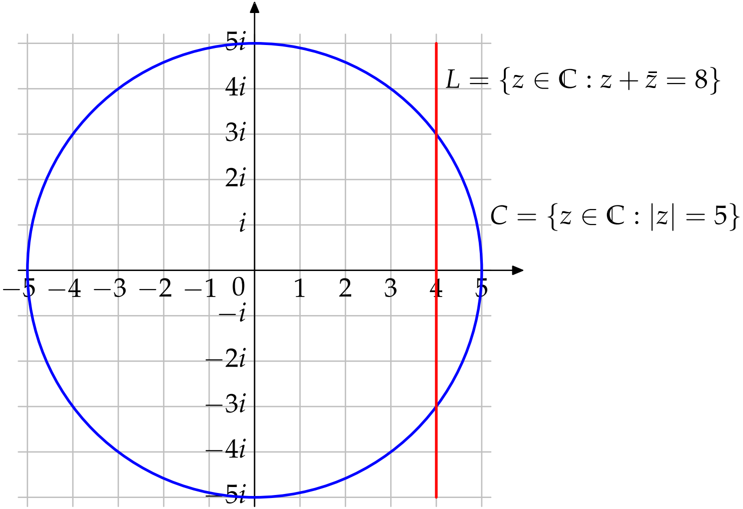
Example 3.5(2): Equation Solving in $\mathbb{C}$

Consider the simultaneous equations $|z| = 5$ and $z + \overline{z} = 8$.



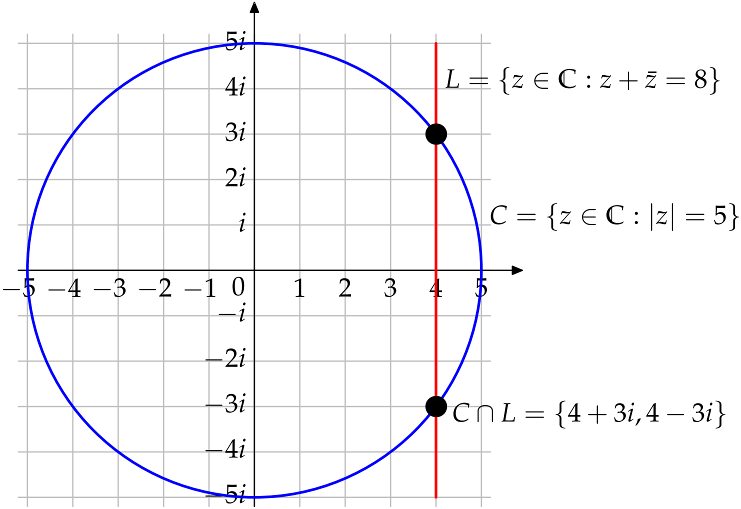
Example 3.5(2): Equation Solving in $\mathbb{C}$

Consider the simultaneous equations $|z| = 5$ and $z + \overline{z} = 8$.



Example 3.5(2): Equation Solving in $\mathbb{C}$

Consider the simultaneous equations $|z| = 5$ and $z + \overline{z} = 8$.


$L = \{z \in \mathbb{C} : z + \bar{z} = 8\}$
$C = \{z \in \mathbb{C} : |z| = 5\}$
$C \cap L = \{4 + 3i, 4 - 3i\}$
$5i$
$4i$
$3i$
$2i$
i
$-i$
$-2i$
$-3i$
$-4i$
$-5i$
-5
-4
-3
-2
-1
0
1
2
3
4
5

Pre-lecture Quiz (Friday 18th October)

Which complex number below is equal to $1/(1-i)$?

(A) $1+i$ (B) $\frac{1}{2}+\frac{i}{2}$ (C) $-1+i$ (D) $\frac{-1}{2}+\frac{i}{2}$.

The number of solutions to the simultaneous equations

$$\operatorname{Im} z = 1 \quad \text{and} \quad |z| = 2$$

is

(A) 0 (B) 1 (C) 2 (D) 3.

Please collect your work at the end of this lecture, if you have not already done so. The model answers on Moodle to Sheet 2 have been updated with some common errors.

(Uncollected work festers in the box outside C240, demoralizing everyone and making the department look untidy.)

Polar Form and Arguments

Any complex number z can be written in the form

$$z = r(\cos\theta + i\sin\theta)$$

where $r \in \mathbb{R}_{\geq 0}$ and θ is an angle, measured in radians. This is called the *polar form* of z. Observe that $r = |z|$. We say that θ is an *argument* of z.

Example 3.6 (See board)

Polar Form and Arguments

Any complex number z can be written in the form

$$z = r(\cos\theta + i\sin\theta)$$

where $r \in \mathbb{R}_{\geq 0}$ and θ is an angle, measured in radians. This is called the *polar form* of z. Observe that $r = |z|$. We say that θ is an *argument* of z.

Example 3.6 (See board)

Definition 3.7

Let $z \in \mathbb{C}$ be non-zero. If $z = r(\cos\theta + i\sin\theta)$ where $-\pi < \theta \leq \pi$, then we say that θ is the *principal argument* of z, and write $\theta = \mathrm{Arg}(z)$.

Quiz: What is the domain of the function Arg?

Polar Form and Arguments

Any complex number z can be written in the form

$$z = r(\cos\theta + i\sin\theta)$$

where $r \in \mathbb{R}_{\geq 0}$ and θ is an angle, measured in radians. This is called the *polar form* of z. Observe that $r = |z|$. We say that θ is an *argument* of z.

Example 3.6 (See board)

Definition 3.7

Let $z \in \mathbb{C}$ be non-zero. If $z = r(\cos\theta + i\sin\theta)$ where $-\pi < \theta \leq \pi$, then we say that θ is the *principal argument* of z, and write $\theta = \operatorname{Arg}(z)$.

Quiz: What is the domain of the function Arg?

Arg is a function with domain $\{z \in \mathbb{C} : z \neq 0\}$ and codomain $\{\theta \in \mathbb{R} : -\pi < \theta \leq \pi\}$.

Polar Form and Arguments

Any complex number z can be written in the form

$$z = r(\cos\theta + i\sin\theta)$$

where $r \in \mathbb{R}_{\geq 0}$ and θ is an angle, measured in radians. This is called the *polar form* of z. Observe that $r = |z|$. We say that θ is an *argument* of z.

Example 3.6 (See board)

Definition 3.7

Let $z \in \mathbb{C}$ be non-zero. If $z = r(\cos\theta + i\sin\theta)$ where $-\pi < \theta \leq \pi$, then we say that θ is the *principal argument* of z, and write $\theta = \mathrm{Arg}(z)$.

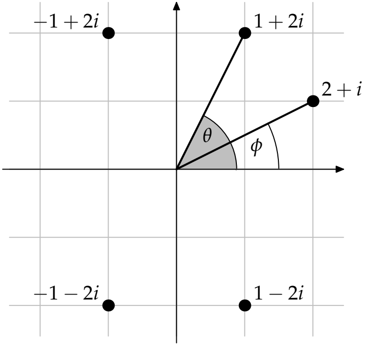
Quiz: What is the domain of the function Arg?

Arg is a function with domain $\{z \in \mathbb{C} : z \neq 0\}$ and codomain $\{\theta \in \mathbb{R} : -\pi < \theta \leq \pi\}$. Is it injective? Is it surjective?

Principal Arguments

Example 3.8

We will find the principal arguments of the complex numbers shown on the Argand diagram below in terms of the angles θ and ϕ.



There is an often misapplied 'rule' that $\text{Arg}(a+bi) = \tan^{-1}(b/a)$. **This only works when $a > 0$.**

Multiplication (and Division) in Polar Form

Example 3.9

Let $z = r(\cos\theta + i\sin\theta)$ and $w = s(\cos\phi + i\sin\phi)$ be complex numbers in polar form. Using the formulae

$$\cos(\theta + \phi) = \cos\theta\cos\phi - \sin\theta\sin\phi$$
$$\sin(\theta + \phi) = \cos\theta\sin\phi + \sin\theta\cos\phi$$

it follows that

$$zw = rs\bigl(\cos(\theta + \phi) + i\sin(\theta + \phi)\bigr).$$

In short: to multiply numbers in polar form, multiply the moduli and add the arguments.

Exercise 3.10

Let z and w be as in Example 3.10 and suppose that $w \neq 0$. Express z/w in polar form.

De Moivre's Theorem

If $\theta \in \mathbb{R}$ and $n \in \mathbb{N}$ then

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

De Moivre's Theorem can be proved using mathematical induction and Example 3.10. We will shortly see a quicker proof, using the exponential function.

Example 3.11

The $n = 3$ case of De Moivre's Theorem implies that

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta$$

De Moivre's Theorem

If $\theta \in \mathbb{R}$ and $n \in \mathbb{N}$ then

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

De Moivre's Theorem can be proved using mathematical induction and Example 3.10. We will shortly see a quicker proof, using the exponential function.

Example 3.11

The $n = 3$ case of De Moivre's Theorem implies that

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta$$

So we proved an identity about the **real** cosine function, $\cos : \mathbb{R} \to \mathbb{R}$ using **complex** numbers.

> *Il apparut que, entre deux vérités du domaine réel, le chemin le plus facile et le plus court passe bien souvent par le domaine complexe*
>
> Paul Painlevé (1900)

De Moivre's Theorem

If $\theta \in \mathbb{R}$ and $n \in \mathbb{N}$ then

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

De Moivre's Theorem can be proved using mathematical induction and Example 3.10. We will shortly see a quicker proof, using the exponential function.

Example 3.11

The $n = 3$ case of De Moivre's Theorem implies that

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta$$

So we proved an identity about the **real** cosine function, $\cos : \mathbb{R} \to \mathbb{R}$ using **complex** numbers.

> *It came to appear that, between two truths of the real domain, the easiest and shortest path quite often passes through the complex domain.*
>
> Paul Painlevé (1900)

A Cubic Equation

Example 3.12

Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^3 - 12x - 8$. [**changed from** $+8$ **to** -8 **in lecture to make end a bit nicer**.] If we substitute $x = 4\cos\theta$ then some rearranging shows that $f(x) = 0$ if and only if $\cos 3\theta = \frac{1}{2}$. By Example 3.7 we know that $\theta = \frac{\pi}{9}$ is one solution. There are two more, giving as the full set of roots

$$4\cos\tfrac{\pi}{9}, \quad 4\cos\tfrac{7\pi}{9}, \quad 4\cos\tfrac{13\pi}{9}.$$

Exercise: by drawing the graph for cos, and using Example 3.6, show that $\cos 3\theta = \frac{1}{2} \iff 3\theta = \pm\pi/3 + 2n\pi$ for some $n \in \mathbb{Z}$. Deduce that the roots of f are

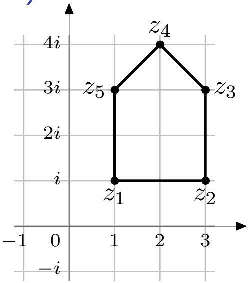
$$4\cos\tfrac{\pi}{9}, \quad 4\cos\tfrac{7\pi}{9}, \quad 4\cos\tfrac{13\pi}{9}.$$

Further Exercise: sketch the graph of f and label the roots correctly. Include the coordinates of the turning points.

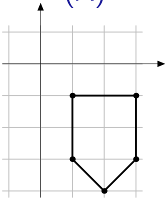
Pre-lecture Quiz (Thursday 24th October)

The Argand diagram to the right shows $z_1, z_2, z_3, z_4, z_5 \in \mathbb{C}$.

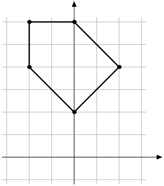
What is $|z_3 - z_1|$?



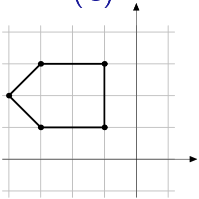
(A)



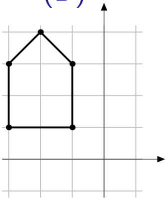
(B)



(C)



(D)



The diagrams above are drawn with the same scale.

Which diagram shows $iz_1, iz_2, iz_3, iz_4, iz_5$?

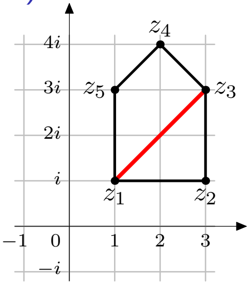
Which diagram shows $\overline{z_1}, \overline{z_2}, \overline{z_4}, \overline{z_4}, \overline{z_5}$?

Pre-lecture Quiz (Thursday 24th October)

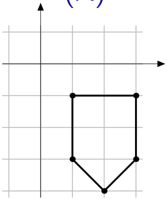
The Argand diagram to the right shows $z_1, z_2, z_3, z_4, z_5 \in \mathbb{C}$.

What is $|z_3 - z_1|$?

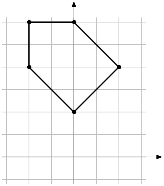
Answer: $|z_3 - z_1| = 2\sqrt{2}$. Geometrically, $|z_3 - z_1|$ is the length of the red line.



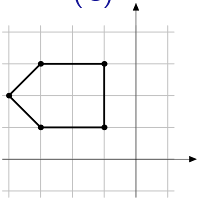
(A)



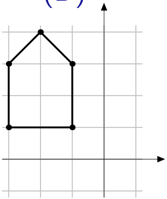
(B)



(C)



(D)



The diagrams above are drawn with the same scale.

Which diagram shows $iz_1, iz_2, iz_3, iz_4, iz_5$?

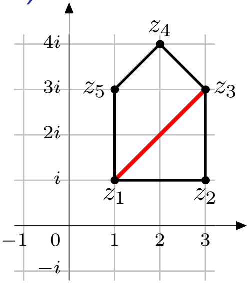
Which diagram shows $\overline{z_1}, \overline{z_2}, \overline{z_4}, \overline{z_4}, \overline{z_5}$?

Pre-lecture Quiz (Thursday 24th October)

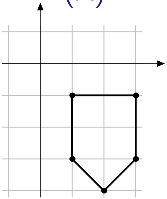
The Argand diagram to the right shows $z_1, z_2, z_3, z_4, z_5 \in \mathbb{C}$.

What is $|z_3 - z_1|$?

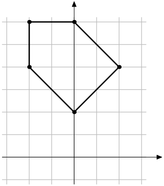
Answer: $|z_3 - z_1| = 2\sqrt{2}$. Geometrically, $|z_3 - z_1|$ is the length of the red line.



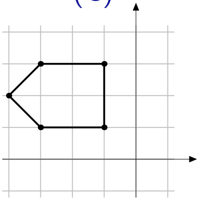
(A)



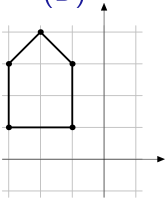
(B)



(C)



(D)



The diagrams above are drawn with the same scale.

Which diagram shows $iz_1, iz_2, iz_3, iz_4, iz_5$? Answer: (C)

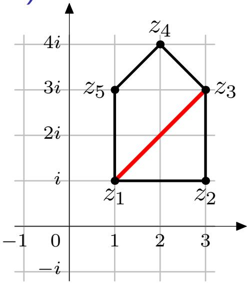
Which diagram shows $\overline{z_1}, \overline{z_2}, \overline{z_4}, \overline{z_4}, \overline{z_5}$?

Pre-lecture Quiz (Thursday 24th October)

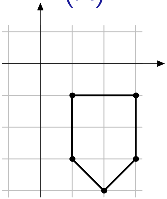
The Argand diagram to the right shows $z_1, z_2, z_3, z_4, z_5 \in \mathbb{C}$.

What is $|z_3 - z_1|$?

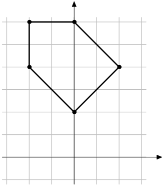
Answer: $|z_3 - z_1| = 2\sqrt{2}$. Geometrically, $|z_3 - z_1|$ is the length of the red line.



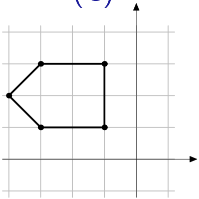
(A)



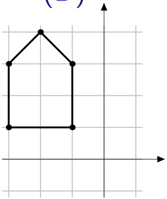
(B)



(C)



(D)

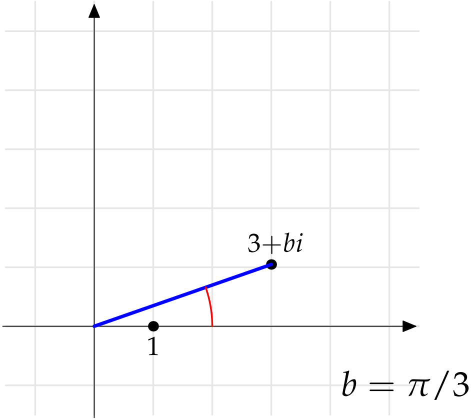


The diagrams above are drawn with the same scale.

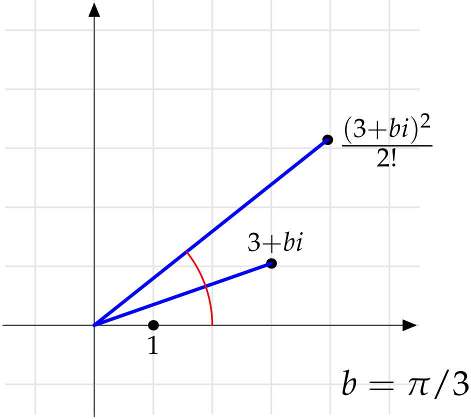
Which diagram shows $iz_1, iz_2, iz_3, iz_4, iz_5$? Answer: (C)

Which diagram shows $\overline{z_1}, \overline{z_2}, \overline{z_4}, \overline{z_4}, \overline{z_5}$? Answer: (A)

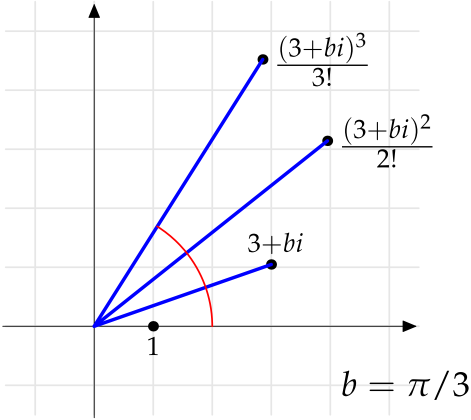
Summands in the Infinite Sum for $e^{3+\pi i/3}$



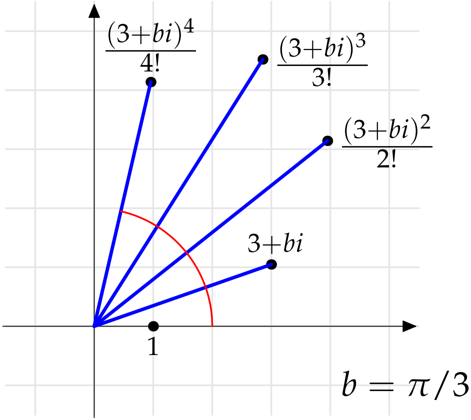
Summands in the Infinite Sum for $e^{3+\pi i/3}$



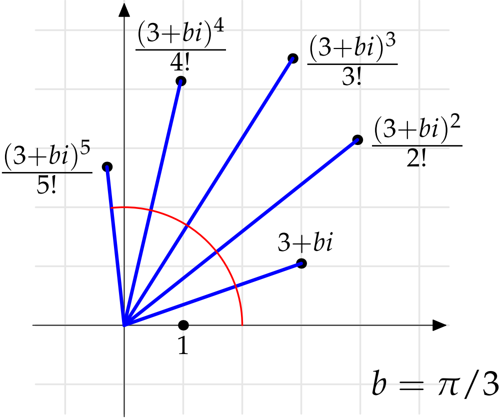
Summands in the Infinite Sum for $\mathrm{e}^{3+\pi i/3}$



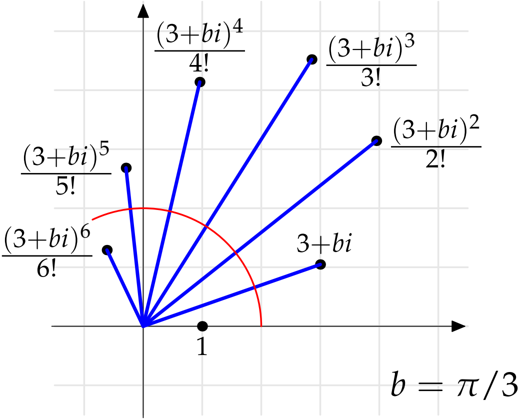
Summands in the Infinite Sum for $e^{3+\pi i/3}$



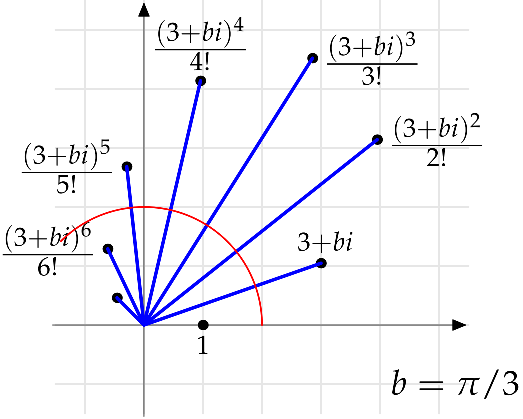
Summands in the Infinite Sum for $e^{3+\pi i/3}$



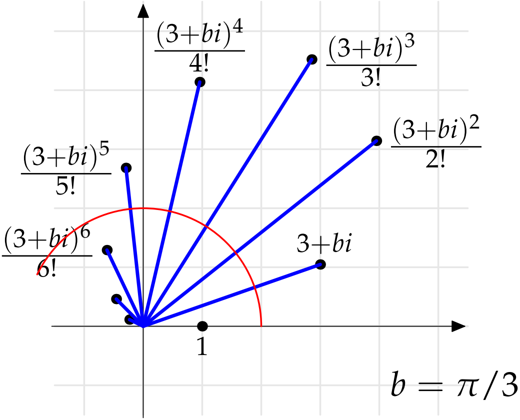
Summands in the Infinite Sum for $\mathrm{e}^{3+\pi i/3}$



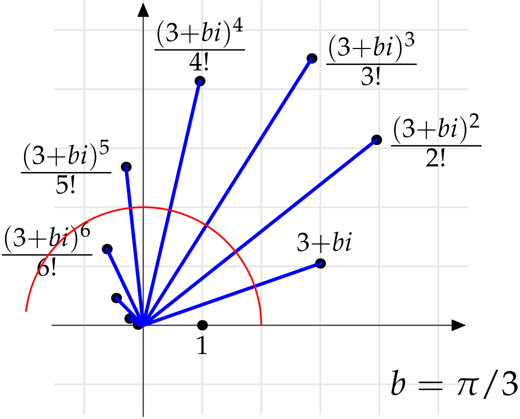
Summands in the Infinite Sum for $e^{3+\pi i/3}$



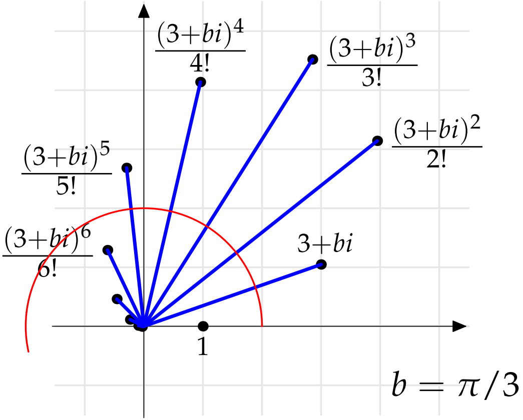
Summands in the Infinite Sum for $e^{3+\pi i/3}$



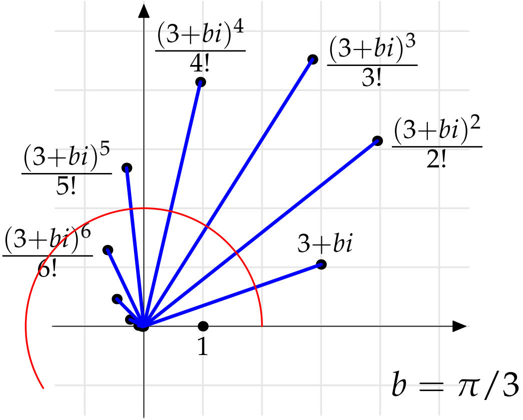
Summands in the Infinite Sum for $e^{3+\pi i/3}$



Summands in the Infinite Sum for $\mathrm{e}^{3+\pi i/3}$



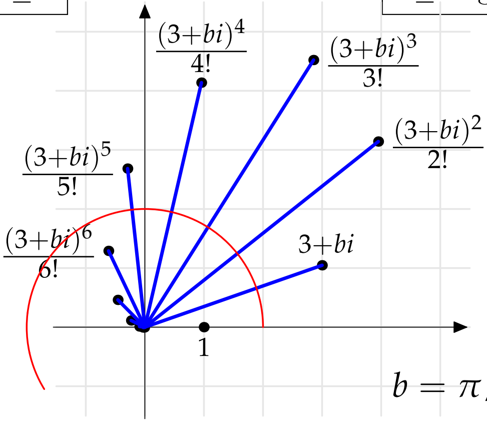
Summands in the Infinite Sum for $e^{3+\pi i/3}$



Summands in the Infinite Sum for $e^{3+\pi i/3}$

$\pi/2 \leq \operatorname{Arg}(w) \leq \pi$

$0 \leq \operatorname{Arg}(w) \leq \pi/2$

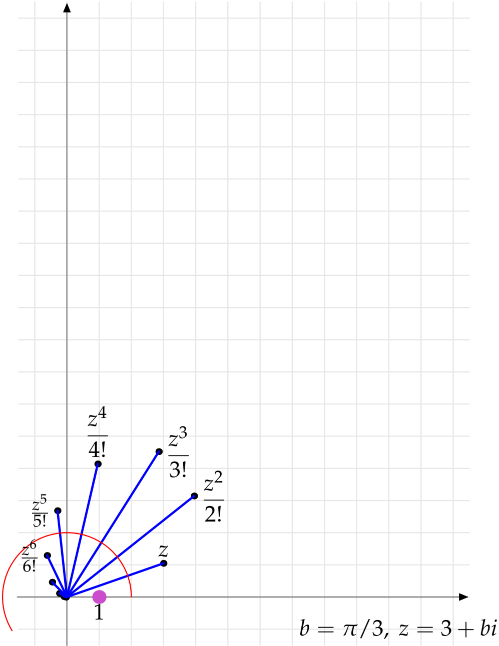


$b = \pi/3$

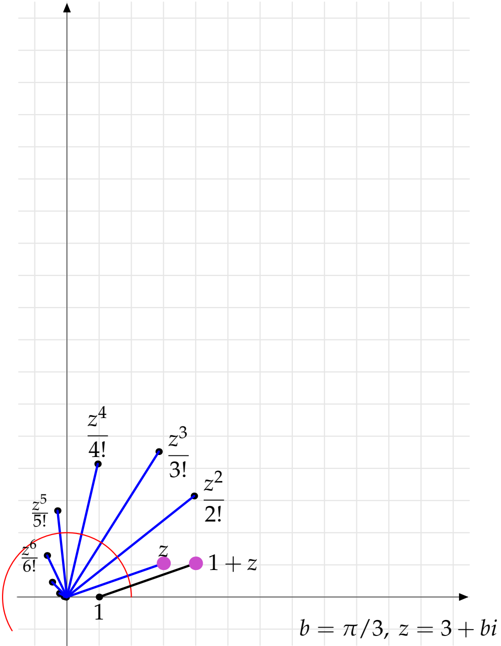
$-\pi < \operatorname{Arg}(w) \leq -\pi/2$

$-\pi/2 \leq \operatorname{Arg}(w) \leq 0$

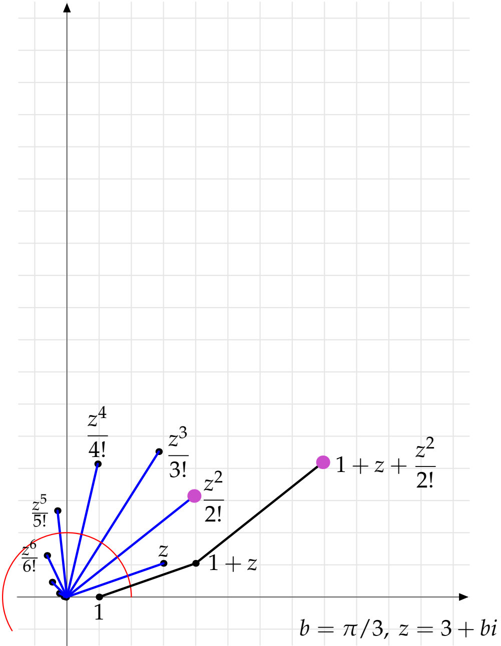
Infinite Sum for $e^{3+\pi i/3}$



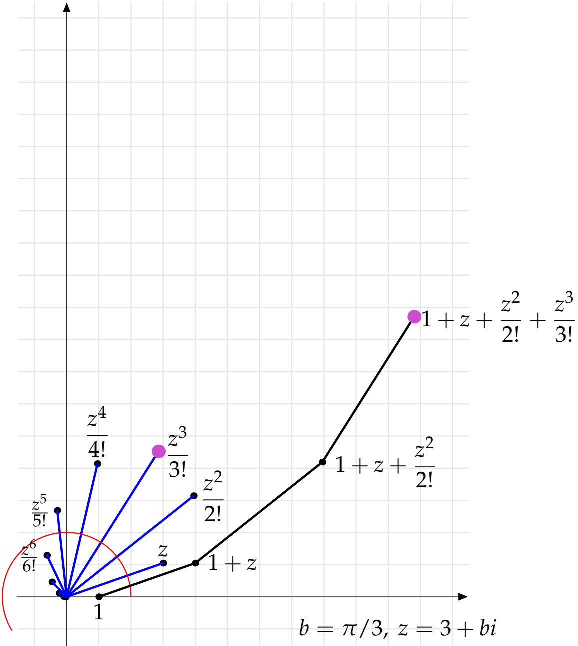
Infinite Sum for $\mathrm{e}^{3+\pi i/3}$



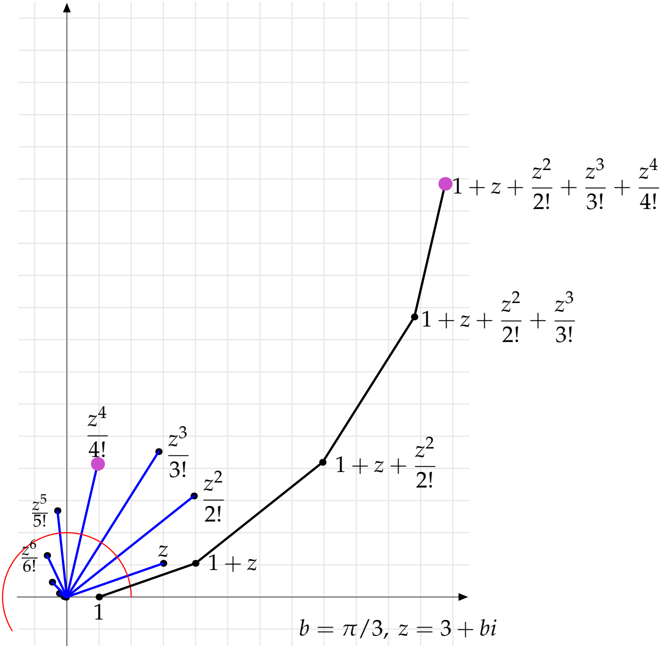
Infinite Sum for $\mathrm{e}^{3+\pi i/3}$



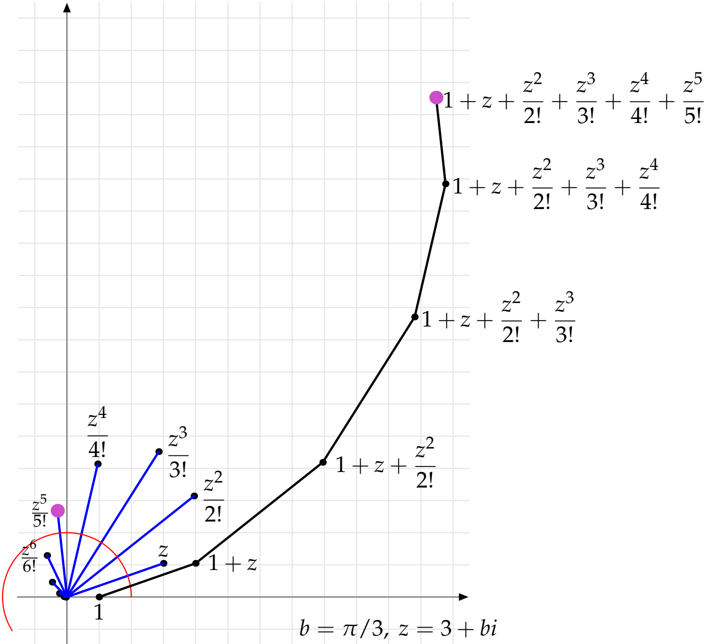
Infinite Sum for $\mathrm{e}^{3+\pi i/3}$



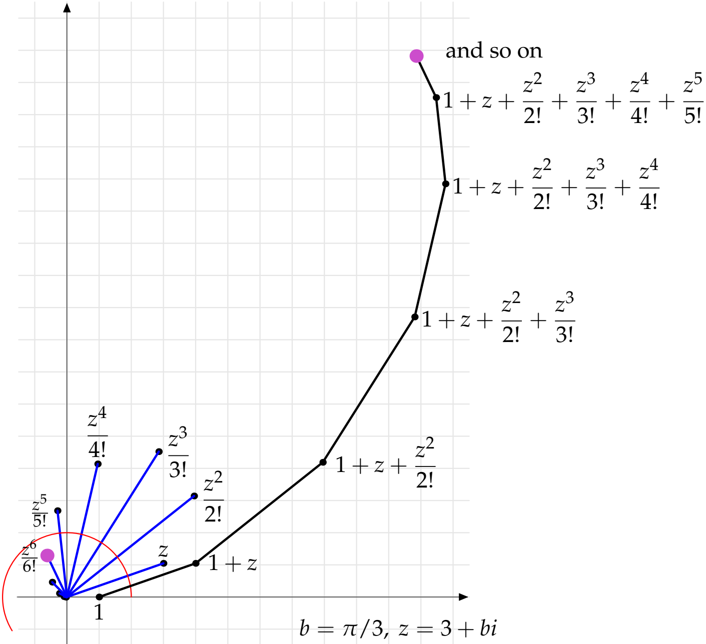
Infinite Sum for $\mathrm{e}^{3+\pi i/3}$



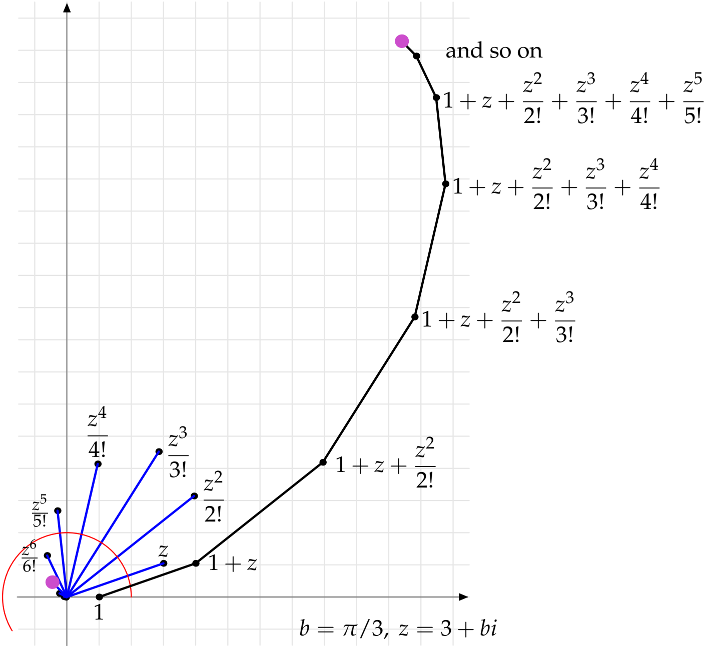
Infinite Sum for $\mathrm{e}^{3+\pi i/3}$


$1+z+\frac{z^2}{2!}+\frac{z^3}{3!}+\frac{z^4}{4!}+\frac{z^5}{5!}$
$1+z+\frac{z^2}{2!}+\frac{z^3}{3!}+\frac{z^4}{4!}$
$1+z+\frac{z^2}{2!}+\frac{z^3}{3!}$
$1+z+\frac{z^2}{2!}$
$1+z$
1
$\frac{z^4}{4!}$
$\frac{z^3}{3!}$
$\frac{z^2}{2!}$
z
$\frac{z^5}{5!}$
$\frac{z^6}{6!}$
$b=\pi/3,\ z=3+bi$

Infinite Sum for $e^{3+\pi i/3}$

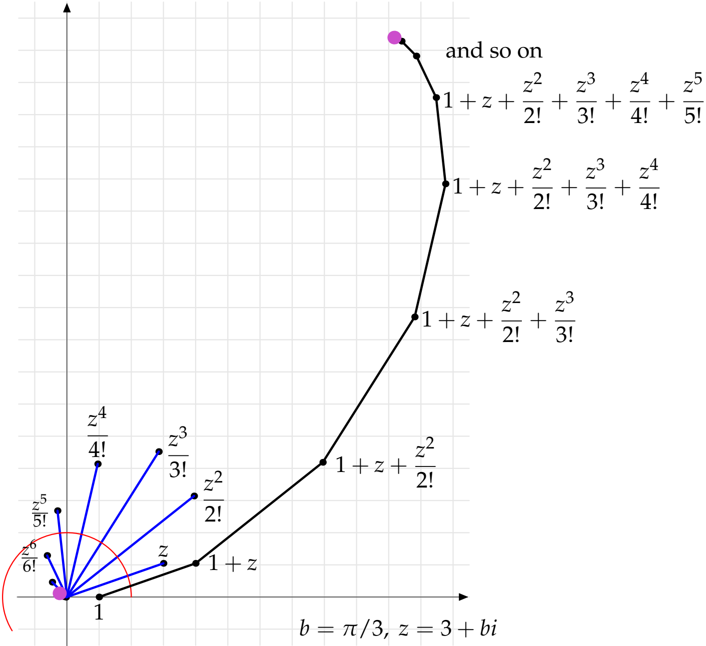

and so on
$1+z+\frac{z^2}{2!}+\frac{z^3}{3!}+\frac{z^4}{4!}+\frac{z^5}{5!}$
$1+z+\frac{z^2}{2!}+\frac{z^3}{3!}+\frac{z^4}{4!}$
$1+z+\frac{z^2}{2!}+\frac{z^3}{3!}$
$1+z+\frac{z^2}{2!}$
$1+z$
1
z
$\frac{z^2}{2!}$
$\frac{z^3}{3!}$
$\frac{z^4}{4!}$
$\frac{z^5}{5!}$
$\frac{z^6}{6!}$
$b=\pi/3$, $z=3+bi$

Infinite Sum for $e^{3+\pi i/3}$

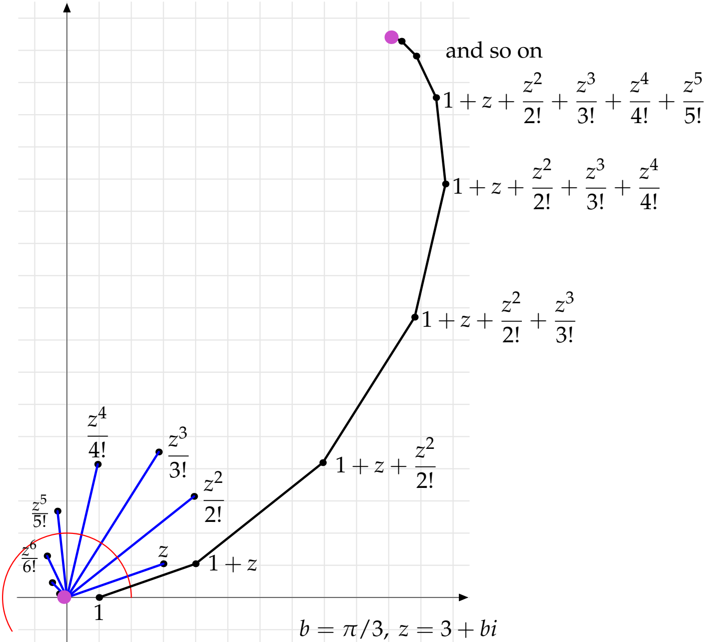


and so on
$1 + z + \frac{z^2}{2!} + \frac{z^3}{3!} + \frac{z^4}{4!} + \frac{z^5}{5!}$
$1 + z + \frac{z^2}{2!} + \frac{z^3}{3!} + \frac{z^4}{4!}$
$1 + z + \frac{z^2}{2!} + \frac{z^3}{3!}$
$1 + z + \frac{z^2}{2!}$
$1 + z$
1
$\frac{z^4}{4!}$
$\frac{z^3}{3!}$
$\frac{z^2}{2!}$
z
$\frac{z^5}{5!}$
$\frac{z^6}{6!}$
$b = \pi/3$, $z = 3 + bi$

Infinite Sum for $\mathrm{e}^{3+\pi i/3}$

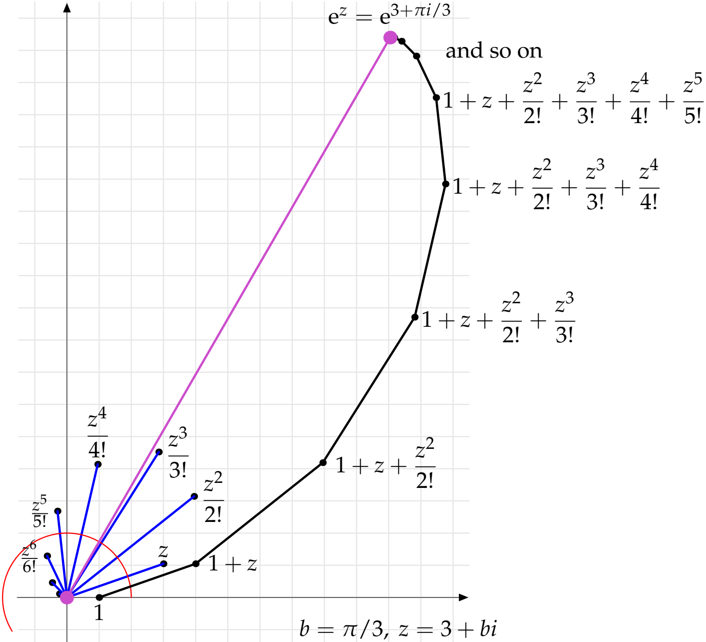

and so on
$1+z+\frac{z^2}{2!}+\frac{z^3}{3!}+\frac{z^4}{4!}+\frac{z^5}{5!}$
$1+z+\frac{z^2}{2!}+\frac{z^3}{3!}+\frac{z^4}{4!}$
$1+z+\frac{z^2}{2!}+\frac{z^3}{3!}$
$1+z+\frac{z^2}{2!}$
$1+z$
$\frac{z^4}{4!}$
$\frac{z^3}{3!}$
$\frac{z^2}{2!}$
$\frac{z^5}{5!}$
z
$\frac{z^6}{6!}$
1
$b=\pi/3$, $z=3+bi$

Infinite Sum for $\mathrm{e}^{3+\pi i/3}$



and so on
$1+z+\frac{z^2}{2!}+\frac{z^3}{3!}+\frac{z^4}{4!}+\frac{z^5}{5!}$
$1+z+\frac{z^2}{2!}+\frac{z^3}{3!}+\frac{z^4}{4!}$
$1+z+\frac{z^2}{2!}+\frac{z^3}{3!}$
$1+z+\frac{z^2}{2!}$
$1+z$
1
$\frac{z^4}{4!}$
$\frac{z^3}{3!}$
$\frac{z^2}{2!}$
z
$\frac{z^5}{5!}$
$\frac{z^6}{6!}$
$b=\pi/3,\ z=3+bi$

Infinite Sum for $\mathrm{e}^{3+\pi i/3}$



$\mathrm{e}^z = \mathrm{e}^{3+\pi i/3}$
and so on
$1 + z + \frac{z^2}{2!} + \frac{z^3}{3!} + \frac{z^4}{4!} + \frac{z^5}{5!}$
$1 + z + \frac{z^2}{2!} + \frac{z^3}{3!} + \frac{z^4}{4!}$
$1 + z + \frac{z^2}{2!} + \frac{z^3}{3!}$
$1 + z + \frac{z^2}{2!}$
$1 + z$
1
$\frac{z^4}{4!}$
$\frac{z^3}{3!}$
$\frac{z^2}{2!}$
z
$\frac{z^5}{5!}$
$\frac{z^6}{6!}$
$b = \pi/3,\ z = 3 + bi$

Complex Exponential Function

Definition 3.13

Let $z = a + bi \in \mathbb{C}$ be a complex number in Cartesian form. We define the *complex exponential function* $\exp : \mathbb{C} \to \mathbb{C}$ by

$$\exp(z) = \mathrm{e}^{a}(\cos b + i \sin b).$$

It is fine to write e^{z} for $\exp(z)$.

Complex Exponential Function

Definition 3.13

Let $z = a + bi \in \mathbb{C}$ be a complex number in Cartesian form. We define the *complex exponential function* $\exp : \mathbb{C} \to \mathbb{C}$ by

$$\exp(z) = \mathrm{e}^{a}(\cos b + i \sin b).$$

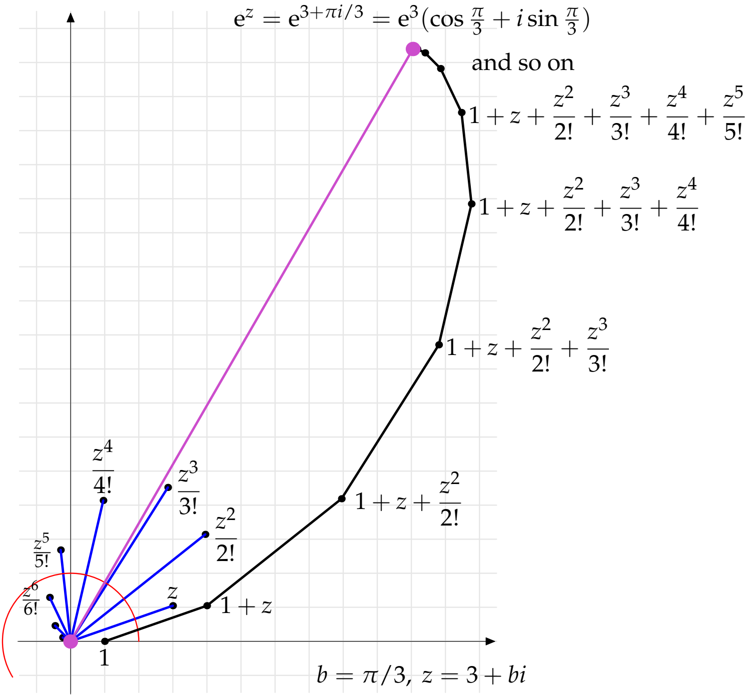
It is fine to write e^{z} for $\exp(z)$.

Exercise 3.14

Show that $\exp(z + w) = \exp z \exp w$ for all complex numbers z and w. [*Hint:* write $z = a + bi$, $w = c + di$ and use Example 3.9.]

A complex number written as $r\mathrm{e}^{i\theta}$ where $r \in \mathbb{R}_{\geq 0}$ and $\theta \in \mathbb{R}$ is said to be in *exponential form*. It is easy to convert between polar and exponential form:

$$z = r(\cos\theta + i\sin\theta) \iff z = r\mathrm{e}^{i\theta}.$$


$e^z = e^{3+\pi i/3} = e^3(\cos\frac{\pi}{3} + i\sin\frac{\pi}{3})$
and so on
$1 + z + \frac{z^2}{2!} + \frac{z^3}{3!} + \frac{z^4}{4!} + \frac{z^5}{5!}$
$1 + z + \frac{z^2}{2!} + \frac{z^3}{3!} + \frac{z^4}{4!}$
$1 + z + \frac{z^2}{2!} + \frac{z^3}{3!}$
$1 + z + \frac{z^2}{2!}$
$1 + z$
$\frac{z^4}{4!}$
$\frac{z^3}{3!}$
$\frac{z^2}{2!}$
$\frac{z^5}{5!}$
z
$\frac{z^6}{6!}$
1
$b = \pi/3,\ z = 3 + bi$

Examples of the Complex Exponential Function

Example 3.15

(1) Put $z = i\pi$ in the complex exponential function. We get $\mathrm{e}^{i\pi} = -1$, or equivalently,

$$\mathrm{e}^{i\pi} + 1 = 0.$$

This is *Euler's Identity*. It relates five fundamental mathematical constants: 0, 1, e, π and i.

Examples of the Complex Exponential Function

Example 3.15

(1) Put $z = i\pi$ in the complex exponential function. We get $\mathrm{e}^{i\pi} = -1$, or equivalently,

$$\mathrm{e}^{i\pi} + 1 = 0.$$

This is *Euler's Identity*. It relates five fundamental mathematical constants: 0, 1, e, π and i.

(2) Let $\theta \in \mathbb{R}$. Put $z = n\theta i$ in the complex exponential funtion to get

$$\cos n\theta + i \sin n\theta = e^{n\theta i} = (e^{\theta i})^n = (\cos\theta + i\sin\theta)^n.$$

This proves De Moivre's Theorem.

Using Exponential Form to Find Roots

The exponential form has the same lack of uniqueness as the polar form:

$$r\mathrm{e}^{i\theta} = s\mathrm{e}^{i\phi} \iff r = s \text{ and } \phi = \theta + 2n\pi \text{ for some } n \in \mathbb{Z}.$$

Example 3.16

See board for solution to equation $z^3 = 8i$.

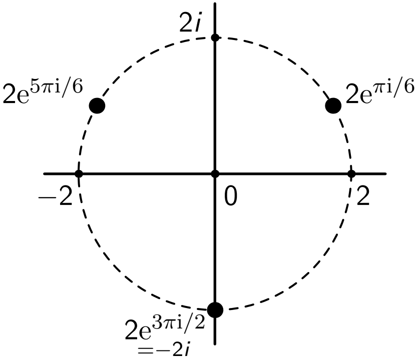
Using Exponential Form to Find Roots

The exponential form has the same lack of uniqueness as the polar form:

$$re^{i\theta} = se^{i\phi} \iff r = s \text{ and } \phi = \theta + 2n\pi \text{ for some } n \in \mathbb{Z}.$$

Example 3.16

See board for solution to equation $z^3 = 8i$.



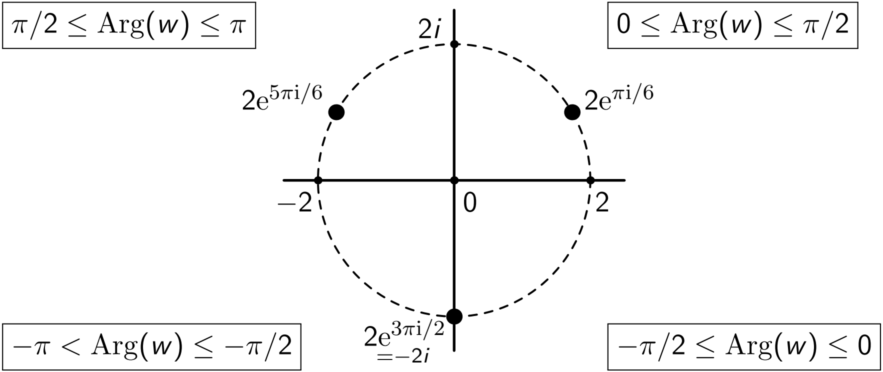
Using Exponential Form to Find Roots

The exponential form has the same lack of uniqueness as the polar form:

$$re^{i\theta} = se^{i\phi} \iff r = s \text{ and } \phi = \theta + 2n\pi \text{ for some } n \in \mathbb{Z}.$$

Example 3.16

See board for solution to equation $z^3 = 8i$.


$\pi/2 \leq \mathrm{Arg}(w) \leq \pi$
$0 \leq \mathrm{Arg}(w) \leq \pi/2$
$2i$
$2e^{5\pi i/6}$
$2e^{\pi i/6}$
-2
0
2
$2e^{3\pi i/2}$
$=-2i$
$-\pi < \mathrm{Arg}(w) \leq -\pi/2$
$-\pi/2 \leq \mathrm{Arg}(w) \leq 0$

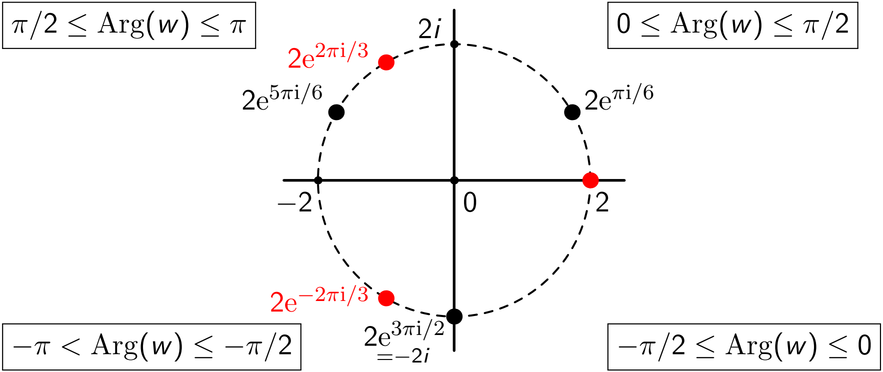
Using Exponential Form to Find Roots

The exponential form has the same lack of uniqueness as the polar form:

$$re^{i\theta} = se^{i\phi} \iff r = s \text{ and } \phi = \theta + 2n\pi \text{ for some } n \in \mathbb{Z}.$$

Example 3.16

See board for solution to equation $z^3 = 8i$.



$\pi/2 \leq \mathrm{Arg}(w) \leq \pi$
$0 \leq \mathrm{Arg}(w) \leq \pi/2$
$2i$
$2e^{2\pi i/3}$
$2e^{5\pi i/6}$
$2e^{\pi i/6}$
-2
0
2
$2e^{-2\pi i/3}$
$2e^{3\pi i/2}$
$=-2i$
$-\pi < \mathrm{Arg}(w) \leq -\pi/2$
$-\pi/2 \leq \mathrm{Arg}(w) \leq 0$

Log of a Complex Number

Let $z = r\mathrm{e}^{i\theta}$ be a complex number in exponential form. If $z = 0$ then there is no $w \in \mathbb{C}$ such that $\mathrm{e}^{w} = z$, since $|\mathrm{e}^{a+bi}| = \mathrm{e}^{a}$ and $e^{a} > 0$ for all $a \in \mathbb{R}$. If $z \neq 0$ then

$$e^{w} = z \iff w = \ln r + (\theta + 2\pi n)i \text{ for some } n \in \mathbb{Z}.$$

Any such number w is called a *logarithm* of z.

Example 3.17

In exponential form $2i = 2\mathrm{e}^{i\pi/2}$. So the set of logarithms of $2i$ is

$$\{\ln 2 + (\frac{\pi}{2} + 2n\pi)i \text{ for some } n \in \mathbb{Z}\}.$$

Log of a Complex Number

Let $z = r\mathrm{e}^{i\theta}$ be a complex number in exponential form. If $z = 0$ then there is no $w \in \mathbb{C}$ such that $\mathrm{e}^{w} = z$, since $|\mathrm{e}^{a+bi}| = \mathrm{e}^{a}$ and $e^{a} > 0$ for all $a \in \mathbb{R}$. If $z \neq 0$ then

$$e^{w} = z \iff w = \ln r + (\theta + 2\pi n)i \text{ for some } n \in \mathbb{Z}.$$

Any such number w is called a *logarithm* of z.

Example 3.17

In exponential form $2i = 2\mathrm{e}^{i\pi/2}$. So the set of logarithms of $2i$ is

$$\left\{\ln 2 + (\frac{\pi}{2} + 2n\pi)i \text{ for some } n \in \mathbb{Z}\right\}.$$

Exercise 3.18

Consider $\exp : \mathbb{C} \to \mathbb{C}$. What are the domain, codomain and range of exp? Is exp surjective? Is exp injective?

Quadratic Equations

You are probably familiar with how to solve quadratic equations over the real numbers. Essentially the same method works over $\mathbb{C}$. Exponential form might be useful for finding square roots.

Lemma 3.19 (Examinable)

Let $a, b, c \in \mathbb{C}$ and suppose that $a \neq 0$. The solutions to the quadratic equation $az^2 + bz + c = 0$ are

$$z = \frac{-b \pm D}{2a}$$

where $D \in \mathbb{C}$ satisfies $D^2 = b^2 - 4ac$.

Quadratic Equations

You are probably familiar with how to solve quadratic equations over the real numbers. Essentially the same method works over $\mathbb{C}$. Exponential form might be useful for finding square roots.

Lemma 3.19 (Examinable)

Let $a, b, c \in \mathbb{C}$ and suppose that $a \neq 0$. The solutions to the quadratic equation $az^2 + bz + c = 0$ are

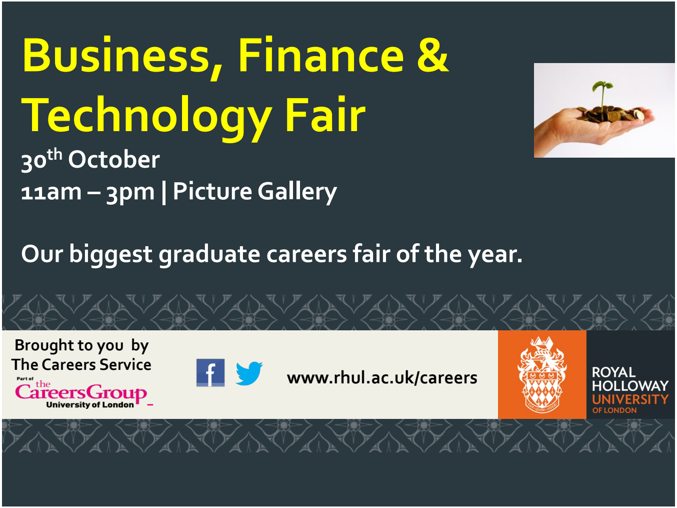
$$z = \frac{-b \pm D}{2a}$$

where $D \in \mathbb{C}$ satisfies $D^2 = b^2 - 4ac$.

Bear in mind that $\sqrt{b^2 - 4ac}$ is ambiguous when $b^2 - 4ac \notin \mathbb{R}_{\geq 0}$. See Bonus Question A on Sheet 3 for one problem this causes.

Administration and Careers Event

- Please take the Part B handout (pages 29 to 36) and Sheet 5.
- Please put your work for Sheet 4 in the box as it goes around.



Business, Finance & Technology Fair

30th October

11am – 3pm | Picture Gallery

Our biggest graduate careers fair of the year.

Brought to you by
The Careers Service
Part of the CareersGroup
University of London

www.rhul.ac.uk/careers

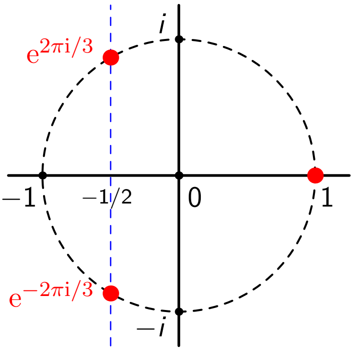
ROYAL
HOLLOWAY
UNIVERSITY
OF LONDON

Example 3.20

Observe that $z^3 - 1 = (z-1)(z^2+z+1)$. So if z is a third root of unity other than 1 then z is a solution of $z^2+z+1=0$. Using Lemma 3.19 we get

$$z = -\frac{1}{2} \pm \frac{\sqrt{3}}{2} i.$$

Since the third roots of unity are 1, $\mathrm{e}^{2\pi i/3}$ and $\mathrm{e}^{4\pi i/3}$, this shows that $\cos\frac{2\pi}{3} = -\frac{1}{2}$ and $\sin\frac{2\pi}{3} = \frac{\sqrt{3}}{2}$.


i
$\mathrm{e}^{2\pi \mathrm{i}/3}$
-1
$-1/2$
0
1
$\mathrm{e}^{-2\pi \mathrm{i}/3}$
$-i$

Fundamental Theorem of Algebra

Theorem 3.21 (Fundamental Theorem of Algebra)

Let $n \in \mathbb{N}$ and let $a_0, a_1, \ldots, a_n \in \mathbb{C}$ with $a_n \neq 0$. Then the equation

$$a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0 = 0$$

has a solution in $\mathbb{C}$.

An Easyish Quartic

Exercise 3.22

Find all solutions to the quartic equation $z^4 + 2z^3 + 3z^2 + 4z + 2 = 0$. (*Hint:* one solution is in $\mathbb{Z}$.)

An Easyish Quartic

Exercise 3.22

Find all solutions to the quartic equation $z^4 + 2z^3 + 3z^2 + 4z + 2 = 0$. (*Hint:* one solution is in $\mathbb{Z}$.)

Solution. Since

$$(-1)^4 + 2(-1)^3 + 3(-1)^2 + 4(-1) + 2 = 0,$$

-1 is a root. So $z - (-1) = z + 1$ is a factor and

$$z^4 + 2z^3 + 3z^2 + 4z + 2 = (z+1)(z^3 + z^2 + 2z + 2).$$

Now -1 is again a root of the cubic $z^3 + z^2 + 2z + 2$, and we get

$$z^3 + z^2 + 2z + 2 = (z+1)(z^2 + 2).$$

Hence

$$z^4 + 2z^3 + 3z^2 + 4z + 2 = (z+1)^2(z^2 + 2)$$

and the roots are -1 (twice), $i\sqrt{2}$ and $-i\sqrt{2}$.

Part B: Natural Numbers and Induction

§4 Induction

A *proposition* is a self-contained statement which is either true or false. For example the statement

There is a real number x such that $x^2 + 1 = 0$

is a false proposition. More briefly, we can write

P : The integers are closed under addition.

This defines P to be the true proposition that the integers are closed under addition. Some statements are too vague or subjective to be considered propositions. For instance:

Q : Houses in Englefield Green are too expensive.

More propositions

We often want to consider statements that depend on the value of a variable. For example, for each $x \in \mathbb{R}$, define

$$P(x): \quad x^2 - 4x + 1 \geq 2.$$

This defines an infinite collection of propositions, one proposition for each real number. Some of these propositions are true, and others are false. For example $P(6)$ and $P(2+\sqrt{5})$ are true, and $P(1)$ is false.

Example 4.1

For $n \in \mathbb{N}$ define

$$Q(n): \quad n^2 + n + 41 \text{ is a prime number}$$

So we have defined propositions

$$\begin{aligned} Q(1)&: \quad 1^2 + 1 + 41 \text{ is a prime number} \\ Q(2)&: \quad 2^2 + 2 + 41 \text{ is a prime number} \\ Q(3)&: \quad 3^2 + 3 + 41 \text{ is a prime number} \end{aligned}$$

and so on. In this case $Q(1), Q(2), \ldots, Q(39)$ are all true propositions. But $Q(40)$ and $Q(41)$ are false.

More Propositions

Example 4.2

For $n \in \mathbb{N}$ define

$P(n)$: The sum of the odd numbers from 1 up to and including $2n - 1$ is equal to n^2.

So we have defined propositions

$$\begin{aligned} P(1)&: \quad 1 = 1^2 \\ P(2)&: \quad 1 + 3 = 2^2 \\ P(3)&: \quad 1 + 3 + 5 = 3^2 \end{aligned}$$

and so on. If you look at a few more cases you will probably be convinced that $P(n)$ is true for every $n \in \mathbb{N}$. But Example 4.1 shows it can be dangerous to make conjectures on limited evidence!

The Principle of Mathematical Induction

Suppose that $P(n)$ is a proposition for each $n \in \mathbb{N}$. The Principle of Mathematical Induction states that if

- $P(1)$ is true
- $P(n) \Longrightarrow P(n+1)$ for each $n \in \mathbb{N}$,

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

Example 4.3

For all $n \in \mathbb{N}$ we have

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

Induction: General Strategy and Example 4.4

(1) Formulate the statement you want to prove as a proposition $P(n)$, depending on a natural number n.

(2) Prove $P(1)$. This is called the *base case*.

(3) Prove that $P(n) \implies P(n+1)$ for each $n \in \mathbb{N}$. In other words: **assume** $P(n)$ **and use it to prove** $P(n+1)$. This is called the *inductive step*.

(4) Announce that you have finished!

Induction: General Strategy and Example 4.4

(1) Formulate the statement you want to prove as a proposition $P(n)$, depending on a natural number n.

(2) Prove $P(1)$. This is called the *base case*.

(3) Prove that $P(n) \implies P(n+1)$ for each $n \in \mathbb{N}$. In other words: **assume** $P(n)$ **and use it to prove** $P(n+1)$. This is called the *inductive step*.

(4) Announce that you have finished!

For the inductive step: imagine you are given a card, that says:

> *'The bearer of this card is faithfully promised that* $P(n)$ *is true'*

You can play this card at any time in your proof of $P(n+1)$. You can even play it more than once, if that seems helpful.

Induction: General Strategy and Example 4.4

(1) Formulate the statement you want to prove as a proposition $P(n)$, depending on a natural number n.

(2) Prove $P(1)$. This is called the *base case*.

(3) Prove that $P(n) \implies P(n+1)$ for each $n \in \mathbb{N}$. In other words: **assume $P(n)$ and use it to prove $P(n+1)$**. This is called the *inductive step*.

(4) Announce that you have finished!

For the inductive step: imagine you are given a card, that says:

> *'The bearer of this card is faithfully promised that $P(n)$ is true'*

You can play this card at any time in your proof of $P(n+1)$. You can even play it more than once, if that seems helpful.

Remember, $P(n)$ is a specific proposition concerning the number $n \in \mathbb{N}$. At A-level you might have written $n = k$ to emphasise this.

Changing the Base Case

Sometimes we need to take the base case to be $P(b)$ for some $b > 1$.

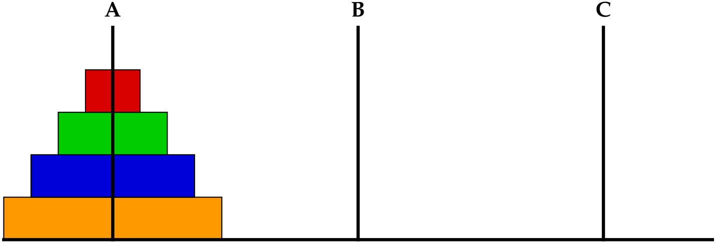
Example 4.5

If $n \in \mathbb{N}$ and $n \geq 4$ then $2^n \geq 4n$.

Towers of Hanoi

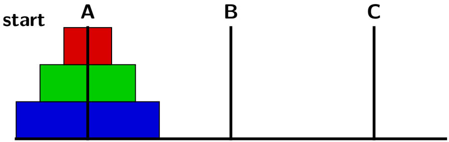
Problem 4.6 (Towers of Hanoi)

You are given a board with three pegs. On peg **A** there are *n* discs of strictly increasing radius. The starting position for a four disc game is shown below.

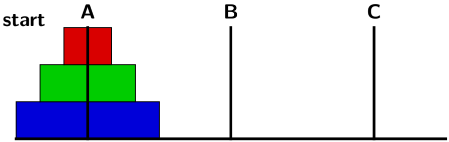


A *move* consists of taking a single disc at the top of the pile on one peg, and moving it to another peg. **At no point may a larger disc be placed on top of a smaller disc.** Your aim is to transfer all the discs from peg **A** to one of the other pegs. How many moves are required?

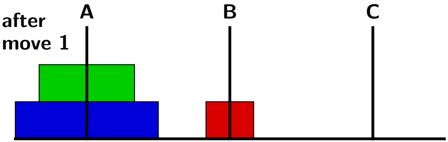
Towers of Hanoi: A Solution for Three Discs



Towers of Hanoi: A Solution for Three Discs



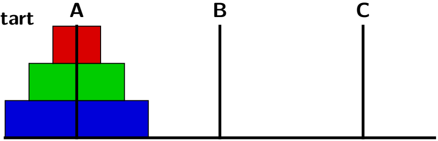
start



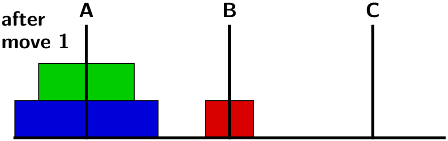
after move 1

Towers of Hanoi: A Solution for Three Discs

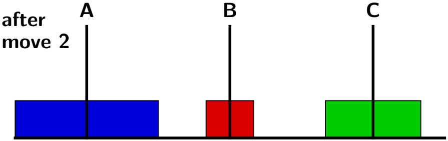
start



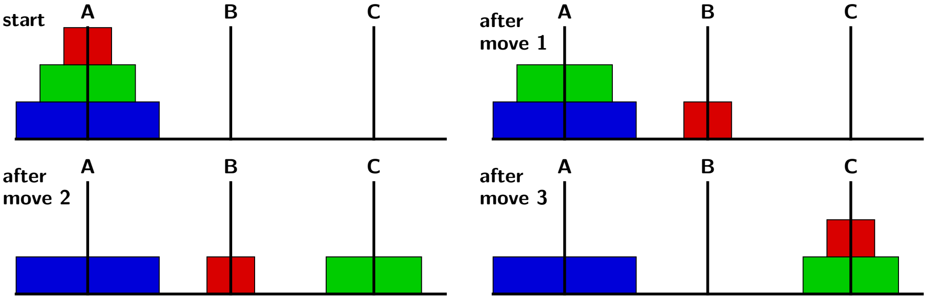
after move 1



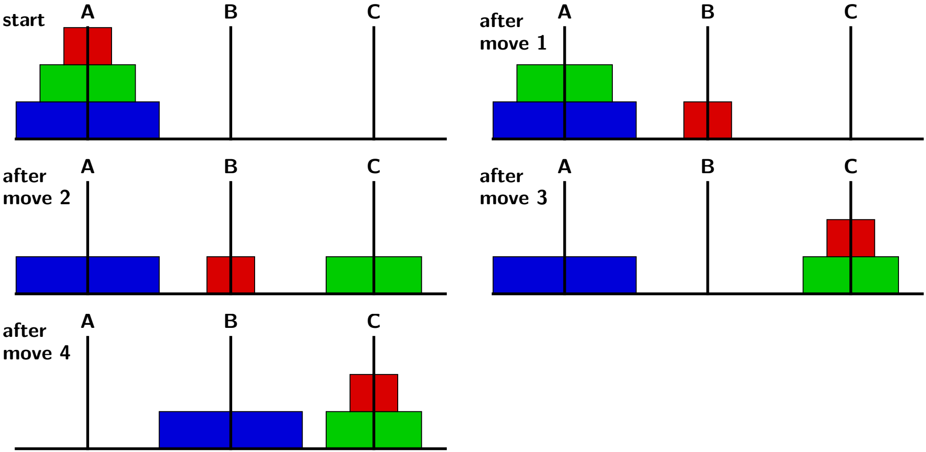
after move 2



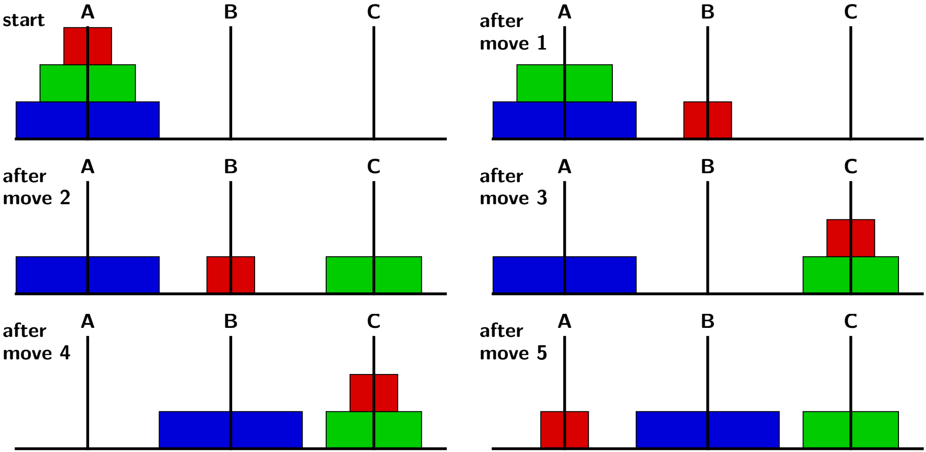
Towers of Hanoi: A Solution for Three Discs



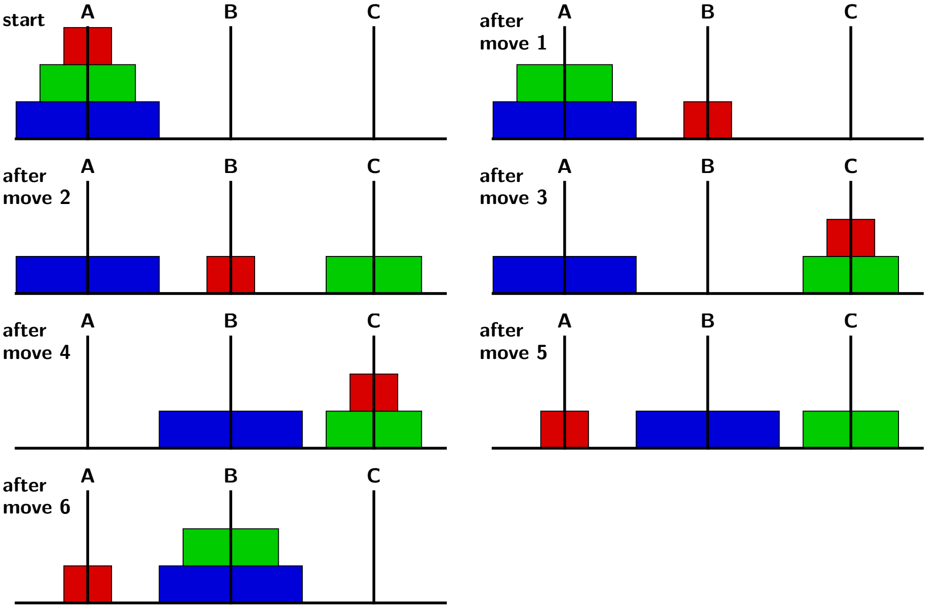
Towers of Hanoi: A Solution for Three Discs



Towers of Hanoi: A Solution for Three Discs



Towers of Hanoi: A Solution for Three Discs



start

after move 1

after move 2

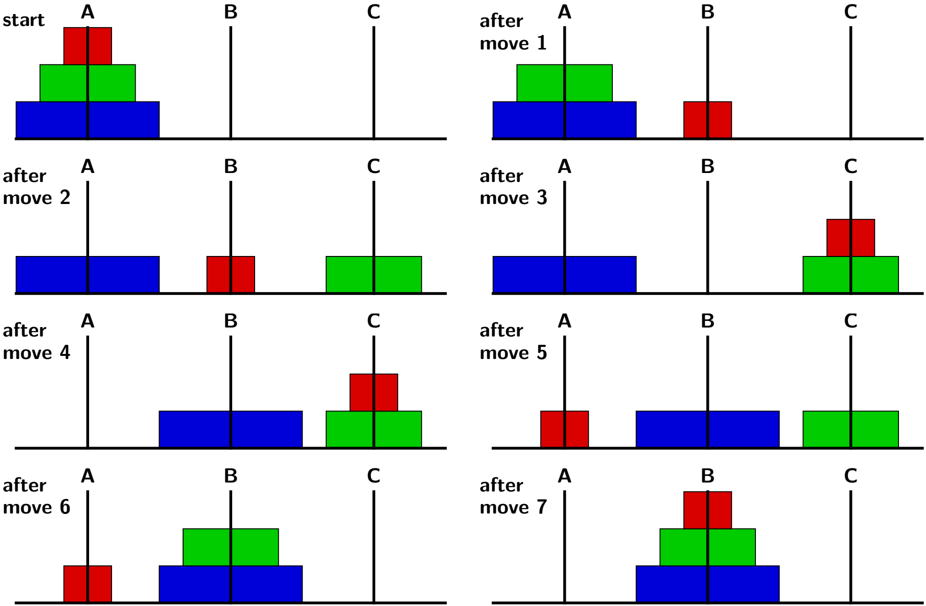
after move 3

after move 4

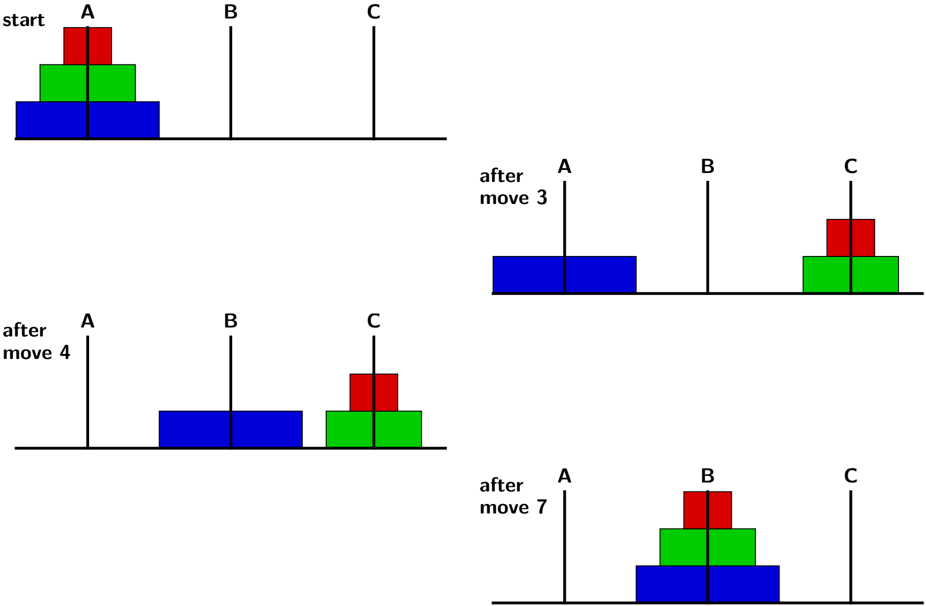
after move 5

after move 6

Towers of Hanoi: A Solution for Three Discs



Towers of Hanoi: A Solution for Three Discs



Sigma Notation

Let m, $n \in \mathbb{Z}$ with $m \leq n$. If $a_m, a_{m+1}, \ldots, a_n$ are complex numbers then we write their sum $a_m + a_{m+1} + \cdots + a_n$ as

$$\sum_{k=m}^{n} a_k.$$

This is read as 'the sum of a_k for k from m to n', or 'sigma a_k for k from m to n'. We say that k is the *summation variable*, m is the *lower limit* and n is the *upper limit*.

Sigma Notation

Let m, $n \in \mathbb{Z}$ with $m \leq n$. If $a_m, a_{m+1}, \ldots, a_n$ are complex numbers then we write their sum $a_m + a_{m+1} + \cdots + a_n$ as

$$\sum_{k=m}^{n} a_k.$$

This is read as 'the sum of a_k for k from m to n', or 'sigma a_k for k from m to n'. We say that k is the *summation variable*, m is the *lower limit* and n is the *upper limit*.

Exercise 4.8

(i) Express the sums $1 + 3 + \cdots + (2n - 1)$ and $1 + 2 + 2^2 + \cdots + 2^n$ using Σ notation.

(ii) Calculate $\sum_{m=-2}^{3} m^2$.

More Examples of Sigma Notation

Example 4.9

Let z be a complex number. Then

(i) $\sum_{k=1}^{n} z =$

(ii) $\sum_{k=1}^{n} k =$

(iii) $\sum_{k=1}^{n} n =$

More Examples of Sigma Notation

Example 4.9

Let z be a complex number. Then

(i) $\sum_{k=1}^{n} z = nz$

(ii) $\sum_{k=1}^{n} k =$

(iii) $\sum_{k=1}^{n} n =$

More Examples of Sigma Notation

Example 4.9

Let z be a complex number. Then

(i) $\sum_{k=1}^{n} z = nz$

(ii) $\sum_{k=1}^{n} k = n(n+1)/2$

(iii) $\sum_{k=1}^{n} n =$

More Examples of Sigma Notation

Example 4.9

Let z be a complex number. Then

(i) $\sum_{k=1}^{n} z = nz$

(ii) $\sum_{k=1}^{n} k = n(n+1)/2$

(iii) $\sum_{k=1}^{n} n = n^2$.

More Examples of Sigma Notation

Example 4.9

Let z be a complex number. Then

(i) $\sum_{k=1}^{n} z = nz$

(ii) $\sum_{k=1}^{n} k = n(n+1)/2$

(iii) $\sum_{k=1}^{n} n = n^2$.

Quiz: (a) $\sum_{k=0}^{2} k^2 2^{k-1} =$

(A) 7 (B) 8 (C) 9 (D) something else

(b) If $n \in \mathbb{N}$ then $\sum_{j=1}^{n} 2^j - \sum_{k=2}^{n} 2^{k-1} =$

(A) 1 (B) 2 (C) 2^n (D) 2^{n-1}

Rules for Manipulating Sigma Notation

(1) The summation variable can be renamed:

$$\sum_{k=0}^{n} 2^k = \sum_{j=0}^{n} 2^j.$$

A similar renaming is possible for sets: $\{x \in \mathbb{R} : x^2 \geq 2\}$ is exactly the same set as $\{y \in \mathbb{R} : y^2 \geq 2\}$.

(2) In a product, expressions not involving the summation variable can be taken outside the sum:

$$\sum_{j=0}^{n} 5(j+1)^2 = 5\sum_{j=0}^{n}(j+1)^2$$

and

$$\sum_{j=0}^{n} 5m(j+m)^2 = 5m\sum_{j=0}^{n}(j+m)^2.$$

(3) Sums can be split up and terms taken out.

(4) The limits can be shifted.

Example 4.10

Define

$$P(n)\colon\ \sum_{k=1}^{n} k^2 = \tfrac{1}{6}n(n+1)(2n+1).$$

Now consider $\sum_{k=1}^{n+1} k^2$. Split off the final summand using rule (3), and then use the inductive assumption $P(n)$ to get

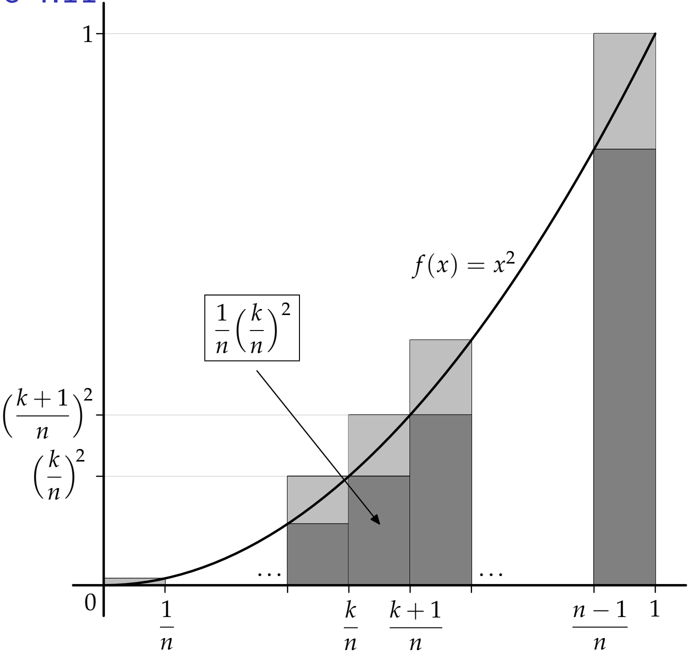
$$\sum_{k=1}^{n+1} k^2 = \sum_{k=1}^{n} k^2 + (n+1)^2 = \tfrac{1}{6}n(n+1)(2n+1) + (n+1)^2.$$

Routine algebraic manipulations give

$$\sum_{k=1}^{n+1} k^2 = \ldots = \tfrac{1}{6}(n+1)(n+2)(2n+3)$$

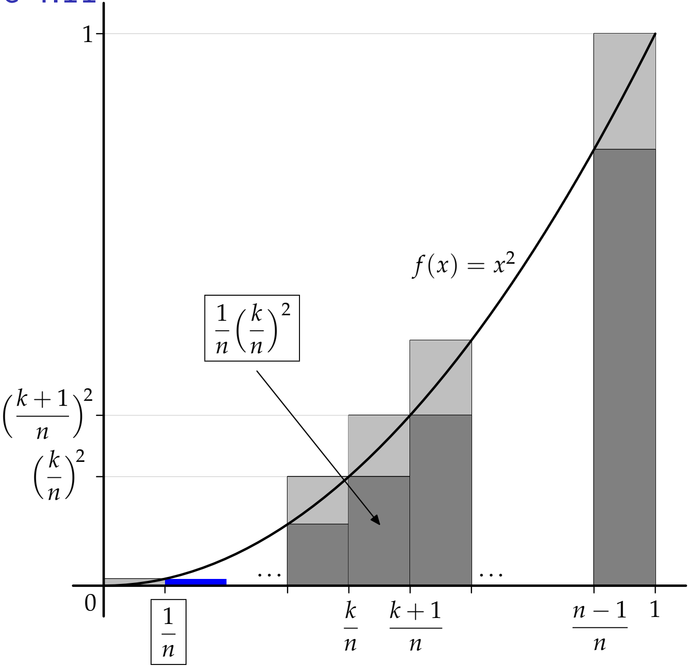
Hence $P(n+1)$ is true. Therefore $P(n) \implies P(n+1)$. By induction $P(n)$ is true for all $n \in \mathbb{N}$.

Example 4.11



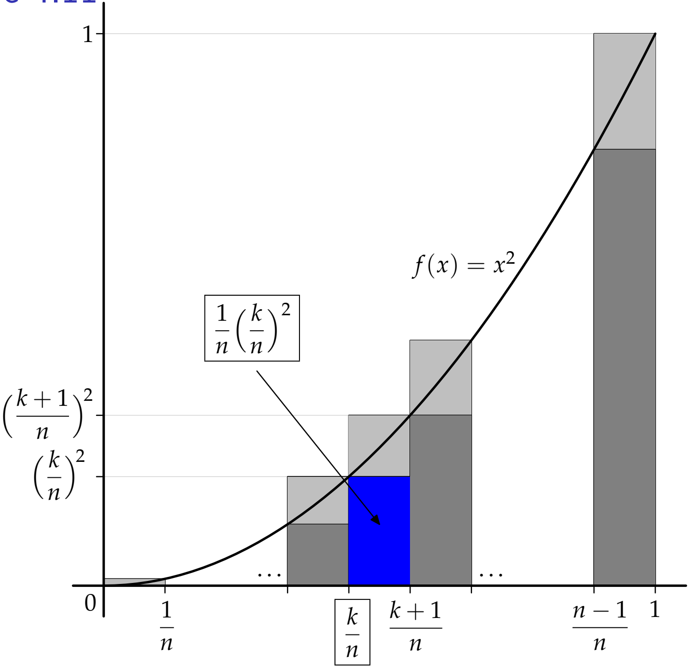
1
$f(x) = x^2$
$\frac{1}{n}\left(\frac{k}{n}\right)^2$
$\left(\frac{k+1}{n}\right)^2$
$\left(\frac{k}{n}\right)^2$
$\dots$
$\dots$
0
$\frac{1}{n}$
$\frac{k}{n}$
$\frac{k+1}{n}$
$\frac{n-1}{n}$
1

Example 4.11

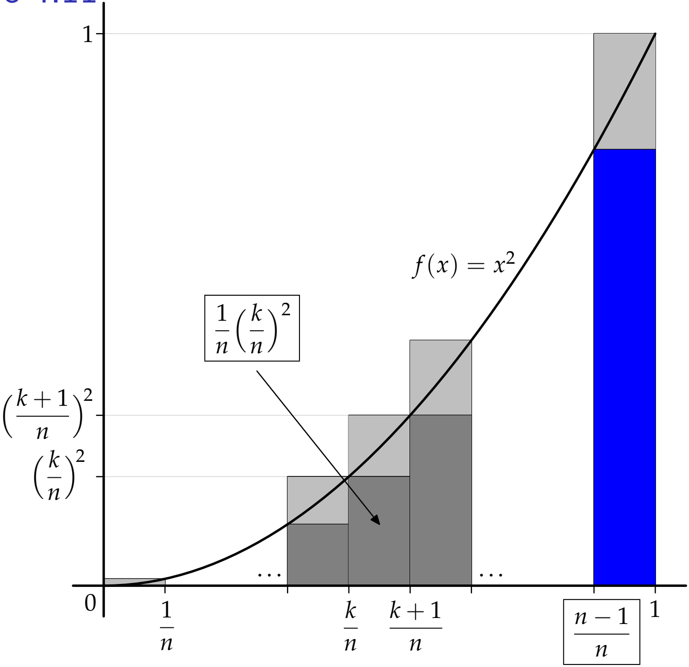


1
$\left(\frac{k+1}{n}\right)^2$
$\left(\frac{k}{n}\right)^2$
0
$\boxed{\frac{1}{n}}$
$\frac{k}{n}$
$\frac{k+1}{n}$
$\frac{n-1}{n}$
1
$\boxed{\frac{1}{n}\left(\frac{k}{n}\right)^2}$
$f(x) = x^2$
$\cdots$
$\cdots$

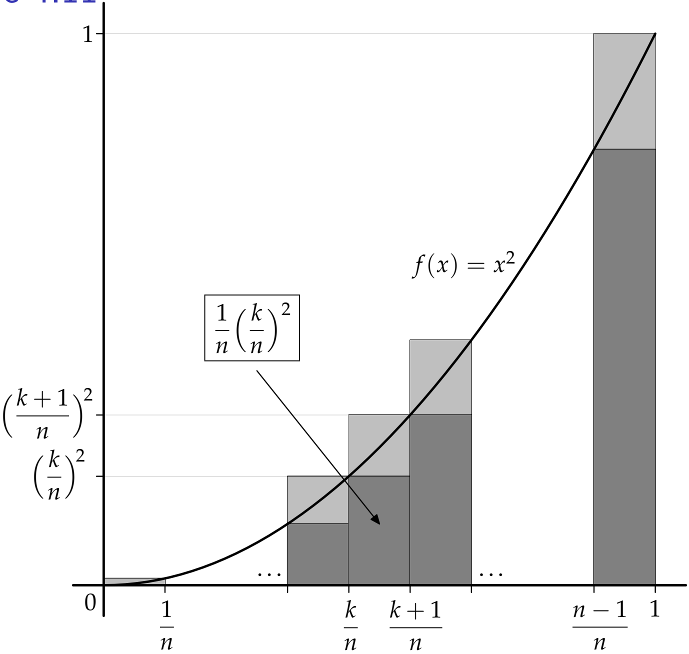
Example 4.11


1
$f(x) = x^2$
$\boxed{\frac{1}{n}\left(\frac{k}{n}\right)^2}$
$\left(\frac{k+1}{n}\right)^2$
$\left(\frac{k}{n}\right)^2$
…
…
0
$\frac{1}{n}$
$\boxed{\frac{k}{n}}$
$\frac{k+1}{n}$
$\frac{n-1}{n}$
1

Example 4.11

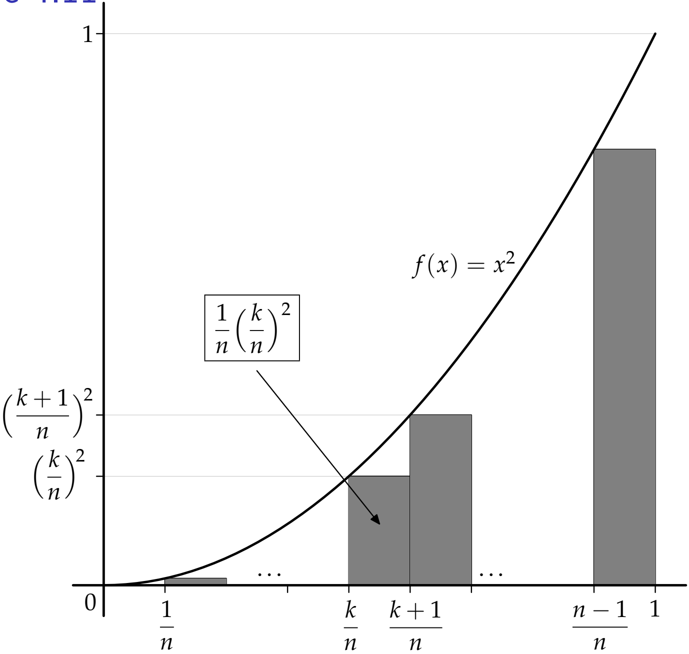

1
$f(x) = x^2$
$\frac{1}{n}\left(\frac{k}{n}\right)^2$
$\left(\frac{k+1}{n}\right)^2$
$\left(\frac{k}{n}\right)^2$
$\cdots$
$\cdots$
0
$\frac{1}{n}$
$\frac{k}{n}$
$\frac{k+1}{n}$
$\frac{n-1}{n}$
1

Example 4.11

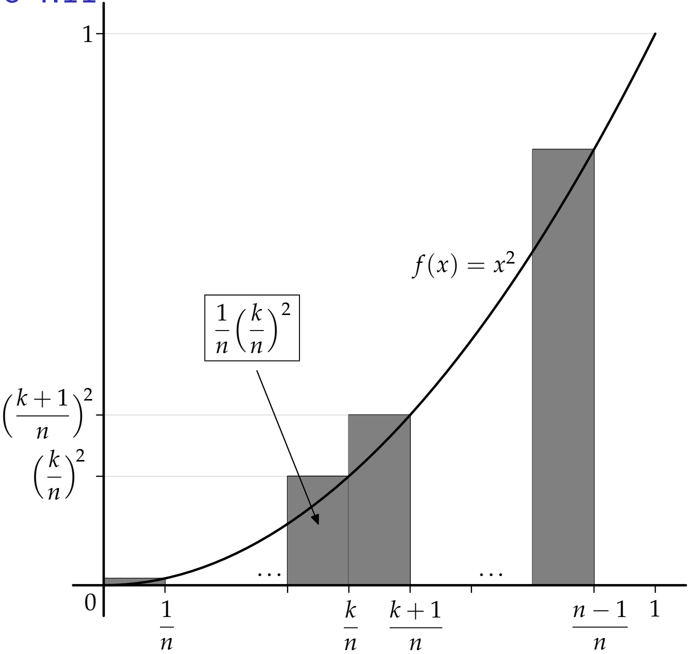


1
$\left(\frac{k+1}{n}\right)^2$
$\left(\frac{k}{n}\right)^2$
0
$\frac{1}{n}\left(\frac{k}{n}\right)^2$
$f(x) = x^2$
$\cdots$
$\cdots$
$\frac{1}{n}$
$\frac{k}{n}$
$\frac{k+1}{n}$
$\frac{n-1}{n}$
1

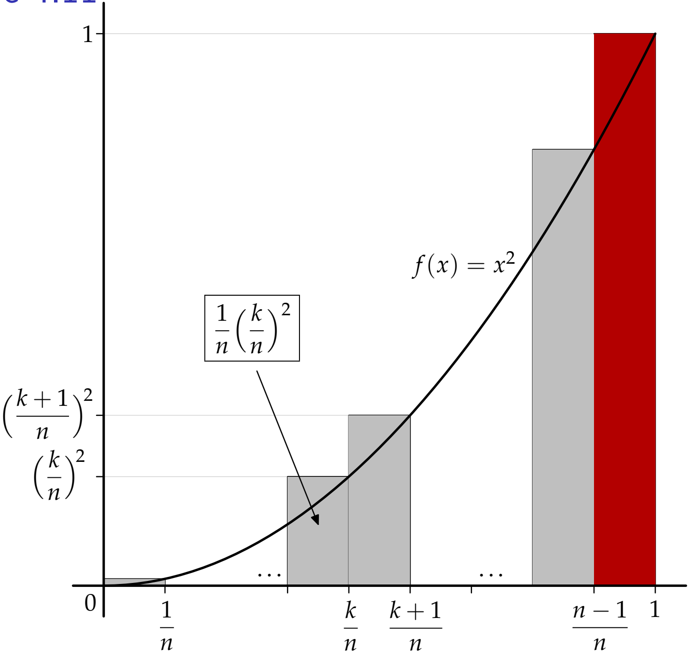
Example 4.11


1
0
$\left(\frac{k+1}{n}\right)^2$
$\left(\frac{k}{n}\right)^2$
$f(x) = x^2$
$\frac{1}{n}\left(\frac{k}{n}\right)^2$
$\dots$
$\dots$
$\frac{1}{n}$
$\frac{k}{n}$
$\frac{k+1}{n}$
$\frac{n-1}{n}$
1

Example 4.11


1
$\left(\frac{k+1}{n}\right)^2$
$\left(\frac{k}{n}\right)^2$
0
$\frac{1}{n}$
$\frac{k}{n}$
$\frac{k+1}{n}$
$\frac{n-1}{n}$
1
$\frac{1}{n}\left(\frac{k}{n}\right)^2$
$f(x) = x^2$
…
…

Example 4.11


1
$\left(\frac{k+1}{n}\right)^2$
$\left(\frac{k}{n}\right)^2$
0
$\frac{1}{n}\left(\frac{k}{n}\right)^2$
$f(x) = x^2$
$\dots$
$\dots$
$\frac{1}{n}$
$\frac{k}{n}$
$\frac{k+1}{n}$
$\frac{n-1}{n}$
1

Correction to Example 4.11

In the lecture, I took the sum over the dark rectangles from $k = 1$ up to n. But the rectangle for k starts at k/n, and so the last rectangle is the one from $x = (n-1)/n$ to $x = n/n$. So the sum should have gone from $k = 1$ up to $n - 1$. Replace

$$\sum_{k=1}^{n}\Big(\frac{k+1}{n} - \frac{k}{n}\Big)\Big(\frac{k}{n}\Big)^2 \quad \text{with} \quad \sum_{k=1}^{n-1}\Big(\frac{k+1}{n} - \frac{k}{n}\Big)\Big(\frac{k}{n}\Big)^2$$

and similarly replace

$$\frac{1}{n^3}\sum_{k=1}^{n} k^2 \quad \text{with} \quad \frac{1}{n^3}\sum_{k=1}^{n-1} k^2$$

whenever they appear. After using Example 4.10 on $\sum_{k=1}^{n-1} k^2$ the correct result is

$$\frac{(n-1)n(2n-1)}{6n^3} \le \int_0^1 x^2 \, \mathrm{d}x \le \frac{(n-1)n(2n-1)}{6n^3} + \frac{1}{n}.$$

Final Step in Example 4.11

After the lecture a few people asked about cancelling the ns at the end. Here it is a version with an extra step (and the correct formulae).

$$\frac{(n-1)n(2n-1)}{6n^3} \leq \int_0^1 x^2 \, \mathrm{d}x \leq \frac{(n-1)n(2n-1)}{6n^3} + \frac{1}{n}$$

$$\implies \frac{(1-1/n)1(2-1/n)}{6} \leq \int_0^1 x^2 \, \mathrm{d}x \leq \frac{(1-1/n)1(2-1/n)}{6} + \frac{1}{n}$$

The n^3 was used to divide each of the three terms in the numerator by n.

Dividing n by n gives $n/n = 1$, which can then be removed from the product.

The printed notes are correct.

§5 Prime Numbers

In this section we will look at prime numbers and prime factorizations.

Division with remainder should be familiar from school. It is stated formally in the next theorem.

Theorem 5.1 (Examinable)

Let $n \in \mathbb{Z}$ and let $m \in \mathbb{N}$. There exist unique integers q and r such that $n = qm + r$ and $0 \leq r < m$.

The proof shows that $q = \lfloor n/m \rfloor$ where $\lfloor x \rfloor$ is the floor function, seen in Question 3 of Sheet 2. So the existence part of the proof gives an effective way to find q.

Integer Division

We say that q is the *quotient*, and r is the *remainder* when n is divided by m. If $r = 0$ then we say that m *divides* n, or that n is a *multiple* of m.

Example 5.2

(i) Let $n = 44$ and $m = 6$. Then $44/6 = 7\frac{2}{6}$ and so, when 44 is divided by 6, the quotient is 7 and the remainder is 2. Note that for this calculation it is better to leave the fractional part as $\frac{2}{6}$ than to simplify it to $\frac{1}{3}$.

(ii) Let $n = 63$ and $m = 7$. Then $63/7 = 9$ so 7 divides 63. The quotient is 9 and the remainder is 0.

(iii) Since $-13 = -3 \times 6 + 5$, when -13 is divided by 6 the quotient is -3 and the remainder is 5.

Integer Division Exercise

Exercise 5.3

Find the quotient q and the remainder r when n is divided by m in each of these cases:

(i) $n = 20,\ m = 7,$ (ii) $n = 21,\ m = 7,$ (iii) $n = 22,\ m = 7$

(iv) $n = 7,\ m = 22,$ (v) $m = -10,\ m = 7,$ (vi) $n = 0,\ m = 1.$

Integer Division Exercise

Exercise 5.3

Find the quotient q and the remainder r when n is divided by m in each of these cases:

(i) $n = 20,\ m = 7,$ (ii) $n = 21,\ m = 7,$ (iii) $n = 22,\ m = 7$

(iv) $n = 7,\ m = 22,$ (v) $m = -10,\ m = 7,$ (vi) $n = 0,\ m = 1.$

Answers:

(i) $q = 2,\ r = 6,$ (ii) $q = 3,\ r = 0,$ (ii) $q = 3,\ r = 1$

Integer Division Exercise

Exercise 5.3

Find the quotient q and the remainder r when n is divided by m in each of these cases:

(i) $n = 20,\ m = 7,$ (ii) $n = 21,\ m = 7,$ (iii) $n = 22,\ m = 7$

(iv) $n = 7,\ m = 22,$ (v) $m = -10,\ m = 7,$ (vi) $n = 0,\ m = 1.$

Answers:

(i) $q = 2,\ r = 6,$ (ii) $q = 3,\ r = 0,$ (ii) $q = 3,\ r = 1$

(iv) $q = 0,\ r = 0,$

Integer Division Exercise

Exercise 5.3

Find the quotient q and the remainder r when n is divided by m in each of these cases:

(i) $n = 20,\ m = 7,$ (ii) $n = 21,\ m = 7,$ (iii) $n = 22,\ m = 7$

(iv) $n = 7,\ m = 22,$ (v) $m = -10,\ m = 7,$ (vi) $n = 0,\ m = 1.$

Answers:

(i) $q = 2,\ r = 6,$ (ii) $q = 3,\ r = 0,$ (ii) $q = 3,\ r = 1$

(iv) $q = 0,\ r = 0,$ (v) $q = -2,\ r = 4,$

Integer Division Exercise

Exercise 5.3

Find the quotient q and the remainder r when n is divided by m in each of these cases:

(i) $n = 20,\ m = 7,$ (ii) $n = 21,\ m = 7,$ (iii) $n = 22,\ m = 7$

(iv) $n = 7,\ m = 22,$ (v) $m = -10,\ m = 7,$ (vi) $n = 0,\ m = 1.$

Answers:

(i) $q = 2,\ r = 6,$ (ii) $q = 3,\ r = 0,$ (ii) $q = 3,\ r = 1$

(iv) $q = 0,\ r = 0,$ (v) $q = -2,\ r = 4,$ (vi) $q = 0,\ r = 0.$

Factorization Into Primes

Definition 5.4

Let $n \in \mathbb{N}$ and suppose that $n > 1$.

(i) We say that n is *prime* if the only natural numbers that divide n are 1 and n.

(ii) We say that n is *composite* if it is not prime.

The first few prime numbers are

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,\ 43,\ 47,\ \ldots.$$

By Definition 5.4, the number 1 is neither prime nor composite.

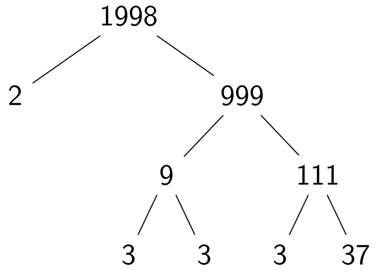
Prime Factorization Example

Example 5.5

Take $n = 1998$. We might spot that $n = 2 \times 999$ and that $999 = 9 \times 111$. Then $9 = 3 \times 3$, and $111 = 3 \times 37$, so

$$1998 = 2 \times 3 \times 3 \times 3 \times 37 = 2 \times 3^3 \times 37.$$

The tree below records these steps. (For some reason mathematical trees usually grow downwards.)



Pre-lecture Quiz (Friday 8 October)

True or False?

(a) 123 is divisible by 3

(b) 1234 is a multiple of 3

(c) 123456789123 is a multiple of 3.

Pre-lecture Quiz (Friday 8 October)

True or False?

(a) 123 is divisible by 3 TRUE

(b) 1234 is a multiple of 3

(c) 123456789123 is a multiple of 3.

Pre-lecture Quiz (Friday 8 October)

True or False?

(a) 123 is divisible by 3 TRUE

(b) 1234 is a multiple of 3 FALSE

(c) 123456789123 is a multiple of 3.

Pre-lecture Quiz (Friday 8 October)

True or False?

(a) 123 is divisible by 3 TRUE

(b) 1234 is a multiple of 3 FALSE

(c) 123456789123 is a multiple of 3. TRUE

Infinitely Many Primes

The next theorem, due to Euclid, needs only the existence of prime factorizations, proved above.

Theorem 5.6 (Examinable)

There are infinitely many prime numbers.

Infinitely Many Primes

The next theorem, due to Euclid, needs only the existence of prime factorizations, proved above.

Theorem 5.6 (Examinable)

There are infinitely many prime numbers.

How much should one trust a proof? Euclid's proof is a mathematical gem that has been understood and enjoyed by mathematicians since 300 BCE. Can any reasonable person doubt that there are infinitely many primes?

Infinitely Many Primes

The next theorem, due to Euclid, needs only the existence of prime factorizations, proved above.

Theorem 5.6 (Examinable)

There are infinitely many prime numbers.

How much should one trust a proof? Euclid's proof is a mathematical gem that has been understood and enjoyed by mathematicians since 300 BCE. Can any reasonable person doubt that there are infinitely many primes?

Exercise 5.7

The first five prime numbers are $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$, $p_6 = 13$. Show that $p_1 + 1$, $p_1 p_2 + 1$, $p_1 p_2 p_3 + 1$, $p_1 p_2 p_3 p_4 + 1$ and $p_1 p_2 p_3 p_4 p_5 + 1$ are all prime, but

$$p_1 p_2 p_3 p_4 p_5 p_6 + 1 = 2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 59 \times 509.$$

So the number N in Euclid's proof is not always prime.

Unique factorization

Let $\mathbb{N}_0$ be the set $\{0, 1, 2, 3, \ldots\}$ of the natural numbers *together with* 0.

Theorem 5.8 (Fundamental Theorem of Arithmetic)

Let $n \in \mathbb{N}$. Let $p_1, p_2, p_3, \ldots$ be the primes in increasing order. There exists unique $e_i \in \mathbb{N}_0$ such that

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \ldots.$$

Unique factorization

Let $\mathbb{N}_0$ be the set $\{0, 1, 2, 3, \dots\}$ of the natural numbers *together with* 0.

Theorem 5.8 (Fundamental Theorem of Arithmetic)

Let $n \in \mathbb{N}$. Let $p_1, p_2, p_3, \dots$ be the primes in increasing order. There exists unique $e_i \in \mathbb{N}_0$ such that

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \dots .$$

Writing out prime factorizations in the form in this theorem is a bit long-winded. For example

$$31460 = 2^2 \times 3^0 \times 5^1 \times 7^0 \times 11^2 \times 13^1 \times 17^0 \times 19^0 \dots ,$$

where all the exponents of the primes 17 or more are zero. But thinking about prime factorizations in this way is useful in proofs.

Administration

- Please take the first installment of the Part C handout.
- Please take Problem Sheet 7.
- Please put answer to Problem Sheet 6 in the box as it goes around.

Irrational Numbers (Proved Using Unique Factorization)

Example 5.9

A manufacturer of cheap calculators claims to you that $\sqrt{3} = \frac{2148105}{1240209}$. Calculate the prime factorizations of 2148105 and 1240209 (in principle you could do this by repeated division, even using one of his cheapest calculators). Hence show that he is wrong.

On Friday we found the prime factorizations

$$\begin{aligned} 2148105 &= 3 \times 5 \times 71 \times 2017 \\ 1240209 &= 3^2 \times 41 \times 3361. \end{aligned}$$

Now

$$\begin{aligned} \sqrt{3} = \frac{2148105}{1240209} &\implies \sqrt{3} \times 1240209 = 2148105 \\ &\implies 3 \times 1240209^2 = 2148105^2 \\ &\implies 3 \times 3^4 \times 41^2 \times 3361^2 = 3^2 \times 5^2 \times 71^2 \times 2017^2. \end{aligned}$$

This contradicts unique factorization.

Binary and Other Bases

Example 5.11

To write 145 in base 3:

Divide 145 by 3:	$145 = 48 \times 3 + \mathbf{1}$
Divide the quotient 48 by 3:	$48 = 16 \times 3 + \mathbf{0}$
Divide the quotient 16 by 3:	$16 = 5 \times 3 + \mathbf{1}$
Divide the quotient 5 by 3:	$5 = 1 \times 3 + \mathbf{2}$
Divide the quotient 1 by 3:	$1 = 0 \times 3 + \mathbf{1}$

We now stop, because the last quotient was 0. Reading the list of remainders from bottom to top we get

$$145 = 1 \times 3^4 + 2 \times 3^3 + 1 \times 3^2 + 0 \times 3^1 + 1 \times 3^0.$$

Hence 145 is 12101 in base 3. We write this as $145 = 12101_3$.

Our usual way of writing numbers uses base 10. If no base is specified, as is usually the case, then base 10 is intended.

Writing a Number in Base b

The example above should suggest a general algorithm.

Algorithm 5.12

Let $n \in \mathbb{N}$ and let $b \in \mathbb{N}$. To write n in base b, divide n by b, then divide the quotient by b, and so on, until the quotient is 0. If $r_0, r_1, r_2, \ldots, r_k$ is the sequence of remainders then

$$n = r_k b^k + r_{k-1} b^{k-1} + \cdots + r_1 b + r_0$$

and $n = (r_k r_{k-1} \ldots r_1 r_0)_b$.

In Example 5.11, the base was 3 and the sequence of remainders was $r_0 = 1$, $r_1 = 0$, $r_2 = 1$, $r_3 = 2$ and $r_4 = 1$.

If time permits we will prove that the algorithm is correct by induction on k, taking as the base case $k = 0$.

Binary

Base 2 is known as *binary*. Binary is particularly important because computers store and process data as sequences of the *bi*nary digi*ts*, or *bits*, 0 and 1.

Exercise 5.13

Show that $21 = 10101_2$ and write 63, 64 and 65 in binary.

Exercise 5.14

Let $n = r_k r_{k-1} \ldots r_1 r_0$ be a number written in binary. Describe, in terms of operations on the string of bits $r_k r_{k-1} \ldots r_1 r_0$, how to

(i) Multiply n by 2,

(ii) Add 1 to n,

(iii) Subtract 1 from n,

(iv) Find the quotient and remainder when n is divided by 2.

[*Hint:* for base 10, you probably learned how to do these at school. The MATHEMATICA command `BaseForm[n,2]` will write $n \in \mathbb{N}_0$ in binary.]

Binary and Computers

For a nice introduction to programming at the level of bits, see `pleasingfungus.com/Manufactoria/`.

```
01001001 01110100 00100000 01101001 01110011 00100000 01100001 00100000
01110100 01110010 01110101 01110100 01101000 00100000 01110101 01101110
01101001 01110110 01100101 01110010 01110011 01100001 01101100 01101100
01111001 00100000 01100001 01100011 01101011 01101110 01101111 01110111
01101100 01100101 01100100 01100111 01100101 01100100 00101100 00100000
01110100 01101000 01100001 01110100 00100000 01100001 00100000 01110011
01101001 01101110 01100111 01101100 01100101 00100000 01101101 01100001
01101110 00100000 01101001 01101110 00100000 01110000 01101111 01110011
01110011 01100101 01110011 01110011 01101001 01101111 01101110 00001010
01101111 01100110 00100000 01100001 00100000 01100111 01101111 01101111
01100100 00100000 01100110 01101111 01110010 01110100 01110101 01101110
01100101 00101100 00100000 01101101 01110101 01110011 01110100 00100000
01100010 01100101 00100000 01101001 01101110 00100000 01110111 01100001
01101110 01110100 00100000 01101111 01100110 00100000 01100001 00100000
01110111 01101001 01100110 01100101 00101110 00001010
```

Jane Austen (1813)

Binary and Computers

For a nice introduction to programming at the level of bits, see `pleasingfungus.com/Manufactoria/`.

```
01001001 01110100 00100000 01101001 01110011 00100000 01100001 00100000
01110100 01110010 01110101 01110100 01101000 00100000 01110101 01101110
01101001 01110110 01100101 01110010 01110011 01100001 01101100 01101100
01111001 00100000 01100001 01100011 01101011 01101110 01101111 01110111
01101100 01100101 01100100 01100111 01100101 01100100 00101100 00100000
01110100 01101000 01100001 01110100 00100000 01100001 00100000 01110011
01101001 01101110 01100111 01101100 01100101 00100000 01101101 01100001
01101110 00100000 01101001 01101110 00100000 01110000 01101111 01110011
01110011 01100101 01110011 01110011 01101001 01101111 01101110 00001010
01101111 01100110 00100000 01100001 00100000 01100111 01101111 01101111
01100100 00100000 01100110 01101111 01110010 01110100 01110101 01101110
01100101 00101100 00100000 01101101 01110101 01110011 01110100 00100000
01100010 01100101 00100000 01101001 01101110 00100000 01110111 01100001
01101110 01110100 00100000 01101111 01100110 00100000 01100001 00100000
01110111 01101001 01100110 01100101 00101110 00001010
```

Jane Austen (1813)

Binary and Computers

For a nice introduction to programming at the level of bits, see `pleasingfungus.com/Manufactoria/`.

```
01001001 01110100 00100000 01101001 01110011 00100000 01100001 00100000
01110100 01110010 01110101 01110100 01101000 00100000 01110101 01101110
01101001 01110110 01100101 01110010 01110011 01100001 01101100 01101100
01111001 00100000 01100001 01100011 01101011 01101110 01101111 01110111
01101100 01100101 01100100 01100111 01100101 01100100 00101100 00100000
01110100 01101000 01100001 01110100 00100000 01100001 00100000 01110011
01101001 01101110 01100111 01101100 01100101 00100000 01101101 01100001
01101110 00100000 01101001 01101110 00100000 01110000 01101111 01110011
01110011 01100101 01110011 01110011 01101001 01101111 01101110 00001010
01101111 01100110 00100000 01100001 00100000 01100111 01101111 01101111
01100100 00100000 01100110 01101111 01110010 01110100 01110101 01101110
01100101 00101100 00100000 01101101 01110101 01110011 01110100 00100000
01100010 01100101 00100000 01101001 01101110 00100000 01110111 01100001
01101110 01110100 00100000 01101111 01100110 00100000 01100001 00100000
01110111 01101001 01100110 01100101 00101110 00001010
```

It is a truth universally acknowledged, that a single man in possession of a good fortune, must be in want of a wife.

Jane Austen (1813)

Part C: Logic and sets

§6 Logic

In pairs discuss the meaning of the following sentences. Each has two interpretations that are logically reasonable.

(a) The picture of the woman in the museum.

(b) The lady hit the man with an umbrella.

(c) Nurses help dog bite victim.

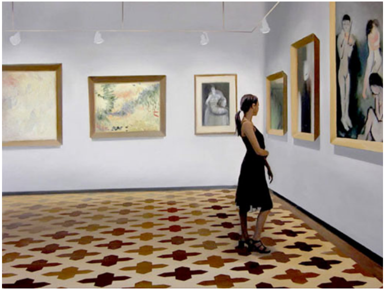
(d) Did you see the girl with the telescope?

(e) Walk to Windsor or swim the Channel and climb the Matterhorn.

§6 Logic

In pairs discuss the meaning of the following sentences. Each has two interpretations that are logically reasonable.

(a) The picture of the woman in the museum.
(b) The lady hit the man with an umbrella.
(c) Nurses help dog bite victim.
(d) Did you see the girl with the telescope?
(e) Walk to Windsor or swim the Channel and climb the Matterhorn.



Part C: Logic and sets

§6 Logic

In pairs discuss the meaning of the following sentences. Each has two interpretations that are logically reasonable.

(a) The picture of the woman in the museum.

(b) The lady hit the man with an umbrella.

(c) Nurses help dog bite victim.

(d) Did you see the girl with the telescope?

(e) Walk to Windsor or swim the Channel and climb the Matterhorn.

The ambiguities in everyday language are often resolved, either from the context, or because we are conditioned to expect one meaning.

In mathematics we instead try to avoid ambiguity by careful use of mathematical language and symbols. Mathematical language has some usages that may seem strange at first.

‘And’, ‘or’ and ‘not’

Another word that is used in mathematics in a way that may seem non-standard is ‘or’. Let P and Q be propositions. (Remember, this means P and Q can be any propositions!)

(i) P *or* Q, written $P \vee Q$, means at least one of P and Q is true.

(ii) P *and* Q, written $P \wedge Q$, means P and Q are both true.

(iii) *not* P, written $\neg P$, means that P is false.

There is a correspondence between the logical operations $\wedge$, $\vee$ and $\neg$ and the set operations $\cap$, $\cup$ and set complement.

Example 6.1

Consider the following propositions, depending on a natural number n.

$$\begin{aligned} P(n)&: \ n \text{ is even} \\ Q(n)&: \ n \text{ is a multiple of } 3 \end{aligned}$$

Will discuss

(a) $\neg P(n) \wedge Q(n)$, (b) $P(n) \wedge Q(n)$, (c) $\neg P(n)$.

Exercise 6.2

Let $R(n) = \big(P(n) \vee Q(n)\big) \wedge \neg\big(P(n) \wedge Q(n)\big)$ where $P(n)$ and $Q(n)$ are as in Example 6.1.

(a) State $R(n)$ in words.

(b) Draw a Venn diagram representing the sets

- $\{n \in \mathbb{N} : P(n)\}$
- $\{n \in \mathbb{N} : Q(n)\}$
- $\{n \in \mathbb{N} : R(n)\}$
- $\{n \in \mathbb{N} : \neg P(n) \wedge Q(n)\}$.

Truth Tables

A concise way to specify a logical operation such as $\vee$, $\wedge$ or $\neg$ is by a *truth table*, such as the one below for $\vee$.

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

Truth tables can be used to prove logical identities. The next result is the analogue of Claim 1.10 for propositions.

Claim 6.3 (De Morgan's Laws for propositions)

Let P and Q be propositions. Then the following are true:

(i) $\neg(P \vee Q) \iff \neg P \wedge \neg Q$,

(ii) $\neg(P \wedge Q) \iff \neg P \vee \neg Q$.

Implication, Logical equivalence and Tautologies

We have already used $\implies$ 'implies' and $\iff$ 'if and only if' many times. Let P and Q be propositions. Stated formally:

- $P \implies Q$ means that if P is true then Q is true.
- $P \iff Q$ means that $P \implies Q$ and $Q \implies P$.

If $P \iff Q$ is true then we say that P and Q are *logically equivalent*. For example, by Claim 6.3(i), the propositions $\neg(P \vee Q)$ and $\neg P \wedge \neg Q$ are logically equivalent.

If a proposition is always true, then it is said to be a *tautology*. For instance

$$(P \iff Q) \iff \big((P \implies Q) \wedge (Q \implies P)\big)$$

is a tautology, and so is $P \iff \neg(\neg P)$. See Question 3 on Sheet 7 for some more examples.

Truth Table for Implication

Truth Table for Implication

By definition, $P \implies Q$ means 'if P is true then Q is true'. If P is false then this statement makes no claim about Q. Therefore if P is false then $P \implies Q$ is true.

This may seem surprising to you. But it is consistent with how we use implication. Think of $P \implies Q$ as a promise: if P is true, then Q is true. If P is false, then it does not matter whether Q is true or not: the promise is still kept.

Truth Table for Implication

By definition, $P \implies Q$ means 'if P is true then Q is true'. If P is false then this statement makes no claim about Q. Therefore if P is false then $P \implies Q$ is true.

This may seem surprising to you. But it is consistent with how we use implication. Think of $P \implies Q$ as a promise: if P is true, then Q is true. If P is false, then it does not matter whether Q is true or not: the promise is still kept.

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

Notice that there is only one false in the column for $P \implies Q$.

$$\boxed{P \implies Q \text{ is false if and only if } P \text{ is true and } Q \text{ is false}}$$

Example 6.4

Logically $P \implies Q$ says nothing about $Q \implies P$. For example, consider these two propositions concerning a real number x.

$$\begin{aligned} P(x)&\colon\ x \geq 2 + \sqrt{5} \\ Q(x)&\colon\ x^2 - 4x + 1 \geq 2 \end{aligned}$$

Then $P(x) \implies Q(x)$ for every $x \in \mathbb{R}$. But $Q(-10)$ is true and $P(-10)$ is false, so $Q(-10) \not\Longrightarrow P(-10)$. Correspondingly, as seen in Example 1.8,

$$\{x \in \mathbb{R} : P(x)\} \subseteq \{x \in \mathbb{R} : Q(x)\},$$

and -10 is in the right-hand set, but not in the left-hand set.

Final Thoughts on Truth Table for Implication

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

(a) From discussion after the lecture, the following seems to be persuasive (and mathematically correct):

> $P \implies Q$ is a promise: if P is true, then Q is true. This promise is only broken if P is true and Q is false. So if we have to assign a truth value to $P \implies Q$ then we must always assign true *except* when P is true and Q is false.

(b) The consequence that any true proposition implies any other true proposition is maybe a little bit alarming. It is more general than **the way you are encouraged to use $\implies$ in arguments**: write $P \implies Q$ if you've shown that P is true and there is some simple reason why Q follows.

Quiz on Implication

Exercise 6.5

Which of the following propositions are true for all $x \in \mathbb{R}$?

(a) $P(x)$: $x \geq 4 \implies x \geq 3$,

(b) $Q(x)$: $x \geq 3 \implies x \geq 4$,

(c) $R(x)$: $x^2 - 2x - 3 = 0 \implies x = -1$, $x = 3$ or $x = 37$,

(d) $S(x)$: $x \geq 0$ and $x^2 - 2x - 3 = 0 \implies x = 3$,

Which of the following propositions are true for all $x, y \in \mathbb{R}$?

(e) $T(x, y)$: $x^2 = y^2 \implies x = y$,

(f) $U(x, y)$: $x^3 = y^3 \implies x = y$.

When can $\implies$ be replaced with $\iff$?

(g) In court, the prosecutor says

> 'If the defendant is guilty then he had an acommplice'.

The defendant states 'That's false'. What can you conclude?

Quiz on Implication

Exercise 6.5

Which of the following propositions are true for all $x \in \mathbb{R}$?

(a) $P(x)$: $x \geq 4 \implies x \geq 3$, True

(b) $Q(x)$: $x \geq 3 \implies x \geq 4$,

(c) $R(x)$: $x^2 - 2x - 3 = 0 \implies x = -1$, $x = 3$ or $x = 37$,

(d) $S(x)$: $x \geq 0$ and $x^2 - 2x - 3 = 0 \implies x = 3$,

Which of the following propositions are true for all $x, y \in \mathbb{R}$?

(e) $T(x, y)$: $x^2 = y^2 \implies x = y$,

(f) $U(x, y)$: $x^3 = y^3 \implies x = y$.

When can $\implies$ be replaced with $\iff$?

(g) In court, the prosecutor says

‘If the defendant is guilty then he had an acommplice’.

The defendant states ‘That’s false’. What can you conclude?

Quiz on Implication

Exercise 6.5

Which of the following propositions are true for all $x \in \mathbb{R}$?

(a) $P(x)$: $x \geq 4 \implies x \geq 3$, True

(b) $Q(x)$: $x \geq 3 \implies x \geq 4$, False

(c) $R(x)$: $x^2 - 2x - 3 = 0 \implies x = -1$, $x = 3$ or $x = 37$,

(d) $S(x)$: $x \geq 0$ and $x^2 - 2x - 3 = 0 \implies x = 3$,

Which of the following propositions are true for all $x, y \in \mathbb{R}$?

(e) $T(x, y)$: $x^2 = y^2 \implies x = y$,

(f) $U(x, y)$: $x^3 = y^3 \implies x = y$.

When can $\implies$ be replaced with $\iff$?

(g) In court, the prosecutor says

> ‘If the defendant is guilty then he had an acommplice’.

The defendant states ‘That’s false’. What can you conclude?

Quiz on Implication

Exercise 6.5

Which of the following propositions are true for all $x \in \mathbb{R}$?

(a) $P(x)$: $x \geq 4 \implies x \geq 3$, True

(b) $Q(x)$: $x \geq 3 \implies x \geq 4$, False

(c) $R(x)$: $x^2 - 2x - 3 = 0 \implies x = -1$, $x = 3$ or $x = 37$, True

(d) $S(x)$: $x \geq 0$ and $x^2 - 2x - 3 = 0 \implies x = 3$,

Which of the following propositions are true for all $x, y \in \mathbb{R}$?

(e) $T(x, y)$: $x^2 = y^2 \implies x = y$,

(f) $U(x, y)$: $x^3 = y^3 \implies x = y$.

When can $\implies$ be replaced with $\iff$?

(g) In court, the prosecutor says

> 'If the defendant is guilty then he had an acommplice'.

The defendant states 'That's false'. What can you conclude?

Quiz on Implication

Exercise 6.5

Which of the following propositions are true for all $x \in \mathbb{R}$?

(a) $P(x)$: $x \geq 4 \implies x \geq 3$, True

(b) $Q(x)$: $x \geq 3 \implies x \geq 4$, False

(c) $R(x)$: $x^2 - 2x - 3 = 0 \implies x = -1$, $x = 3$ or $x = 37$, True

(d) $S(x)$: $x \geq 0$ and $x^2 - 2x - 3 = 0 \implies x = 3$, True

Which of the following propositions are true for all $x, y \in \mathbb{R}$?

(e) $T(x, y)$: $x^2 = y^2 \implies x = y$,

(f) $U(x, y)$: $x^3 = y^3 \implies x = y$.

When can $\implies$ be replaced with $\iff$?

(g) In court, the prosecutor says

> 'If the defendant is guilty then he had an acommplice'.

The defendant states 'That's false'. What can you conclude?

Quiz on Implication

Exercise 6.5

Which of the following propositions are true for all $x \in \mathbb{R}$?

(a) $P(x)$: $x \geq 4 \implies x \geq 3$, True

(b) $Q(x)$: $x \geq 3 \implies x \geq 4$, False

(c) $R(x)$: $x^2 - 2x - 3 = 0 \implies x = -1$, $x = 3$ or $x = 37$, True

(d) $S(x)$: $x \geq 0$ and $x^2 - 2x - 3 = 0 \implies x = 3$, True

Which of the following propositions are true for all $x, y \in \mathbb{R}$?

(e) $T(x, y)$: $x^2 = y^2 \implies x = y$, False

(f) $U(x, y)$: $x^3 = y^3 \implies x = y$.

When can $\implies$ be replaced with $\iff$?

(g) In court, the prosecutor says

> ‘If the defendant is guilty then he had an acommplice’.

The defendant states ‘That’s false’. What can you conclude?

Quiz on Implication

Exercise 6.5

Which of the following propositions are true for all $x \in \mathbb{R}$?

(a) $P(x)$: $x \geq 4 \implies x \geq 3$, True

(b) $Q(x)$: $x \geq 3 \implies x \geq 4$, False

(c) $R(x)$: $x^2 - 2x - 3 = 0 \implies x = -1$, $x = 3$ or $x = 37$, True

(d) $S(x)$: $x \geq 0$ and $x^2 - 2x - 3 = 0 \implies x = 3$, True

Which of the following propositions are true for all $x, y \in \mathbb{R}$?

(e) $T(x, y)$: $x^2 = y^2 \implies x = y$, False

(f) $U(x, y)$: $x^3 = y^3 \implies x = y$. True

When can $\implies$ be replaced with $\iff$?

(g) In court, the prosecutor says

> 'If the defendant is guilty then he had an acommplice'.

The defendant states 'That's false'. What can you conclude?

Quiz on Implication

Exercise 6.5

Which of the following propositions are true for all $x \in \mathbb{R}$?

(a) $P(x)$: $x \geq 4 \implies x \geq 3$, $\not\Longleftarrow$ True

(b) $Q(x)$: $x \geq 3 \implies x \geq 4$, False

(c) $R(x)$: $x^2 - 2x - 3 = 0 \implies x = -1$, $x = 3$ or $x = 37$, $\not\Longleftarrow$ True

(d) $S(x)$: $x \geq 0$ and $x^2 - 2x - 3 = 0 \implies x = 3$, $\Longleftrightarrow$ True

Which of the following propositions are true for all $x, y \in \mathbb{R}$?

(e) $T(x, y)$: $x^2 = y^2 \implies x = y$, False

(f) $U(x, y)$: $x^3 = y^3 \implies x = y$. $\Longleftrightarrow$ True

When can $\implies$ be replaced with $\iff$?

(g) In court, the prosecutor says

> ‘If the defendant is guilty then he had an acommplice’.

The defendant states ‘That’s false’. What can you conclude?

Proof by Contrapositive

Claim 6.6

Let P and Q be propositions. Then $P \implies Q$ and $\neg Q \implies \neg P$ are logically equivalent.

Proof by Contrapositive

Claim 6.6

Let P and Q be propositions. Then $P \implies Q$ and $\neg Q \implies \neg P$ are logically equivalent.

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

Switching to the contrapositive can be useful first step in a proof, particularly when statements appear in negated form.

Claim 6.7

Let $a \in \mathbb{Q}$ and let $x \in \mathbb{R}$. If $x \notin \mathbb{Q}$ then $x + a \notin \mathbb{Q}$.

Quiz

(1) Cards. You are shown a number of cards. Each card has a letter printed on one side, and a number printed on the other. Four cards are put on a table. You can see:

(A) o (B) t (C) 5 (D) 6

Which cards would you turn over to test the conjecture: ‘If a card has a vowel on one side then it has a prime on the other’? (Turn over all the cards that might disprove the conjecture.)

Quiz

(1) Cards. You are shown a number of cards. Each card has a letter printed on one side, and a number printed on the other. Four cards are put on a table. You can see:

(A) o (B) t (C) 5 (D) 6

Which cards would you turn over to test the conjecture: 'If a card has a vowel on one side then it has a prime on the other'? (Turn over all the cards that might disprove the conjecture.)

(2) Alcohol. In the far-off land of Erewhon, only people over the age of 18 are allowed to drink alcohol in public. If your job is to enforce this law, who of the following would you investigate?

(A) A person drinking a glass of wine

(B) A person drinking coke

(C) Someone clearly over 50 with an unidentifable drink

(D) Someone who looks about 16 with an unidentifiable drink

(Investigate all the people who might be committing an offence.)

Quiz (Wason Selection Task)

(1) Cards. You are shown a number of cards. Each card has a letter printed on one side, and a number printed on the other. Four cards are put on a table. You can see:

(A) o (B) t (C) 5 (D) 6

Which cards would you turn over to test the conjecture: 'If a card has a vowel on one side then it has a prime on the other'? (Turn over all the cards that might disprove the conjecture.)

(2) Alcohol. In the far-off land of Erewhon, only people over the age of 18 are allowed to drink alcohol in public. If your job is to enforce this law, who of the following would you investigate?

(A) A person drinking a glass of wine

(B) A person drinking coke

(C) Someone clearly over 50 with an unidentifable drink

(D) Someone who looks about 16 with an unidentifiable drink

(Investigate all the people who might be committing an offence.)

Using Implication to Clarify Proofs

It is often tempting to start with the statement we are trying to prove, and manipulate it until it becomes obviously true. **But this is only valid if every step is reversible**.

Using Implication to Clarify Proofs

It is often tempting to start with the statement we are trying to prove, and manipulate it until it becomes obviously true. **But this is only valid if every step is reversible**.

Exercise 6.9

Criticize and improve the following proof that $2^n \geq 6n$ for all n such that $n \geq 5$.

$P(n) = 2^n \geq 6n$ where $n \geq 5$.

$P(5) = 2^5 \geq 6 \times 5$. True.

$P(n+1)$ where $n \in \mathbb{N}$, $n \geq 5$.

$$2^{n+1} \geq 6(n+1)$$

$$2^n \geq 3n+3$$

$$6n \geq 3n+3$$

$$3n \geq 3$$

Hence by the Principle of Mathematical Induction, $P(n)$ is true for all $n \in \mathbb{N}$ when $n \geq 5$.

Question 6 on Sheet 6

Define a function $d : \mathbb{N} \to \mathbb{N}$ so that $d(n)$ is the number of natural numbers m such that n is divisible by m. For example, 12 is divisible by 1, 2, 3, 4, 6 and 12, so $d(12) = 6$.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$d(n)$	1	2	2	3	2	4	2	4	3	4	2	6	2	4	4	5

(d) Describe, in terms of their prime factorizations, the natural numbers n such that (i) $d(n) = 3$ and (ii) $d(n) = 4$.

Proving that Two Sets are Equal

Question 2(c) of Sheet 7 shows that $(P \vee Q) \wedge R$ and $(P \wedge R) \vee (Q \wedge R)$ are logically equivalent. The corresponding set theory identity is (i) below.

Claim 6.10

Let X, Y and Z be sets. Then

(i) $(X \cup Y) \cap Z = (X \cap Z) \cup (Y \cap Z)$,

(ii) $(X \cap Y) \cup Z = (X \cup Z) \cap (Y \cup Z)$.

The proof will use the following principle: if A and B are sets then

$$A = B \iff A \subseteq B \text{ and } B \subseteq A.$$

This if often a good way to show that two sets are equal.

‘For all’ and ‘exists’

Let $P(x)$ be a propositions depending on an element x of a set X.

- If $P(x)$ is true for all $x \in X$, then we write $(\forall x \in X)\, P(x)$.
- If there exists an element $x \in X$ such that $P(x)$ is true, then we write $(\exists x \in X)\, P(x)$.

The negation of

- $(\forall x \in X)\, P(x)$ is $(\exists x \in X)\, \neg P(x)$.
- $(\exists x \in X)\, P(x)$ is $(\forall x \in X)\, \neg P(x)$.

‘For all’ and ‘exists’ **[Do injective example]**

Let $P(x)$ be a propositions depending on an element x of a set X.

- If $P(x)$ is true for all $x \in X$, then we write $(\forall x \in X)\, P(x)$.
- If there exists an element $x \in X$ such that $P(x)$ is true, then we write $(\exists x \in X)\, P(x)$.

The negation of

- $(\forall x \in X)\, P(x)$ is $(\exists x \in X)\, \neg P(x)$.
- $(\exists x \in X)\, P(x)$ is $(\forall x \in X)\, \neg P(x)$.

‘For all’ and ‘exists’

Let $P(x)$ be a propositions depending on an element x of a set X.

- If $P(x)$ is true for all $x \in X$, then we write $(\forall x \in X)\, P(x)$.
- If there exists an element $x \in X$ such that $P(x)$ is true, then we write $(\exists x \in X)\, P(x)$.

The negation of

- $(\forall x \in X)\, P(x)$ is $(\exists x \in X)\, \neg P(x)$.
- $(\exists x \in X)\, P(x)$ is $(\forall x \in X)\, \neg P(x)$.

Exercise 6.11

Sometimes the set X in $\forall x \in X$ is indicated by inequalities.

$(\forall \epsilon > 0)\, Q(\epsilon)$ means that $Q(\epsilon)$ is true for all ϵ in the set of positive real numbers,

$(\forall n \geq N)\, S(n)$ means that $S(n)$ is true for all $n \in \mathbb{N}$ such that $n \geq N$.

Let $a_1, a_2, a_3, \ldots$ be real numbers. Write down the negation of

$$(\exists \ell \in \mathbb{R})(\forall \epsilon > 0)(\exists N \in \mathbb{N})(\forall n \geq N)\ |a_n - \ell| < \epsilon.$$

Definitions

Definitions are a frequent source of confusion. Here is the definition of prime from Definition 5.4.

> *Let $n \in \mathbb{N}$ and suppose that $n > 1$. We say that n is prime if the only natural numbers that divide n are 1 and n.*

By convention, when 'if' is written in a definition, it means 'if and only if'.

Exercise 6.12

In examinations you may be asked to give some definitions. Here is a typical question and a sadly not atypical answer.

> *'What does it mean to say that $f : X \to Y$ is injective'?*
>
> **Answer:** $f(x) \neq f(x')$. *So f is injective if there aren't two arrows in the same dot, like $f(x) = x + 1$.*

Criticize this answer.

Extras: Exercise 6.13. Assume *P*, *Q*, *R*.

P: If it is raining then the sky is cloudy.

Q: If it rains in the morning then Prof. X carries his umbrella all day.

R: People who carry umbrellas never get soaked.

Which of the following statements can be deduced from *P*, *Q* and *R*? (Next slide has all the answers.)

A: A cloudy sky is a necessary condition for rain.

B: A cloudy sky is a sufficient condition for rain.

C: It is raining only if the sky is cloudy.

D: Rain in the morning is a necessary condition for Prof. X to carry his umbrella.

E: Rain in the morning is a sufficient condition for Prof. X to carry his umbrella.

F: Rain falling implies that the sky is cloudy.

G: The sky is cloudy implies that rain is falling.

H: If Prof. X is soaked then it did not rain this morning.

Extras: Exercise 6.13. Assume *P*, *Q*, *R*.

P: If it is raining then the sky is cloudy.
$\text{RAIN} \Longrightarrow \text{CLOUD}$

Q: If it rains in the morning then Prof. X carries his umbrella all day.
$\text{MORNING RAIN} \Longrightarrow \text{UMBRELLA}$

R: People who carry umbrellas never get soaked.
$\text{UMBRELLA} \Longrightarrow \text{NOT SOAKED}$

Which of the following statements can be deduced from *P*, *Q* and *R*? (Next slide has all the answers.)

A: A cloudy sky is a necessary condition for rain.

B: A cloudy sky is a sufficient condition for rain.

C: It is raining only if the sky is cloudy.

D: Rain in the morning is a necessary condition for Prof. X to carry his umbrella.

E: Rain in the morning is a sufficient condition for Prof. X to carry his umbrella.

F: Rain falling implies that the sky is cloudy.

G: The sky is cloudy implies that rain is falling.

H: If Prof. X is soaked then it did not rain this morning.

Extras: Exercise 6.13. Assume P, Q, R.

P: If it is raining then the sky is cloudy.

RAIN ⟹ CLOUD

Q: If it rains in the morning then Prof. X carries his umbrella all day.

MORNING RAIN ⟹ UMBRELLA

R: People who carry umbrellas never get soaked.

UMBRELLA ⟹ NOT SOAKED

Which of the following statements can be deduced from P, Q and R?
(Next slide has all the answers.)

A: A cloudy sky is a necessary condition for rain. True

B: A cloudy sky is a sufficient condition for rain. False

C: It is raining only if the sky is cloudy. True

D: Rain in the morning is a necessary condition for Prof. X to carry his umbrella. False

E: Rain in the morning is a sufficient condition for Prof. X to carry his umbrella. True

F: Rain falling implies that the sky is cloudy. True

G: The sky is cloudy implies that rain is falling. False

H: If Prof. X is soaked then it did not rain this morning. True

§7 Sets and Counting

Definition 7.1

Let X be a set. We say that X is *finite* if it has finitely many elements, and *infinite* otherwise. The *size* of a finite set X is its number of elements. We denote the size of X by $|X|$,

Note that $|X|$ is read as 'mod X'.

§7 Sets and Counting

Definition 7.1

Let X be a set. We say that X is *finite* if it has finitely many elements, and *infinite* otherwise. The *size* of a finite set X is its number of elements. We denote the size of X by $|X|$,

Note that $|X|$ is read as 'mod X'.

Reminder of elements of a set and subsets of a set.

Elements, Subsets and Sizes

Exercise 7.2

State the truth value (true or false) of each of the propositions below.

(a) 1 is an element of $\mathbb{N}$

(b) $\{1\}$ is an element of $\mathbb{N}$

(c) $|\ x \in \mathbb{R} : x^2 = -1\}| = 0$

(d) $|\{z \in \mathbb{C} : z^3 = 1\}| = 3$

(e) $\Big|\Big\{\mathbb{N}, \mathbb{Q}, \{0, 1\}\Big\}\Big| = 3$

(f) The set of natural numbers is infinite

(g) The empty set is a subset of every set

(h) The empty set is an element of every set

Elements, Subsets and Sizes

Exercise 7.2

State the truth value (true or false) of each of the propositions below.

(a) 1 is an element of $\mathbb{N}$ True

(b) $\{1\}$ is an element of $\mathbb{N}$

(c) $| \, x \in \mathbb{R} : x^2 = -1\}| = 0$

(d) $|\{z \in \mathbb{C} : z^3 = 1\}| = 3$

(e) $\left|\left\{\mathbb{N}, \mathbb{Q}, \{0, 1\}\right\}\right| = 3$

(f) The set of natural numbers is infinite

(g) The empty set is a subset of every set

(h) The empty set is an element of every set

Elements, Subsets and Sizes

Exercise 7.2

State the truth value (true or false) of each of the propositions below.

(a) 1 is an element of $\mathbb{N}$ True

(b) $\{1\}$ is an element of $\mathbb{N}$ False

(c) $|\ x \in \mathbb{R} : x^2 = -1\}| = 0$

(d) $|\{z \in \mathbb{C} : z^3 = 1\}| = 3$

(e) $\left|\left\{\mathbb{N}, \mathbb{Q}, \{0, 1\}\right\}\right| = 3$

(f) The set of natural numbers is infinite

(g) The empty set is a subset of every set

(h) The empty set is an element of every set

Elements, Subsets and Sizes

Exercise 7.2

State the truth value (true or false) of each of the propositions below.

(a) 1 is an element of $\mathbb{N}$ True

(b) $\{1\}$ is an element of $\mathbb{N}$ False

(c) $| x \in \mathbb{R} : x^2 = -1\}| = 0$ True

(d) $|\{z \in \mathbb{C} : z^3 = 1\}| = 3$

(e) $\left|\left\{\mathbb{N}, \mathbb{Q}, \{0, 1\}\right\}\right| = 3$

(f) The set of natural numbers is infinite

(g) The empty set is a subset of every set

(h) The empty set is an element of every set

Elements, Subsets and Sizes

Exercise 7.2

State the truth value (true or false) of each of the propositions below.

(a) 1 is an element of $\mathbb{N}$ True

(b) $\{1\}$ is an element of $\mathbb{N}$ False

(c) $| x \in \mathbb{R} : x^2 = -1\}| = 0$ True

(d) $|\{z \in \mathbb{C} : z^3 = 1\}| = 3$ True

(e) $\left|\left\{\mathbb{N}, \mathbb{Q}, \{0, 1\}\right\}\right| = 3$

(f) The set of natural numbers is infinite

(g) The empty set is a subset of every set

(h) The empty set is an element of every set

Elements, Subsets and Sizes

Exercise 7.2

State the truth value (true or false) of each of the propositions below.

(a) 1 is an element of $\mathbb{N}$ True

(b) $\{1\}$ is an element of $\mathbb{N}$ False

(c) $| x \in \mathbb{R} : x^2 = -1\}| = 0$ True

(d) $|\{z \in \mathbb{C} : z^3 = 1\}| = 3$ True

(e) $\left|\left\{\mathbb{N}, \mathbb{Q}, \{0, 1\}\right\}\right| = 3$ True

(f) The set of natural numbers is infinite

(g) The empty set is a subset of every set

(h) The empty set is an element of every set

Elements, Subsets and Sizes

Exercise 7.2

State the truth value (true or false) of each of the propositions below.

(a) 1 is an element of $\mathbb{N}$ True

(b) $\{1\}$ is an element of $\mathbb{N}$ False

(c) $| x \in \mathbb{R} : x^2 = -1\}| = 0$ True

(d) $|\{z \in \mathbb{C} : z^3 = 1\}| = 3$ True

(e) $\left|\left\{\mathbb{N}, \mathbb{Q}, \{0, 1\}\right\}\right| = 3$ True

(f) The set of natural numbers is infinite True

(g) The empty set is a subset of every set

(h) The empty set is an element of every set

Elements, Subsets and Sizes

Exercise 7.2

State the truth value (true or false) of each of the propositions below.

(a) 1 is an element of $\mathbb{N}$ True

(b) $\{1\}$ is an element of $\mathbb{N}$ False

(c) $| x \in \mathbb{R} : x^2 = -1\}| = 0$ True

(d) $|\{z \in \mathbb{C} : z^3 = 1\}| = 3$ True

(e) $\big|\big\{\mathbb{N}, \mathbb{Q}, \{0, 1\}\big\}\big| = 3$ True

(f) The set of natural numbers is infinite True

(g) The empty set is a subset of every set True

(h) The empty set is an element of every set

Elements, Subsets and Sizes

Exercise 7.2

State the truth value (true or false) of each of the propositions below.

(a) 1 is an element of $\mathbb{N}$ True

(b) $\{1\}$ is an element of $\mathbb{N}$ False

(c) $| \ x \in \mathbb{R} : x^2 = -1\}| = 0$ True

(d) $|\{z \in \mathbb{C} : z^3 = 1\}| = 3$ True

(e) $\big|\big\{\mathbb{N}, \mathbb{Q}, \{0, 1\}\big\}\big| = 3$ True

(f) The set of natural numbers is infinite True

(g) The empty set is a subset of every set True

(h) The empty set is an element of every set False

Principle of Inclusion and Exclusion

Let X and Y be finite sets. In the sum $|X| + |Y|$ we count each element of X once, and each element of Y once. So the elements of $X \cap Y$ are counted twice, once as elements of X, and once as elements of Y. If we subtract $|X \cap Y|$ to correct for this overcounting, we get

$$|X \cup Y| = |X| + |Y| - |X \cap Y|.$$

Principle of Inclusion and Exclusion

Let X and Y be finite sets. In the sum $|X| + |Y|$ we count each element of X once, and each element of Y once. So the elements of $X \cap Y$ are counted twice, once as elements of X, and once as elements of Y. If we subtract $|X \cap Y|$ to correct for this overcounting, we get

$$|X \cup Y| = |X| + |Y| - |X \cap Y|.$$

For example, if $z \in X \cap Y$ then z is counted in $|X|$, $|Y|$ and in $|X \cap Y|$, for a total contribution of $1 + 1 - 1 = 1$.

If X and Y are contained in a universe set U then, since

$$|(X \cup Y)'| = |U| - |X \cup Y|$$

we have

$$|(X \cup Y)'| = |U| - |X| - |Y| + |X \cap Y|.$$

Exercise on Inclusion / Exclusion

Exercise 7.3

At the University of Erewhon, there are 100 students. At each algebra lecture there are 65 students and at each analysis lecture that are 70 students. Let b be the number of students doing both algebra and analysis.

(i) If $b = 50$, how many students are doing neither algebra nor analysis?

(ii) What is the greatest possible value of b?

(iii) What is the least possible value of b?

Principle of Inclusion and Exclusion for Three Sets

Claim 7.4

If X, Y and Z are finite sets then

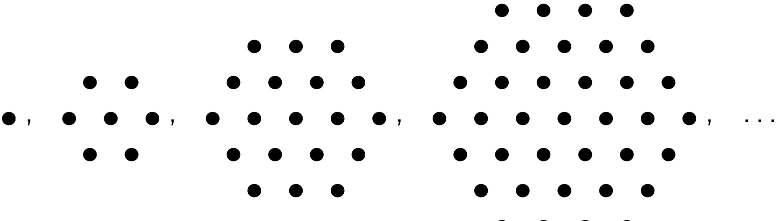
$$|X \cup Y \cup Z| = |X| + |Y| + |Z| - |X \cap Y| - |Y \cap Z| - |Z \cap X| + |X \cap Y \cap Z|.$$

Exercise 7.5

Suppose that X, Y, Z are subsets of a finite universe set U. Use Claim 7.4 to write down a formula for the size of $\left|(X \cup Y \cup Z)'\right|$.

Example 7.6

Let a_n be the number of dots in the nth diagram below. So $a_1 = 1$, $a_2 = 7$, $a_3 = 19$, $a_4 = 37$, and so on.



Cartesian Products

Exercise 7.8

Let

$$X = \{x \in \mathbb{R} : 1 \leq x \leq 3\}$$
$$Y = \{y \in \mathbb{R} : 1 \leq y \leq 2\}.$$

Decide on the truth value of the following propositions.

(a) $(1, 2) = (2, 1)$

(b) $\{1, 2\} = \{2, 1\}$

(c) $(5/2, 3/2) \in X \times Y$

(d) $(3/2, 5/2) \in X \times Y$

(e) $Y \times Y \subseteq X \times Y$

(f) $X \subseteq Y$

(g) $\varnothing \times X \subseteq \varnothing \times Y$

Cartesian Products

Exercise 7.8

Let

$$X = \{x \in \mathbb{R} : 1 \leq x \leq 3\}$$
$$Y = \{y \in \mathbb{R} : 1 \leq y \leq 2\}.$$

Decide on the truth value of the following propositions.

(a) $(1, 2) = (2, 1)$ False

(b) $\{1, 2\} = \{2, 1\}$

(c) $(5/2, 3/2) \in X \times Y$

(d) $(3/2, 5/2) \in X \times Y$

(e) $Y \times Y \subseteq X \times Y$

(f) $X \subseteq Y$

(g) $\varnothing \times X \subseteq \varnothing \times Y$

Cartesian Products

Exercise 7.8

Let

$$X = \{x \in \mathbb{R} : 1 \leq x \leq 3\}$$
$$Y = \{y \in \mathbb{R} : 1 \leq y \leq 2\}.$$

Decide on the truth value of the following propositions.

(a) $(1, 2) = (2, 1)$ False

(b) $\{1, 2\} = \{2, 1\}$ True

(c) $(5/2, 3/2) \in X \times Y$

(d) $(3/2, 5/2) \in X \times Y$

(e) $Y \times Y \subseteq X \times Y$

(f) $X \subseteq Y$

(g) $\varnothing \times X \subseteq \varnothing \times Y$

Cartesian Products

Exercise 7.8

Let

$$X = \{x \in \mathbb{R} : 1 \leq x \leq 3\}$$
$$Y = \{y \in \mathbb{R} : 1 \leq y \leq 2\}.$$

Decide on the truth value of the following propositions.

(a) $(1, 2) = (2, 1)$ False

(b) $\{1, 2\} = \{2, 1\}$ True

(c) $(5/2, 3/2) \in X \times Y$ True

(d) $(3/2, 5/2) \in X \times Y$

(e) $Y \times Y \subseteq X \times Y$

(f) $X \subseteq Y$

(g) $\varnothing \times X \subseteq \varnothing \times Y$

Cartesian Products

Exercise 7.8

Let

$$X = \{x \in \mathbb{R} : 1 \leq x \leq 3\}$$
$$Y = \{y \in \mathbb{R} : 1 \leq y \leq 2\}.$$

Decide on the truth value of the following propositions.

(a) $(1, 2) = (2, 1)$ False

(b) $\{1, 2\} = \{2, 1\}$ True

(c) $(5/2, 3/2) \in X \times Y$ True

(d) $(3/2, 5/2) \in X \times Y$ False

(e) $Y \times Y \subseteq X \times Y$

(f) $X \subseteq Y$

(g) $\varnothing \times X \subseteq \varnothing \times Y$

Cartesian Products

Exercise 7.8

Let

$$X = \{x \in \mathbb{R} : 1 \leq x \leq 3\}$$
$$Y = \{y \in \mathbb{R} : 1 \leq y \leq 2\}.$$

Decide on the truth value of the following propositions.

(a) $(1, 2) = (2, 1)$ False

(b) $\{1, 2\} = \{2, 1\}$ True

(c) $(5/2, 3/2) \in X \times Y$ True

(d) $(3/2, 5/2) \in X \times Y$ False

(e) $Y \times Y \subseteq X \times Y$ True

(f) $X \subseteq Y$

(g) $\varnothing \times X \subseteq \varnothing \times Y$

Cartesian Products

Exercise 7.8

Let

$$X = \{x \in \mathbb{R} : 1 \leq x \leq 3\}$$
$$Y = \{y \in \mathbb{R} : 1 \leq y \leq 2\}.$$

Decide on the truth value of the following propositions.

(a) $(1, 2) = (2, 1)$ False

(b) $\{1, 2\} = \{2, 1\}$ True

(c) $(5/2, 3/2) \in X \times Y$ True

(d) $(3/2, 5/2) \in X \times Y$ False

(e) $Y \times Y \subseteq X \times Y$ True

(f) $X \subseteq Y$ False

(g) $\varnothing \times X \subseteq \varnothing \times Y$

Cartesian Products

Exercise 7.8

Let

$$X = \{x \in \mathbb{R} : 1 \leq x \leq 3\}$$
$$Y = \{y \in \mathbb{R} : 1 \leq y \leq 2\}.$$

Decide on the truth value of the following propositions.

(a) $(1, 2) = (2, 1)$ False

(b) $\{1, 2\} = \{2, 1\}$ True

(c) $(5/2, 3/2) \in X \times Y$ True

(d) $(3/2, 5/2) \in X \times Y$ False

(e) $Y \times Y \subseteq X \times Y$ True

(f) $X \subseteq Y$ False

(g) $\varnothing \times X \subseteq \varnothing \times Y$ True

Independent Choices

Suppose that X and Y are finite sets. The number of ordered pairs (x, y) with $x \in X$ and $y \in Y$ is $|X||Y|$, since we have $|X|$ choices for x and $|Y|$ independent choices for y. Hence $|X \times Y| = |X||Y|$.

Example 7.9

A menu offers a choice of 3 starters, 5 main courses, and 2 desserts.

(a) How many three course meals can be ordered?

(b) How many two course meals can be ordered?

§8 Euclid's Algorithm and Congruences

Definition 8.1

Let $m, n \in \mathbb{N}$. We say that $d \in \mathbb{N}$ is the *greatest common divisor* of m and n, and write $\gcd(m, n) = d$, if d is the greatest natural number that divides both m and n.

Example 8.2 See board

Part D: Integers and rings

§8 Euclid's Algorithm and Congruences

Definition 8.1

Let $m, n \in \mathbb{N}$. We say that $d \in \mathbb{N}$ is the *greatest common divisor* of m and n, and write $\gcd(m, n) = d$, if d is the greatest natural number that divides both m and n.

Example 8.2 See board

Exercise 8.3

Find $\gcd(m, n)$ in each of these cases:

(i) $m = 310$, $n = 42$,

(ii) $m = 23$, $n = 46$,

(iii) $m = 31460$, $n = 41\,991\,752$.

Hint: on page 38 we saw that $31460 = 2^2 \times 5 \times 11^2 \times 13$. You do not need to factor m completely to find the gcd.

Euclid's Algorithm

Lemma 8.4 (Examinable)

Let $m, n \in \mathbb{N}$. Let $n = qm + r$. Then

$$\gcd(n, m) = \gcd(m, r).$$

Algorithm 8.5 (Euclid's Algorithm)

Let n, $m \in \mathbb{N}$. Find the quotient q and the remainder r when n is divided by m.

- If $r = 0$ then m divides n and $\gcd(n, m) = m$.
- Otherwise repeat from the start with m and r.

Example 8.6

Let $n = 3933$ and let $m = 389$. The equations below show the quotient and remainder at each step of Euclid's Algorithm:

$$\begin{aligned}
\mathbf{3933} &= 10 \times \mathbf{389} + \mathbf{43} \\
\mathbf{389} &= 9 \times \mathbf{43} + \mathbf{2} \\
\mathbf{43} &= 21 \times \mathbf{2} + \mathbf{1} \\
\mathbf{2} &= 2 \times \mathbf{1}.
\end{aligned}$$

Hence $\gcd(3933, 389) = 1$.

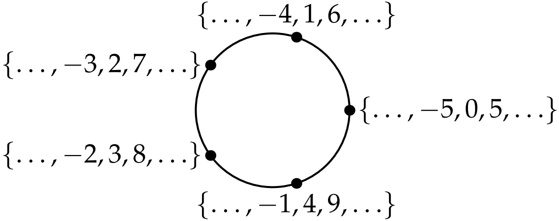
Example 8.7: Work backwards to get

$$\begin{aligned}
1 &= \mathbf{43} - 21 \times \mathbf{2} \\
&= \mathbf{43} - 21 \times (\mathbf{389} - 9 \times \mathbf{43}) \\
&= 190 \times \mathbf{43} - 21 \times \mathbf{389} \\
&= 190 \times (\mathbf{3933} - 10 \times \mathbf{389}) - 21 \times \mathbf{389} \\
&= 190 \times \mathbf{3933} - 1921 \times \mathbf{389}.
\end{aligned}$$

Congruences

Definition 8.8

Let $m \in \mathbb{N}$. Let $n, n' \in \mathbb{Z}$. If $n - n'$ is divisible by m then we say that n is *congruent to n' modulo m*, and write $n \equiv n' \bmod m$.



Example 8.9

(a) Since $5848 = 2 \times 2652 + 544$, we have $5848 \equiv 544 \bmod 2652$.

(b) $-7 \equiv 10 \bmod 17$ since $-7 - 10$ is divisible by 17.

(c) $27 \times 33 \equiv 17 \times 33 \equiv 7 \times 33 \equiv 7 \times 3 \equiv 1 \bmod 10$. **Exercise:** make up a similar example working modulo 5.

Congruent Numbers

Lemma 8.10 (Examinable)

Let $m \in \mathbb{N}$ and let $r, r', s, s' \in \mathbb{Z}$. If $r \equiv r' \bmod m$ and $s \equiv s' \bmod m$ then

(i) $r + s \equiv r' + s' \bmod m$,

(ii) $rs \equiv r's' \bmod m$.

Lemma 8.10 justifies many manipulations with congruences.

For example, suppose we know that $2x \equiv 1 \bmod 5$. Let $r = r' = 3$ and let $s = 2x$, $s' = 1$. Then by Lemma 8.11 we have $3 \times 2x \equiv 3 \times 1 \bmod 5$. This simplifies to $x \equiv 3 \bmod 5$.

Solving Congruences

Exercise 8.11

(a) Find $x \in \mathbb{Z}$ such that $0 \leq x < 11$ and $x + 9 \equiv 7 \bmod 12$.

(b) Find an $x \in \mathbb{Z}$ such that $3x \equiv 2 \bmod 5$.

(c) Find *all* $x \in \mathbb{Z}$ such that $3x \equiv 2 \bmod 5$.

When the modulus m is larger, Euclid's algorithm can be used.

Example 8.12′ See board.

The printed notes have a similar example using larger numbers.

Not all congruences can be solved. For example $2x \equiv 3 \bmod 4$ has no solution, because $2x$ is always even, but any number congruent to 3 modulo 4 is odd.

Solving Congruences

Exercise 8.11

(a) Find $x \in \mathbb{Z}$ such that $0 \leq x < 11$ and $x + 9 \equiv 7 \bmod 12$.

$x = 10$ is the unique such x

(b) Find an $x \in \mathbb{Z}$ such that $3x \equiv 2 \bmod 5$.

(c) Find *all* $x \in \mathbb{Z}$ such that $3x \equiv 2 \bmod 5$.

When the modulus m is larger, Euclid's algorithm can be used.

Example 8.12′ See board.

The printed notes have a similar example using larger numbers.

Not all congruences can be solved. For example $2x \equiv 3 \bmod 4$ has no solution, because $2x$ is always even, but any number congruent to 3 modulo 4 is odd.

Solving Congruences

Exercise 8.11

(a) Find $x \in \mathbb{Z}$ such that $0 \leq x < 11$ and $x + 9 \equiv 7 \bmod 12$.

$x = 10$ is the unique such x

(b) Find an $x \in \mathbb{Z}$ such that $3x \equiv 2 \bmod 5$.

$x = 4$, or $x = -1$, or $x = 9$ or $\dots$

(c) Find *all* $x \in \mathbb{Z}$ such that $3x \equiv 2 \bmod 5$.

When the modulus m is larger, Euclid's algorithm can be used.

Example 8.12′ See board.

The printed notes have a similar example using larger numbers.

Not all congruences can be solved. For example $2x \equiv 3 \bmod 4$ has no solution, because $2x$ is always even, but any number congruent to 3 modulo 4 is odd.

Solving Congruences

Exercise 8.11

(a) Find $x \in \mathbb{Z}$ such that $0 \leq x < 11$ and $x + 9 \equiv 7 \bmod 12$.

$x = 10$ is the unique such x

(b) Find an $x \in \mathbb{Z}$ such that $3x \equiv 2 \bmod 5$.

$x = 4$, or $x = -1$, or $x = 9$ or $\ldots$

(c) Find *all* $x \in \mathbb{Z}$ such that $3x \equiv 2 \bmod 5$.

$3x \equiv 2 \bmod 5 \iff x = 4 + 5q$ for some $q \in \mathbb{Z}$

When the modulus m is larger, Euclid's algorithm can be used.

Example 8.12$'$ See board.

The printed notes have a similar example using larger numbers.

Not all congruences can be solved. For example $2x \equiv 3 \bmod 4$ has no solution, because $2x$ is always even, but any number congruent to 3 modulo 4 is odd.

Solving Congruences

Exercise 8.11

(a) Find $x \in \mathbb{Z}$ such that $0 \leq x < 11$ and $x + 9 \equiv 7 \bmod 12$.

$x = 10$ is the unique such x

(b) Find an $x \in \mathbb{Z}$ such that $3x \equiv 2 \bmod 5$.

$x = 4$, or $x = -1$, or $x = 9$ or ...

(c) Find *all* $x \in \mathbb{Z}$ such that $3x \equiv 2 \bmod 5$.

$$\begin{aligned} 3x \equiv 2 \bmod 5 &\iff x = 4 + 5q \text{ for some } q \in \mathbb{Z} \\ &\iff x \equiv 4 \bmod 5 \end{aligned}$$

When the modulus m is larger, Euclid's algorithm can be used.

Example 8.12$'$ See board.

The printed notes have a similar example using larger numbers.

Not all congruences can be solved. For example $2x \equiv 3 \bmod 4$ has no solution, because $2x$ is always even, but any number congruent to 3 modulo 4 is odd.

The ISBN Code

An ISBN is a sequence of length 10 with entries from

$$\{1, 2, \dots, 9, \mathrm{X}\}.$$

The check digit is chosen so that if $u_1 u_2 u_3 u_4 u_5 u_6 u_7 u_8 u_9 u_{10}$ is an ISBN then the *check equation*

$$\sum_{j=1}^{10} (11 - j) u_j \equiv 0 \text{ mod } 11$$

holds. It might be necessary to take 10 as a check digit. In this case the letter X is used to stand for 10.

Exercise 8.13

(a) Suppose that an error is made in position 8, and the ISBN is miscopied as 1-4398-3568-5. Show that the error will be detected because the check equation no longer holds.

(b) Suppose that the digits in positions 8 and 9 are swapped, and so 1-4398-3589-5 is written down. Show again that the error will be detected.

The Square Code

The square code is the set of all sequences

$$(u_1, u_2, u_3, u_4, u_1 + u_2, u_3 + u_4, u_1 + u_3, u_2 + u_4)$$

where $u_1, u_2, u_3, u_4 \in \{0, 1\}$ and the addition is done modulo 2.

Exercise: Alice wants to send Bob a number m between 0 and 15. She writes m in binary as $m = 2^3 b_3 + 2^2 b_2 + 2^1 b_1 + 2^0 b_0$ and then sends Bob the codeword in the Square Code starting $b_3 b_2 b_1 b_0 \ldots$

Imagine you are Bob and you receive 10011001. What do you think Alice's number is?

The Square Code

The square code is the set of all sequences

$$(u_1, u_2, u_3, u_4, u_1 + u_2, u_3 + u_4, u_1 + u_3, u_2 + u_4)$$

where $u_1, u_2, u_3, u_4 \in \{0, 1\}$ and the addition is done modulo 2.

Exercise: Alice wants to send Bob a number m between 0 and 15. She writes m in binary as $m = 2^3 b_3 + 2^2 b_2 + 2^1 b_1 + 2^0 b_0$ and then sends Bob the codeword in the Square Code starting $b_3 b_2 b_1 b_0 \ldots$

Imagine you are Bob and you receive 10011001. What do you think Alice's number is?

(A) 8 (B) 9 (C) 11 (D) 13.

The Square Code as a Party Trick

Question *i* can be stated more briefly as: is the *i*th position of the codeword for your number equal to 1?

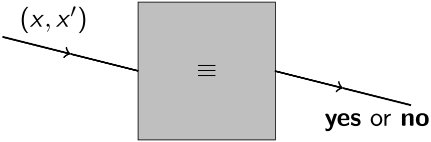
1	Is your number	8, 9, 10, 11, 12, 13, 14 or 15?
2	" " "	4, 5, 6, 7, 12, 13, 14 or 15?
3	" " "	2, 3, 6, 7, 10, 11, 14 or 15?
4	" " "	1, 3, 5, 7, 9, 11, 13 or 15?
5	" " "	4, 5, 6, 7, 8, 9, 10 or 11?
6	" " "	1, 2, 5, 6, 9, 10, 13 or 14?
7	" " "	2, 3, 6, 7, 8, 9, 12 or 13?
8	" " "	1, 3, 4, 6, 9, 11, 12 or 14?

§9 Relations and the Integers Modulo m

The following definition generalizes the congruence relation.

Definition 9.1

Let X be a set. A *relation* on X is a black box which, given an ordered pair (x, x') where x, $x' \in X$, outputs either **yes** or **no**. A **yes** means x is related to x', and a **no** means x is not related to x'.



Two relations on a set X are equal if they agree on all ordered pairs (x, x'). As for functions, it is irrelevant how the black box arrives at its answer.

Examples of Relations

Example 9.2

(i) Fix $m \in \mathbb{N}$. Let $n, n' \in \mathbb{Z}$. For the input (n, n'), let the black box output **yes** if $n \equiv n' \bmod m$ and **no** otherwise. This defines the congruence modulo m relation on $\mathbb{Z}$.

(ii) Let P be the set of all subsets of $\{1, 2, 3\}$. Given an ordered pair (X, Y) of elements of P, let the black box output **yes** if $X \subseteq Y$ and **no** otherwise.

Relations can be defined more briefly. For example, suppose that $X = \{1, 2, 3, 4, 5, 6\}$. Then

$$x \text{ relates to } y \iff x < y$$

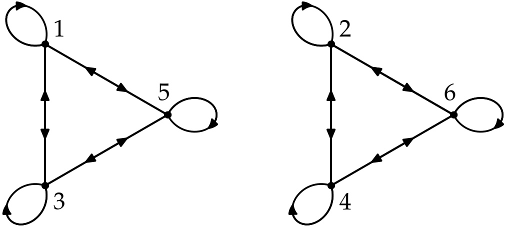
defines the relation 'strictly less than' on X. An analogous relation can be defined replacing X with any other subset of $\mathbb{R}$.

Diagrams

Let X be a set and let $\sim$ be a relation defined on X. To represent $\sim$ on a diagram, draw a dot for each element of X. Then for each x, $y \in X$ such that $x \sim y$, draw an arrow *from* x *to* y. If $x \sim x$ draw a loop from x to itself.

Example 9.3

Let $X = \{1, 2, 3, 4, 5, 6\}$. The relation $x \equiv y$ mod 2 on X is:



Exercise: Draw a similar diagram for the relation on $\{1, 2, 3, 4, 5, 6\}$ defined by

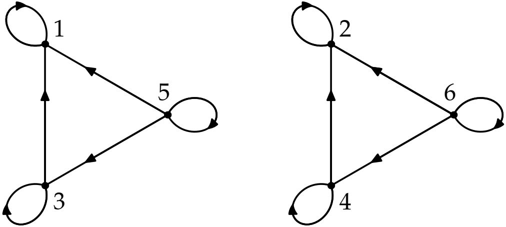
$$x \sim y \iff x - y \text{ is even and } x > y.$$

Diagrams

Let X be a set and let $\sim$ be a relation defined on X. To represent $\sim$ on a diagram, draw a dot for each element of X. Then for each $x, y \in X$ such that $x \sim y$, draw an arrow *from* x *to* y. If $x \sim x$ draw a loop from x to itself.

Example 9.3

Let $X = \{1, 2, 3, 4, 5, 6\}$. The relation $x \equiv y$ mod 2 on X is:



Exercise: Draw a similar diagram for the relation on $\{1, 2, 3, 4, 5, 6\}$ defined by

$$x \sim y \iff x - y \text{ is even and } x > y.$$

Properties of relations

Definition 9.4

Let $\sim$ be a relation on a set X. We say that $\sim$ is

(i) *reflexive* if $x \sim x$ for all $x \in X$;

(ii) *symmetric* if for all $x, y \in X$,

$$x \sim y \Longrightarrow y \sim x;$$

(iii) *transitive* if for all $x, y, z \in X$,

$$x \sim y \text{ and } y \sim z \Longrightarrow x \sim z.$$

A relation that is reflexive, symmetric and transitive is said to be an *equivalence relation*.

Example 9.5

Fix $m \in \mathbb{N}$. The congruence relation $n \equiv n' \bmod m$ is an equivalence relation on $\mathbb{Z}$.

More on Relations

In general a relation can have any combination of the properties reflexive, symmetric and transitive. See Question 2 of Sheet 10.

Exercise 9.7

Let X be the set of people sitting in a full lecture room. For each of the following relations, decide whether it is (i) reflexive, (ii) symmetric and (iii) transitive.

(a) $x \sim y$ if x and y are sitting in the same row,

(b) $x \sim y$ if x is sitting in a strictly higher row than y,

(c) $x \sim y$ if x and y are friends.

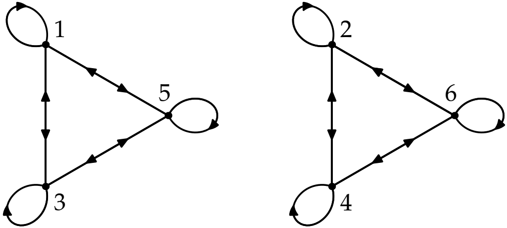
Equivalence relations and partitions

Suppose that $\sim$ is an equivalence relation on a set X. For $x \in X$, we define the *equivalence class of* x to be the set of all elements of X that relate to x. In symbols

$$[x] = \{z \in X : z \sim x\}.$$

For example, the equivalence classes for the relation $x \equiv y \bmod 2$ on the set $\{1, 2, 3, 4, 5, 6\}$ are

$$[0] = [2] = [4] = \{0, 2, 4\}$$
$$[1] = [3] = [5] = \{1, 3, 5\}$$



Main Theorem on Equivalence Classes

Theorem 9.8

Let $\sim$ be an equivalence relation on a set X. Let $x, y \in X$.

(i) $x \in [x]_\sim$,

(ii) $x \sim y \iff [x]_\sim = [y]_\sim$,

(ii) $x \not\sim y \iff [x]_\sim \cap [y]_\sim = \varnothing$.

Thus, by (i), every element of X lies in an equivalence class, and by (ii) and (iii), X is a disjoint union of the distinct equivalence classes.

The proof of Theorem 9.8 is non-examinable and will be skipped if time is pressing. See Theorem 31.13 in *How to think like a mathematician* for a careful (and exhaustively analysed) proof.

The Number System $\mathbb{Z}_m$ of Integers Modulo m.

Fix $m \in \mathbb{N}$. Let

$$\mathbb{Z}_m = \{[n] : n \in \mathbb{Z}\}$$

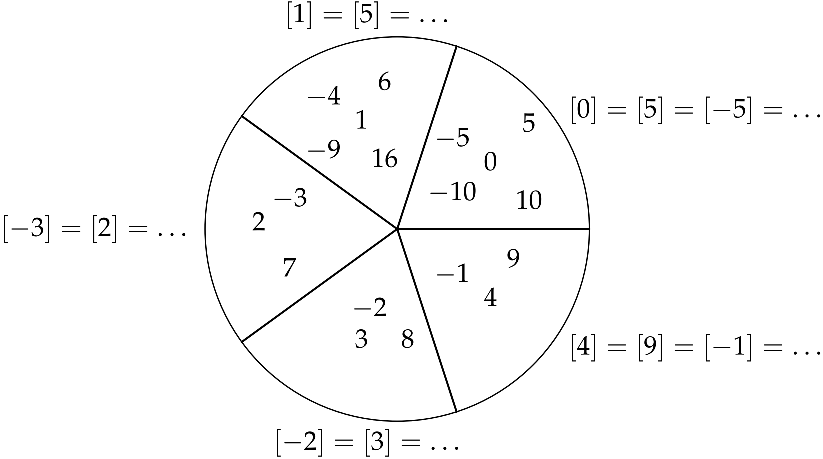
be the set of equivalence classes for congruence modulo m.

The Number System $\mathbb{Z}_m$ of Integers Modulo m.

Fix $m \in \mathbb{N}$. Let

$$\mathbb{Z}_m = \{[n] : n \in \mathbb{Z}\}$$

be the set of equivalence classes for congruence modulo m.
For example, $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$.



Addition and Multiplication in $\mathbb{Z}_m$

We turn the set $\mathbb{Z}_m$ of equivalence classes into a number system by defining addition and multiplication as follows.

Definition 9.9

Fix $m \in \mathbb{N}$. Given $[r], [s] \in \mathbb{Z}_m$ we define $[r] + [s] = [r + s]$ and $[r][s] = [rs]$.

Exercise 9.10

Recall that a square number is a number of the form n^2 where $n \in \mathbb{N}$.

(i) Calculate $1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, \ldots$ modulo 4. State and prove a conjecture on the pattern you observe.

(ii) Is 2015 the sum of two square numbers?

Addition and Multiplication Tables

Example 9.11

The addition and multiplication tables for $\mathbb{Z}_5$ are shown below. For example, the entry in the addition table in the row for [4] and the column for [3] is

$$[4] + [3] = [2]$$

since $4 + 3 = 7$ and $7 \equiv 2 \bmod 5$.

$+$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

$\times$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

You may omit [0] from the multiplication table if you prefer.

§10 Rings

Definition 10.1

Suppose that R is a set on which addition and multiplication are defined, so that given any two elements $x, y \in R$, their sum $x + y$ and product xy are elements of R. Then R is a ring if

(1) (*Commutative law of addition*) $x + y = y + x$ for all $x, y \in R$,

(2) (*Existence of zero*) There is an element $0 \in R$ such that $0 + x = x$ for all $x \in R$,

(3) (*Existence of additive inverses*) For each $x \in R$ there exists an element $-x \in R$ such that $-x + x = 0$, where 0 is the element in property (2),

(4) (*Associative law of addition*) $(x + y) + z = x + (y + z)$ for all $x, y, z \in R$,

(5) (*Existence of one*) There exists an element $1 \in R$ such that $1x = x1 = x$ for all $x \in R$,

(6) (*Associative law of multiplication*) $(xy)z = x(yz)$ for all $x, y, z \in R$,

(7) (*Distributivity*) $x(y + z) = xy + xz$ and $(x + y)z = xz + yz$ for all $x, y, z \in R$.

The number systems $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ and $\mathbb{Z}_m$ for $m \in \mathbb{N}$ are rings.

Fields

Definition 10.2

(i) A ring R is *commutative* if $xy = yx$ for all $x, y \in R$.

(ii) A commutative ring R is a *field* if for all non-zero $x \in R$ there exists an element $y \in R$ such that $xy = yx = 1$, where 1 is the one element in property (5). We say that y is the *inverse* of x and write $y = x^{-1}$.

Some familiar examples of fields are $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$. More interestingly, $\mathbb{Z}_5$ is a field.

Theorem 10.3 (Examinable)

If p is prime then $\mathbb{Z}_p$ is a field.

Example 10.4

See board.

Properties of Rings

Lemma 10.5

Let R be a ring.

(i) There is a unique zero element in R satisfying property *(2)*.

(ii) There is a unique one element in R satisfying property *(5)*.

(iii) For each $x \in R$ there exists a unique $y \in R$ such that $y + x = x + y = 0$.

(iv) If x, $z \in R$ and $x + z = x$ then $z = 0$.

(v) We have $0x = 0 = x0$ for all $x \in R$.

(vi) We have $-x = (-1)x = x(-1)$ for all $x \in R$.

(vii) For all $x \in R$ we have $-(-x) = x$. [**typo** $x \in R$**, not** $x \in X$]

(viii) For all x, $y \in R$ we have

$$-(xy) = (-x)y = y(-x) \text{ and } (-x)(-y) = xy.$$

(ix) $0 = 1$ if and only if $R = \{0\}$.

Polynomial Rings

We define polynomial rings over an arbitrary field: the main examples to bear in mind are $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Z}_p$ for prime p.

Definition 10.6

Let F be a field. Let $F[x]$ denote the set of all polynomials

$$f(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0$$

where $d \in \mathbb{N}_0$ and $a_0, a_1, a_2, \ldots, a_d \in F$. If $d = 0$, so $f(x) = a_0$, then $f(x)$ is a *constant polynomial*.

Polynomial Rings

We define polynomial rings over an arbitrary field: the main examples to bear in mind are $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Z}_p$ for prime p.

Definition 10.6

Let F be a field. Let $F[x]$ denote the set of all polynomials

$$f(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0$$

where $d \in \mathbb{N}_0$ and $a_0, a_1, a_2, \ldots, a_d \in F$. If $d = 0$, so $f(x) = a_0$, then $f(x)$ is a *constant polynomial*.

When writing polynomials we usually omit coefficients of 1, and do not include powers of x whose coefficient is 0. For example, in $\mathbb{Z}_2[x]$, we write $x^2 + [1]$ rather than $[1]x^2 + [0]x + [1]$.

The x in $f(x)$ is called an *indeterminate*. You can think of it as standing for an unspecified element of F.

Ring Structure of $F[x]$

Polynomials are added and multiplied in the expected way.

Example 10.7

In $\mathbb{Z}_3[x]$, we have

$$\begin{aligned}
&(x^4 + [2]x^3 + [1]) + ([2]x^4 + x^2 + [1]) \\
&= ([1]x^4 + [2]x^3 + [1]) + ([2]x^4 + [1]x^2 + [1]) \\
&= ([1] + [2])x^4 + [2]x^3 + [1]x^2 + ([1] + [1]) \\
&= [0]x^4 + [2]x^3 + [1]x^2 + [2]
\end{aligned}$$

and

$$(x + [1])(x + [2]) = x^2 + ([1] + [2])x + [1][2] = x^2 + [2].$$

Ring Structure of $F[x]$

Polynomials are added and multiplied in the expected way.

Example 10.7

In $\mathbb{Z}_3[x]$, we have

$$\begin{aligned} &(x^4 + [2]x^3 + [1]) + ([2]x^4 + x^2 + [1]) \\ = &([1]x^4 + [2]x^3 + [1]) + ([2]x^4 + [1]x^2 + [1]) \\ &= ([1] + [2])x^4 + [2]x^3 + [1]x^2 + ([1] + [1]) \\ &= [0]x^4 + [2]x^3 + [1]x^2 + [2] \end{aligned}$$

and

$$(x + [1])(x + [2]) = x^2 + ([1] + [2])x + [1][2] = x^2 + [2].$$

Ring Structure of $F[x]$

Polynomials are added and multiplied in the expected way.

Example 10.7

In $\mathbb{Z}_3[x]$, we have

$$\begin{aligned}
&(x^4 + [2]x^3 + [1]) + ([2]x^4 + x^2 + [1]) \\
&= ([1]x^4 + [2]x^3 + [1]) + ([2]x^4 + [1]x^2 + [1]) \\
&= ([1] + [2])x^4 + [2]x^3 + [1]x^2 + ([1] + [1]) \\
&= [0]x^4 + [2]x^3 + [1]x^2 + [2]
\end{aligned}$$

and

$$(x + [1])(x + [2]) = x^2 + ([1] + [2])x + [1][2] = x^2 + [2].$$

Ring Structure of $F[x]$

Polynomials are added and multiplied in the expected way.

Example 10.7

In $\mathbb{Z}_3[x]$, we have

$$\begin{aligned} &(x^4 + [2]x^3 + [1]) + ([2]x^4 + x^2 + [1]) \\ = &([1]x^4 + [2]x^3 + [1]) + ([2]x^4 + [1]x^2 + [1]) \\ &= ([1] + [2])x^4 + [2]x^3 + [1]x^2 + ([1] + [1]) \\ &= [0]x^4 + [2]x^3 + [1]x^2 + [2] \end{aligned}$$

and

$$(x + [1])(x + [2]) = x^2 + ([1] + [2])x + [1][2] = x^2 + [2].$$

Ring Structure of $F[x]$

Polynomials are added and multiplied in the expected way.

Example 10.7

In $\mathbb{Z}_3[x]$, we have

$$\begin{aligned}
&(x^4 + [2]x^3 + [1]) + ([2]x^4 + x^2 + [1]) \\
&= ([1]x^4 + [2]x^3 + [1]) + ([2]x^4 + [1]x^2 + [1]) \\
&\qquad = ([1] + [2])x^4 + [2]x^3 + [1]x^2 + ([1] + [1]) \\
&\qquad = [0]x^4 + [2]x^3 + [1]x^2 + [2]
\end{aligned}$$

and

$$(x + [1])(x + [2]) = x^2 + ([1] + [2])x + [1][2] = x^2 + [2].$$

Ring Structure of $F[x]$

Polynomials are added and multiplied in the expected way.

Example 10.7

In $\mathbb{Z}_3[x]$, we have

$$\begin{aligned}
&(x^4 + [2]x^3 + [1]) + ([2]x^4 + x^2 + [1]) \\
= &([1]x^4 + [2]x^3 + [1]) + ([2]x^4 + [1]x^2 + [1]) \\
&= ([1] + [2])x^4 + [2]x^3 + [1]x^2 + ([1] + [1]) \\
&= [0]x^4 + [2]x^3 + [1]x^2 + [2] \\
&= [2]x^3 + x^2 + [2]
\end{aligned}$$

and

$$(x + [1])(x + [2]) = x^2 + ([1] + [2])x + [1][2] = x^2 + [2].$$

Polynomial Division

Definition 10.8

Let $f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_2x^2 + a_1x + a_0$ where $a_d \neq 0$.

(i) We say that d is the *degree* of $f(x)$ and write $\deg f(x) = d$.

(ii) The *leading coefficient* of $f(x)$ is a_d. If $a_d = 1$ we say that $f(x)$ is *monic*.

The degree of zero polynomial $f(x) = 0$ is undefined.

Polynomial Division

Definition 10.8

Let $f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_2x^2 + a_1x + a_0$ where $a_d \neq 0$.

(i) We say that d is the *degree* of $f(x)$ and write $\deg f(x) = d$.

(ii) The *leading coefficient* of $f(x)$ is a_d. If $a_d = 1$ we say that $f(x)$ is *monic*.

The degree of zero polynomial $f(x) = 0$ is undefined.

Theorem 10.9

Let F be a field, let $f(x) \in F[x]$ be a non-zero polynomial and let $g(x) \in F[x]$. There exist polynomials $q(x), r(x) \in F[x]$ such that

$$g(x) = q(x)f(x) + r(x)$$

and either $r(x) = 0$ or $\deg r(x) < \deg f(x)$.

Examples of Polynomial Division

Example 10.10

(1) Working in $\mathbb{Q}[x]$, let $g(x) = 3x^2 + 2x - 1$ and let $f(x) = 2x + 1$. Then

$$g(x) = (\tfrac{3}{2}x + \tfrac{1}{4})f(x) - \tfrac{5}{4}$$

so the quotient is $q(x) = \frac{3}{2}x + \frac{1}{4}$ and the remainder is $r(x) = -\frac{5}{4}$. If instead we take $h(x) = x + 1$ then

$$g(x) = (3x - 1)h(x).$$

So when $g(x)$ is divided by $h(x)$ the quotient is $3x - 1$ and the remainder is 0.

(2) Working in $\mathbb{Z}_3[x]$, let $g(x) = x^4 + x^3 + [2]x^2 + x + 1$ and let $f(x) = x^2 + x$. Then

$$g(x) = (x^2 + [2]x)f(x) + 2[x] + 1.$$

Remainder Theorem

Theorem 10.11

Let F be a field and let $f(x) \in F[x]$ be a polynomial. Let $c \in F$. Then

$$f(x) = q(x)(x - c) + r$$

for some polynomial $q(x) \in F[x]$ and some $r \in \mathbb{F}$. Moreover $f(c) = 0$ if and only if $r = 0$.

Example of Remainder Theorem

Example 10.12

Working in $\mathbb{Z}_3[x]$, let $g(x) = x^4 + x^3 + [2]x^2 + x + [1]$ as in Example 10.10(2). Since

$$g([1]) = [1] + [1] + [2] + [1] + [1] = [6] = [0],$$

the Factor Theorem says that $x - [1]$ divides $g(x)$. Division gives

$$g(x) = (x - [1])(x^3 + [2]x^2 + x + [2]).$$

The cubic $x^3 + [2]x^2 + x + [2]$ also has $[1]$ as a root. Dividing it by $x - [1]$ gives

$$g(x) = (x - [1])^2(x^2 + [1]).$$

Therefore $g(x)$ has $[1]$ as a root with multiplicity 2, and no other roots in $\mathbb{Z}_3$.

Polynomials in $\mathbb{C}[x]$

We end with a corollary of Theorem 10.9 that gives a stronger version of the Fundamental Theorem of Algebra (Theorem 3.21).

Corollary 10.13

Let $f(x) \in \mathbb{C}[x]$ be a polynomial of degree n. There exist distinct $w_1, w_2, \ldots, w_r \in \mathbb{C}$ and $m_1, \ldots, m_r \in \mathbb{N}$ such that

$$m_1 + \cdots + m_r = n$$

and

$$\begin{aligned} a_n z^n + a_{n-1} z^{n-1} + \ \cdots + a_1 z + a_0 \\ = a_n (z - w_1)^{m_1} (z - w_2)^{m_2} \ldots (z - w_r)^{m_r}. \end{aligned}$$

Almost all the Comments

> *I don't think the library is a welcoming place to study . . . I suggest to improve the library. There are no extraneous notes for the course on moodle, the lecturer should put his notes for us to study from as well.*

Reply: the 60+ pages of notes I have written/am writing for this course are all on Moodle. You also have detailed answers to all the problem sheets. There is nothing 'extra' I am keeping from you.

Almost all the Comments

> *I don't think the library is a welcoming place to study . . . I suggest to improve the library. There are no extraneous notes for the course on moodle, the lecturer should put his notes for us to study from as well.*

Reply: the 60+ pages of notes I have written/am writing for this course are all on Moodle. You also have detailed answers to all the problem sheets. There is nothing 'extra' I am keeping from you.

> The tutor explained things well: *Do not have a tutor*

Clarification: for the first three questions, 'tutor' means your lecturer.

Almost all the Comments

> *I don't think the library is a welcoming place to study ... I suggest to improve the library. There are no extraneous notes for the course on moodle, the lecturer should put his notes for us to study from as well.*

Reply: the 60+ pages of notes I have written/am writing for this course are all on Moodle. You also have detailed answers to all the problem sheets. There is nothing 'extra' I am keeping from you.

> The tutor explained things well: *Do not have a tutor*

Clarification: for the first three questions, 'tutor' means your lecturer.

> *Please turn off air conditioning in the lecture hall during winter mornings.*

Reply: the controls are at the front.