MT181 Number Systems

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

Administration:

- If you are taking MT194 Numbers and Functions you must attend a meeting to arrange tutorial times with your tutor. Some meetings are at 11am today. Check your college email account or the noticeboard in the department.
- Workshops begin next week.
- Sign-in sheet. **Please return to the lecturer after each lecture.**
- Make sure you get the Part A Notes, Problem Sheet 1, and the sheet of Challenge Problems when they are passed around.
- All handouts will be put on Moodle: moodle.rhul.ac.uk

MT181 Number Systems

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

Administration:

- If you are taking MT194 Numbers and Functions you must attend a meeting to arrange tutorial times with your tutor. Some meetings are at 11am today. Check your college email account or the noticeboard in the department.
- Workshops begin next week.
- Sign-in sheet. **Please return to the lecturer after each lecture.**
- Make sure you get the Part A Notes, Problem Sheet 1, and the sheet of Challenge Problems when they are passed around.
- All handouts will be put on Moodle: moodle.rhul.ac.uk
- **Lectures in BLT1:** Monday 9am, Thursday 9am, Friday 9am.
- **Office hours in McCrea 240:** Tuesday 11am, Wednesday 2pm and Friday 3pm.

Recommended Reading

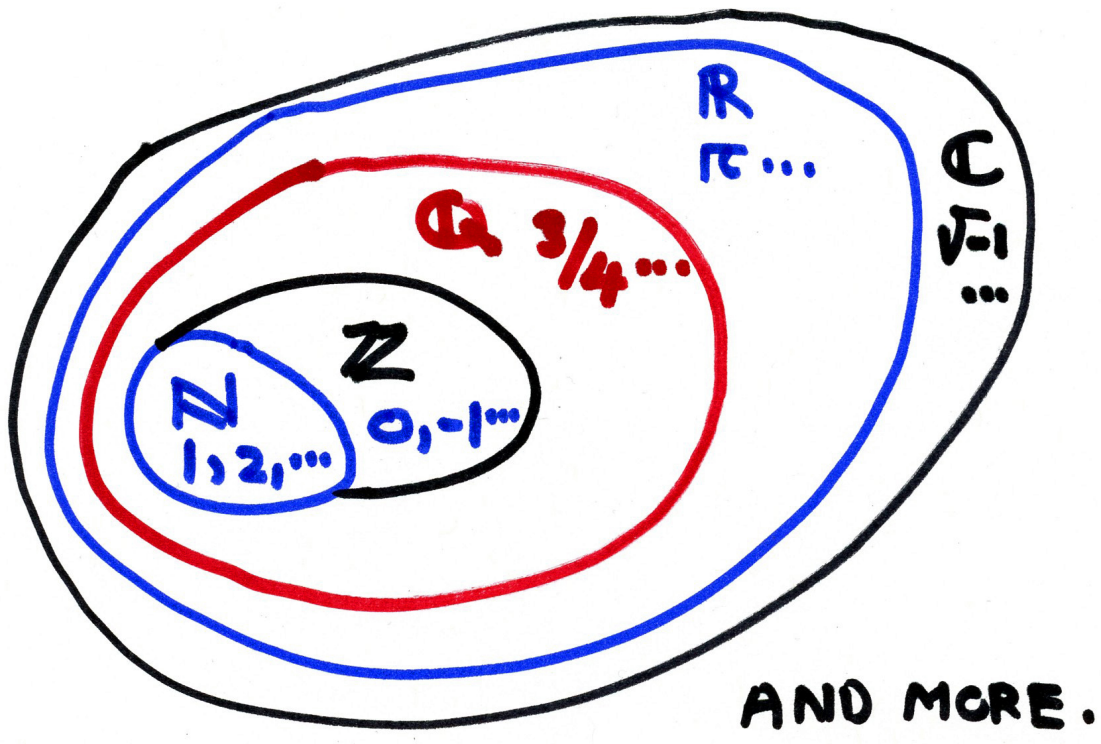
[1] *How to think like a mathematician*. Kevin Houston, Cambridge University Press, 2009.

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

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

Overview

This course will give a straightforward introduction to the fundamental number systems used in mathematics: the natural numbers $\mathbb{N}$, the integers $\mathbb{Z}$, the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, the complex numbers $\mathbb{C}$, the integers modulo a prime $\mathbb{Z}_p$, and others. In parallel, we will develop the basic language of pure mathematics: sets, functions, relations, propositions, etc.



Problem Sheets and Other Exercises

- There will be eight compulsory problem sheets. Each problem sheet is worth 1.25% of your overall grade. This mark is awarded for any reasonable attempt at each sheet.
- Doing the exercises in the notes will help you to review the ideas from lectures. Some exercises will be used for quizzes in lectures.
- Optional questions on problem sheets are harder than average. They are non-examinable and included for interest only.

Problem Sheets and Other Exercises

- There will be eight compulsory problem sheets. Each problem sheet is worth 1.25% of your overall grade. This mark is awarded for any reasonable attempt at each sheet.
- Doing the exercises in the notes will help you to review the ideas from lectures. Some exercises will be used for quizzes in lectures.
- Optional questions on problem sheets are harder than average. They are non-examinable and included for interest only.

Other ways to make yourself think about the material.

- Read other books from the library.
- Discuss questions with your colleagues.
- Web: `www.cut-the-knot.org`, `math.stackexchange.com`.
- Check your answers to computational problems with computer algebra packages such as MATHEMATICA.

Part A: Complex Numbers

§1 Introduction: Sets and Numbers

Definition 1.1

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

If X is a set and x is an element of X then we write $x \in X$. If y is not an element of X then we write $y \notin X$.

Exercise 1.2

True or false?

(i) 29 is an element of the set of prime numbers;

(ii) 87 is an element of the set of prime numbers;

(ii) $\{2, 3, 5, 7, 11\} = \{5, 7, 11, 2, 3\}$;

(iv) Julian Assange is an element of the set of people who live in the Ecuadorian Embassy to the UK.

Part A: Complex Numbers

§1 Introduction: Sets and Numbers

Definition 1.1

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

If X is a set and x is an element of X then we write $x \in X$. If y is not an element of X then we write $y \notin X$.

Exercise 1.2

True or false?

(i) 29 is an element of the set of prime numbers; **TRUE**

(ii) 87 is an element of the set of prime numbers;

(ii) $\{2, 3, 5, 7, 11\} = \{5, 7, 11, 2, 3\}$;

(iv) Julian Assange is an element of the set of people who live in the Ecuadorian Embassy to the UK.

Part A: Complex Numbers

§1 Introduction: Sets and Numbers

Definition 1.1

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

If X is a set and x is an element of X then we write $x \in X$. If y is not an element of X then we write $y \notin X$.

Exercise 1.2

True or false?

(i) 29 is an element of the set of prime numbers; **TRUE**

(ii) 87 is an element of the set of prime numbers; **FALSE**

(ii) $\{2, 3, 5, 7, 11\} = \{5, 7, 11, 2, 3\}$;

(iv) Julian Assange is an element of the set of people who live in the Ecuadorian Embassy to the UK.

Part A: Complex Numbers

§1 Introduction: Sets and Numbers

Definition 1.1

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

If X is a set and x is an element of X then we write $x \in X$. If y is not an element of X then we write $y \notin X$.

Exercise 1.2

True or false?

(i) 29 is an element of the set of prime numbers; **TRUE**

(ii) 87 is an element of the set of prime numbers; **FALSE**

(ii) $\{2, 3, 5, 7, 11\} = \{5, 7, 11, 2, 3\}$; **TRUE**

(iv) Julian Assange is an element of the set of people who live in the Ecuadorian Embassy to the UK.

Part A: Complex Numbers

§1 Introduction: Sets and Numbers

Definition 1.1

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

If X is a set and x is an element of X then we write $x \in X$. If y is not an element of X then we write $y \notin X$.

Exercise 1.2

True or false?

(i) 29 is an element of the set of prime numbers; **TRUE**

(ii) 87 is an element of the set of prime numbers; **FALSE**

(ii) $\{2, 3, 5, 7, 11\} = \{5, 7, 11, 2, 3\}$; **TRUE**

(iv) Julian Assange is an element of the set of people who live in the Ecuadorian Embassy to the UK. **TRUE**

The Natural Numbers $\mathbb{N}$

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

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

One important property of the natural numbers is that if $m, n \in \mathbb{N}$ then $m + n \in \mathbb{N}$. Because of this we say that $\mathbb{N}$ is closed under addition.

Definition 1.3

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 $y \in X$. The terms *closed under multiplication* and *closed under subtraction* are defined analogously. We say that X is *closed under division* if $x/y \in X$ whenever $x \in X$, $y \in X$ and $y \neq 0$.

Exercise 1.4

Is the set $\mathbb{N}$ of natural numbers closed under (i) multiplication; (ii) subtraction; (iii) division?

- After this lecture the Student-Staff Committee elections for first year representatives will be held.
- Spare copies of handouts at front.

Integers $\mathbb{Z}$, Rational Numbers $\mathbb{Q}$ and Real Numbers $\mathbb{R}$

We write $\mathbb{Z}$ for the set of integers (also called whole numbers):

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

The integers are closed under subtraction, but not division.

Integers $\mathbb{Z}$, Rational Numbers $\mathbb{Q}$ and Real Numbers $\mathbb{R}$

We write $\mathbb{Z}$ for the set of integers (also called whole numbers):

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

The integers are closed under subtraction, but not division.

We write $\mathbb{Q}$ for the set of all rational numbers (also called fractions). More formally, $\mathbb{Q}$ is the set of all numbers that can be expressed as p/q where $p, q \in \mathbb{Z}$ and $q \neq 0$.

Integers $\mathbb{Z}$, Rational Numbers $\mathbb{Q}$ and Real Numbers $\mathbb{R}$

We write $\mathbb{Z}$ for the set of integers (also called whole numbers):

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

The integers are closed under subtraction, but not division.

We write $\mathbb{Q}$ for the set of all rational numbers (also called fractions). More formally, $\mathbb{Q}$ is the set of all numbers that can be expressed as p/q where $p, q \in \mathbb{Z}$ and $q \neq 0$.

We write $\mathbb{R}$ for the set of real numbers, thought of as all points on the real number line. So $0 \in \mathbb{R}$, $-1/2 \in \mathbb{R}$, $\sqrt{2} \in \mathbb{R}$, $\pi \in \mathbb{R}$.

Integers $\mathbb{Z}$, Rational Numbers $\mathbb{Q}$ and Real Numbers $\mathbb{R}$

We write $\mathbb{Z}$ for the set of integers (also called whole numbers):

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

The integers are closed under subtraction, but not division.

We write $\mathbb{Q}$ for the set of all rational numbers (also called fractions). More formally, $\mathbb{Q}$ is the set of all numbers that can be expressed as p/q where $p, q \in \mathbb{Z}$ and $q \neq 0$.

We write $\mathbb{R}$ for the set of real numbers, thought of as all points on the real number line. So $0 \in \mathbb{R}$, $-1/2 \in \mathbb{R}$, $\sqrt{2} \in \mathbb{R}$, $\pi \in \mathbb{R}$.

The rational numbers and the real numbers are closed under addition, subtraction, multiplication and division.

Complex Numbers $\mathbb{C}$

Definition 1.5

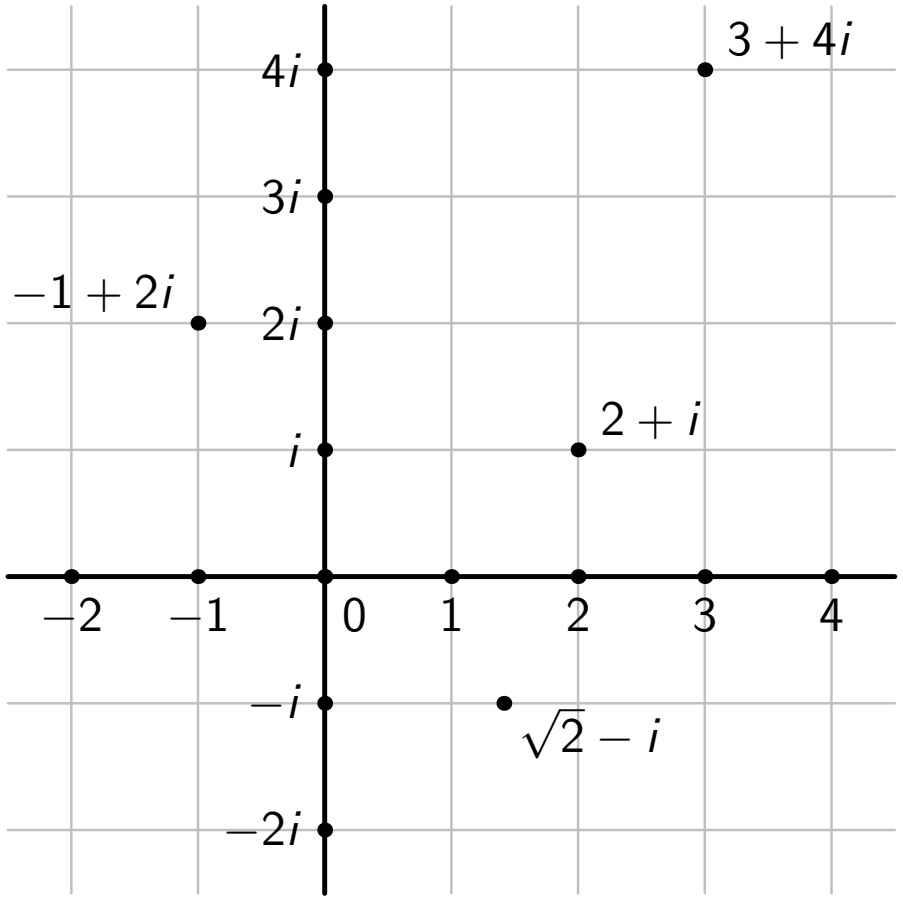
A *complex number* is an expression of the form $a + bi$ where $a, b \in \mathbb{R}$ and i is a special symbol with the property that $i^2 = -1$. The expression $a + bi$ is said to be in *Cartesian form*.

All the usual rules for adding, subtracting, multiplying and dividing complex numbers follow from the property that $i^2 = -1$.

The complex numbers are closed under addition, subtraction, multiplication and division.

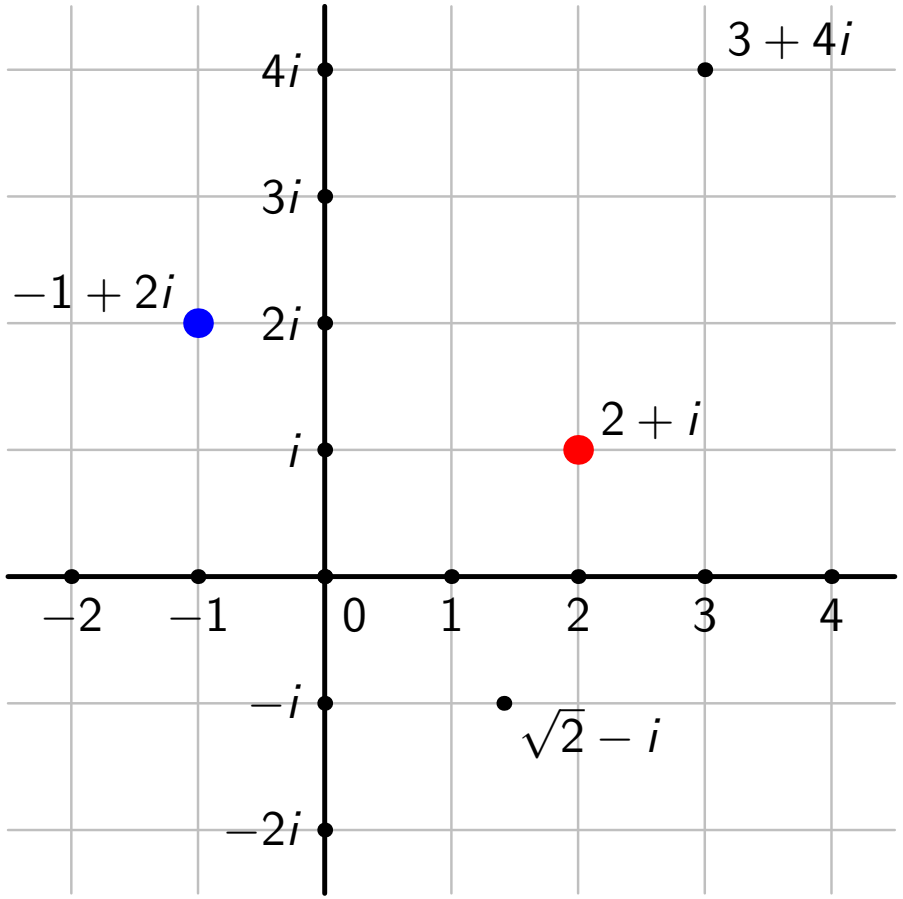
Argand Diagram

We represent complex numbers by points in a plane (called an *Argand diagram*) as shown below.



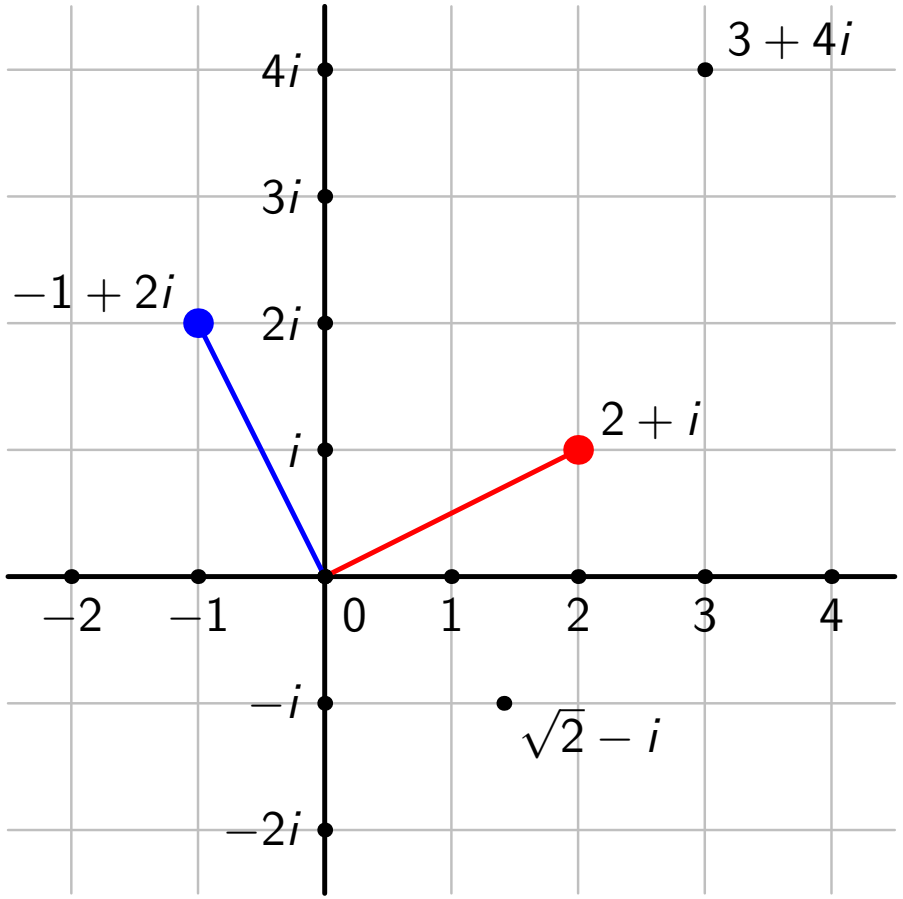
Argand Diagram

We represent complex numbers by points in a plane (called an *Argand diagram*) as shown below.



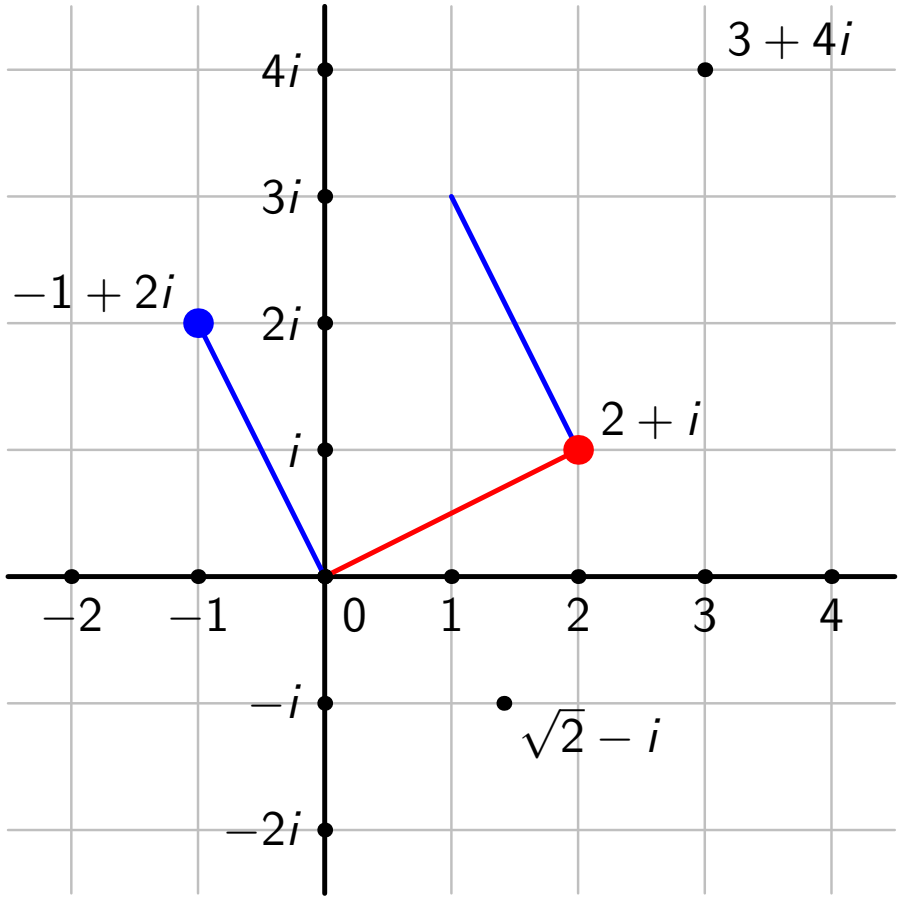
Argand Diagram

We represent complex numbers by points in a plane (called an *Argand diagram*) as shown below.



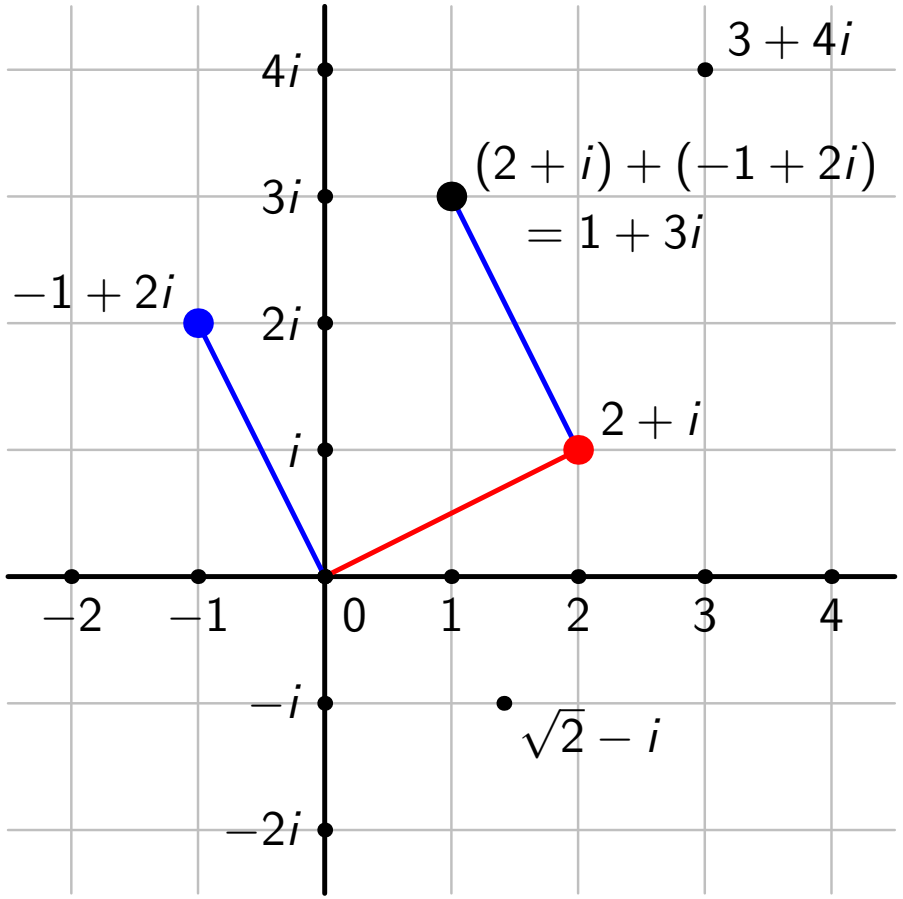
Argand Diagram

We represent complex numbers by points in a plane (called an *Argand diagram*) as shown below.



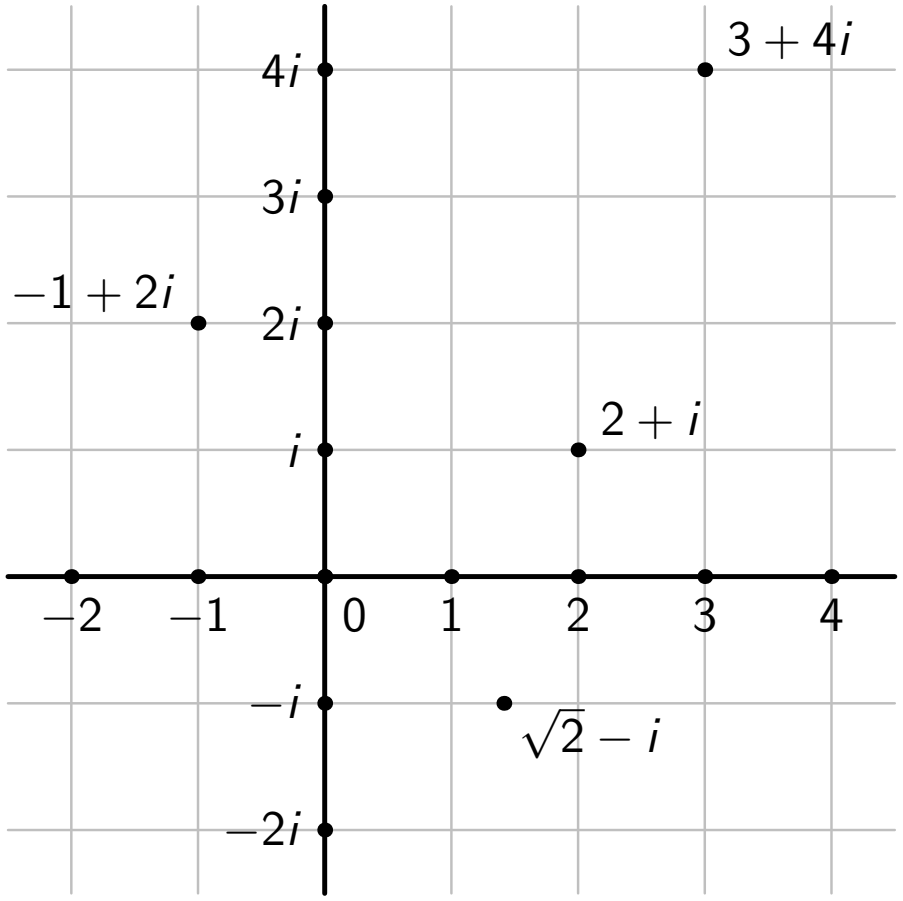
Argand Diagram

We represent complex numbers by points in a plane (called an *Argand diagram*) as shown below.



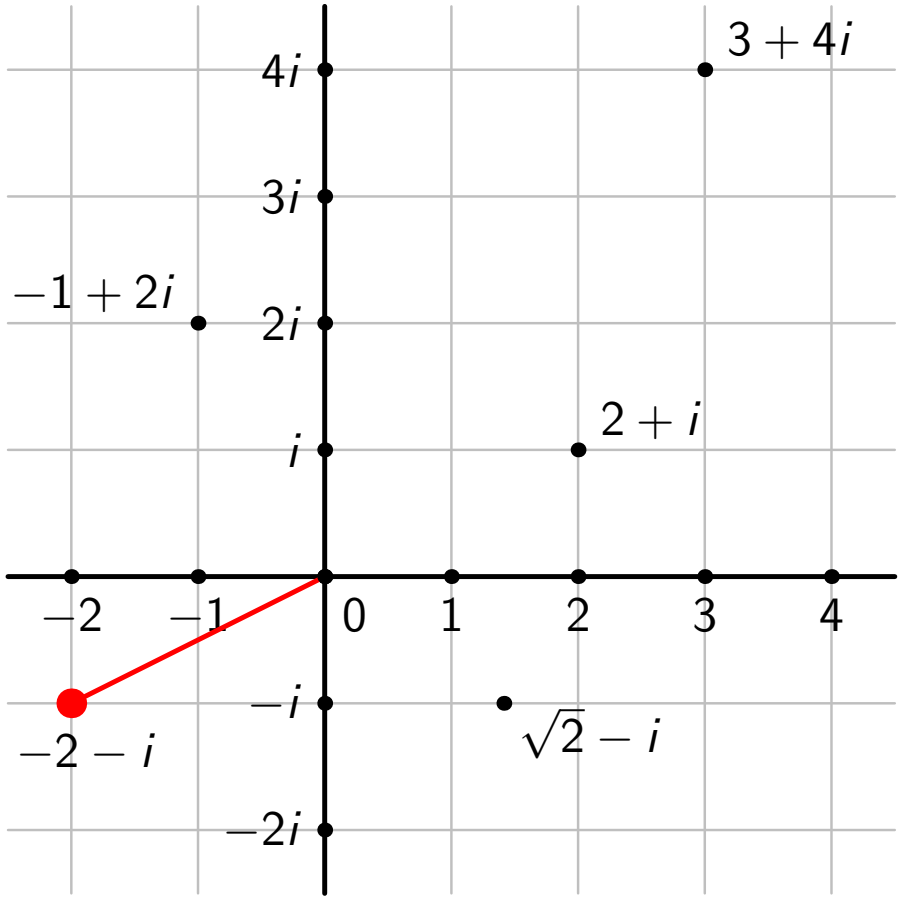
Argand Diagram

We represent complex numbers by points in a plane (called an *Argand diagram*) as shown below.



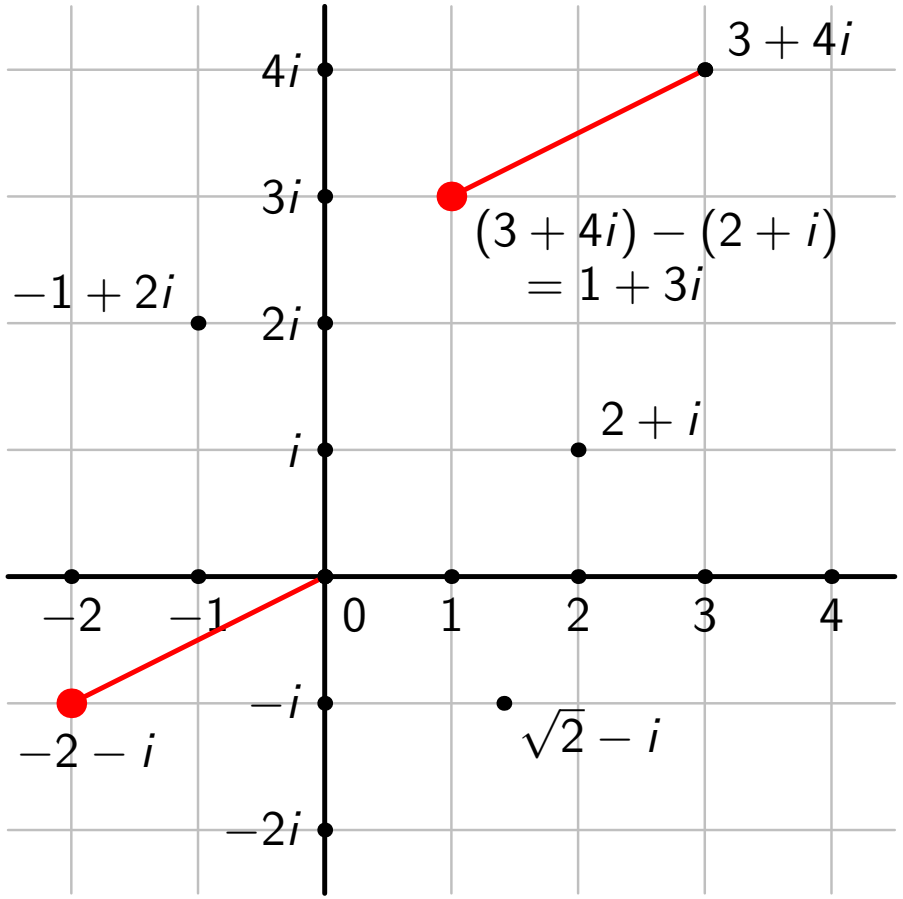
Argand Diagram

We represent complex numbers by points in a plane (called an *Argand diagram*) as shown below.



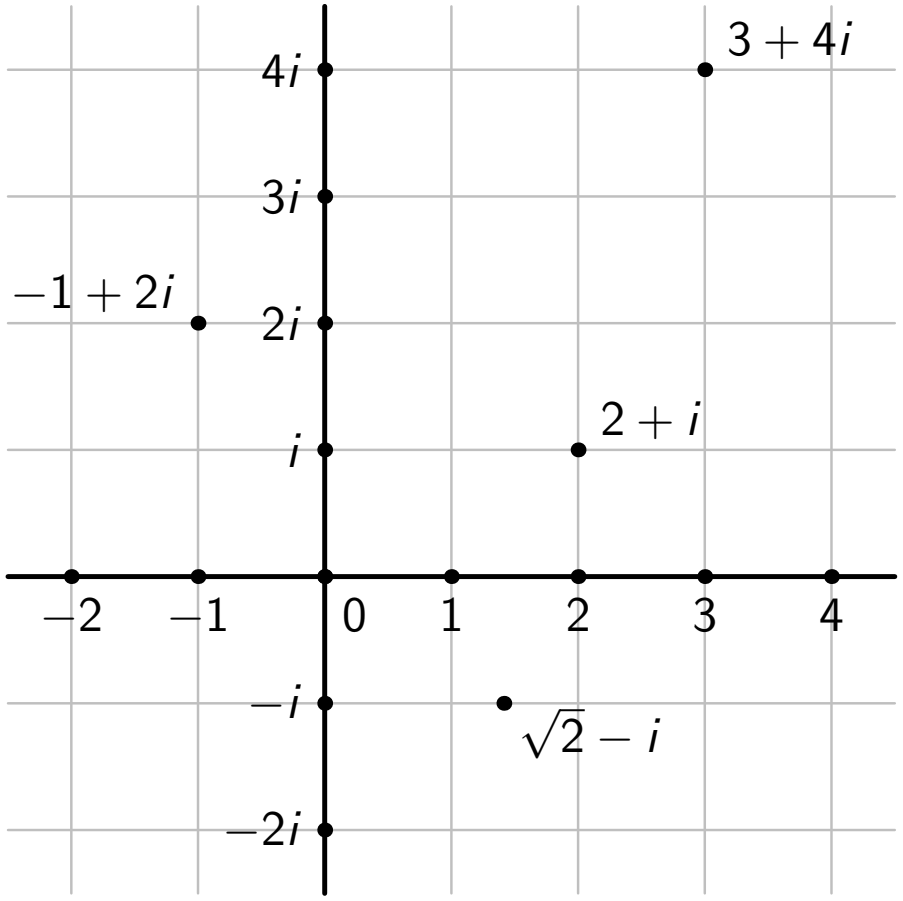
Argand Diagram

We represent complex numbers by points in a plane (called an *Argand diagram*) as shown below.



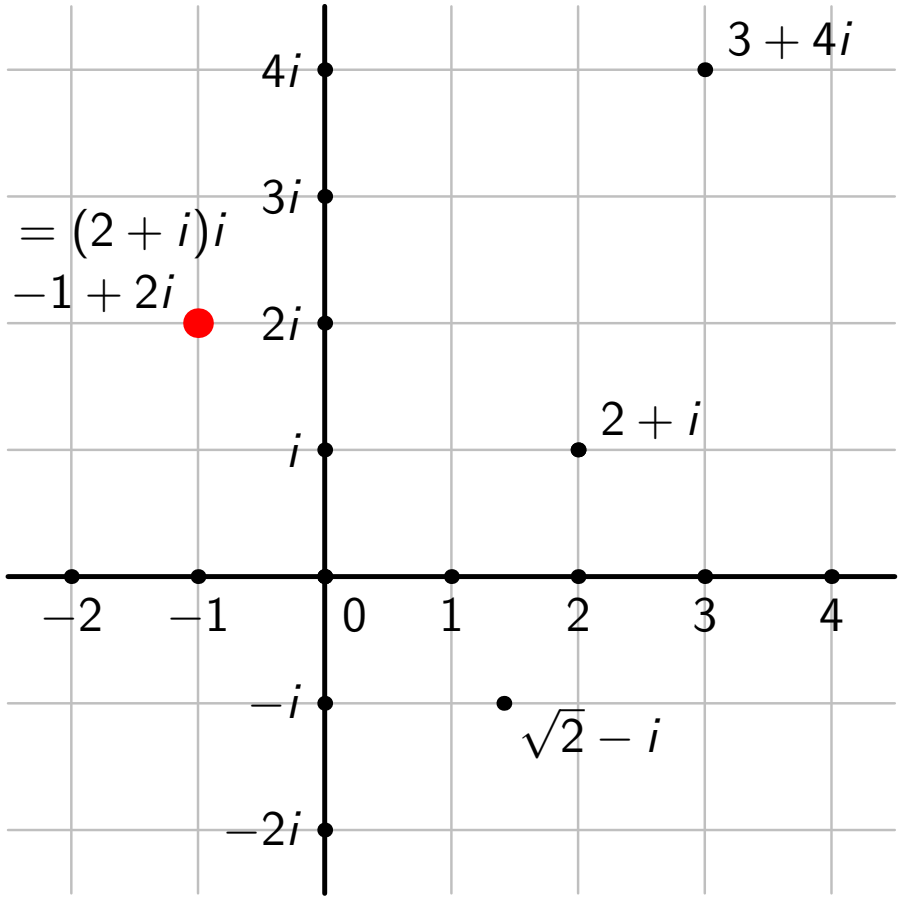
Argand Diagram

We represent complex numbers by points in a plane (called an *Argand diagram*) as shown below.



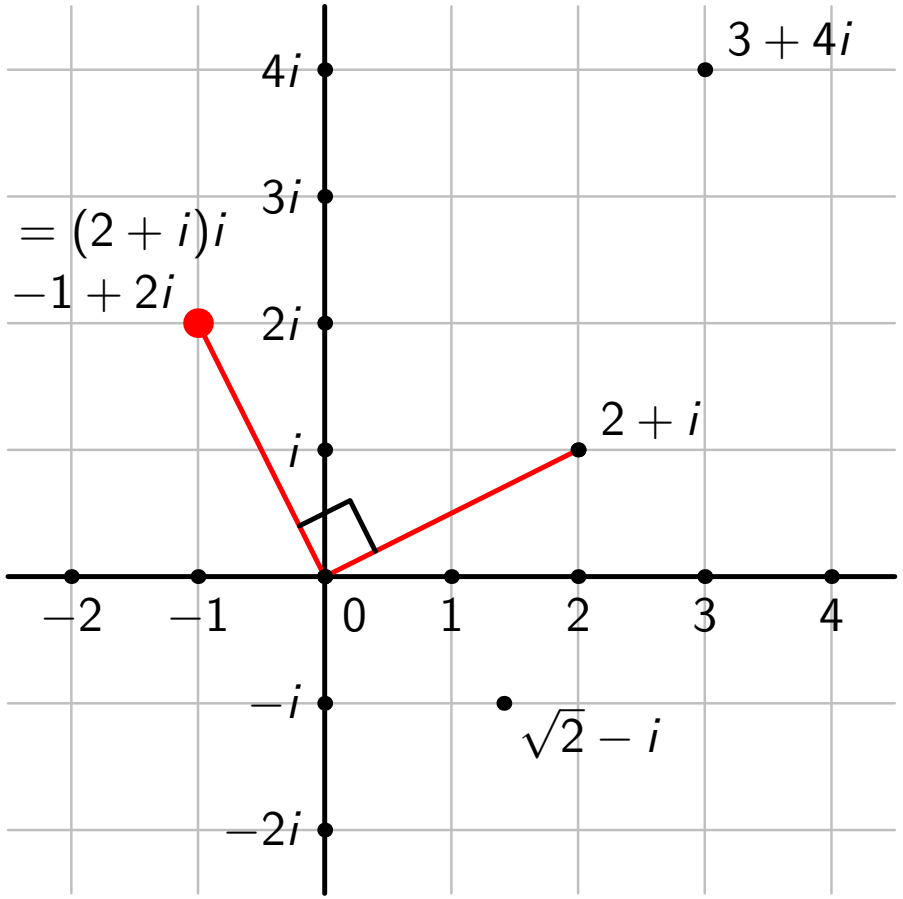
Argand Diagram

We represent complex numbers by points in a plane (called an *Argand diagram*) as shown below.



Argand Diagram

We represent complex numbers by points in a plane (called an *Argand diagram*) as shown below.



Administration

- Submit answers on paper (not in notebooks). Please staple multiple sheets together. Work submitted on Thursday will be returned on Monday.

Complex Conjugation

Definition 1.6

If $z = a + bi$ then we say that a is the *real part* of z and that b is the *imaginary part* of z, and write $\operatorname{Re} z = a$, $\operatorname{Im} z = b$.

The *complex conjugate* of $a + bi$ is $a - bi$. **We denote the complex conjugate of $z \in \mathbb{C}$ by $\bar{z}$.**

The *modulus* of $a + bi$ is $\sqrt{a^2 + b^2}$.

Claim 1.7

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

(i) $z\overline{z} = |z|^2$ *and* $|zw| = |z||w|$.

(ii) $\overline{\overline{z}} = z$,

(iii) $\overline{z + w} = \overline{z} + \overline{w}$, $\overline{zw} = \overline{z}\,\overline{w}$, *and* $\overline{z/w} = \overline{z}/\overline{w}$.

Exercise 1.8

Note that by Claim 1.7(i) [**misprinted as 1.8(i) in notes**], if $z \in \mathbb{C}$ and $z \neq 0$ then

$$1/z = \bar{z}/z\bar{z} = \bar{z}/|z|^2.$$

Use this to write $1/(c+di)$ and $(a+bi)/(c+di)$ in Cartesian form.

Polar Form of a Complex Number

Any complex number z can be written in the form

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

where $r > 0$ and θ is an angle. This is called the *polar form* of z. Observe that $|z| = r$. In this course all angles are measured in radians!

Definition 1.9

If $z = r(\cos\theta + i\sin\theta)$ then we say that θ is *an argument* of z, and write $\theta = \arg(z)$.

Definition 1.10

Let z be a non-zero complex number. 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 $\theta = \mathrm{Arg}(z)$.

Example 1.11

Let $z = 1 + i\sqrt{3}$. Then $\mathrm{Arg}(z) = \pi/3$ and the polar form of z is $z = 2(\cos\pi/3 + i\sin\pi/3)$.

Quiz

Let $z = 1 + i$.

- Write down a general form for the arguments of z.
- What is $\mathrm{Arg}(z)$?
- What is $\mathrm{Arg}(-z)$?

Imagine a rectangle with vertices at 0, 1, $1 + 2i$ and $2i$.

- What is the image of this rectangle under the transformation sending $z \in \mathbb{C}$ to $z + 3 + i$?
- What is the image of this square under the transformation sending $z \in \mathbb{C}$ to $2iz$?

Multiplication and Division in Polar Form

There is an easy way to multiply and divide complex numbers written in polar form.

Claim 1.12

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

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

Exercise 1.13

Let z, w be as in Claim 1.12 and suppose that $w \neq 0$. Find a similar expression for the polar form of z/w.

Another Set Closed Under the Arithmetic Operations

It is important, but maybe not very surprising, that the rational, real and complex numbers are each closed under addition, subtraction, multiplication and division. Here is a more surprising example, similar to Question 3(e) on Sheet 1. (Examples of this sort are important in number theory.)

Example 1.14

Let K be the set of all real numbers of the form $a + b\sqrt{2}$, where $a, b \in \mathbb{Q}$. Then K is closed under addition, subtraction, multiplication and division.

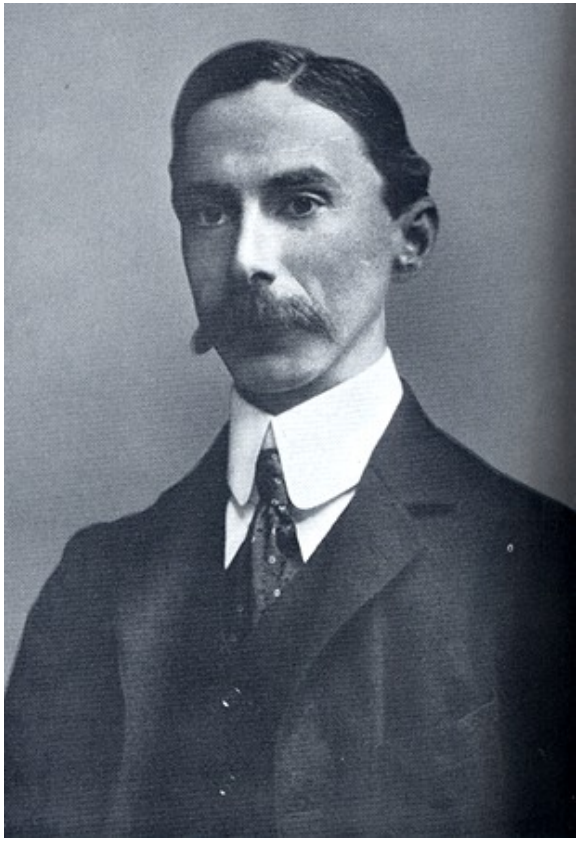
Aside on Set Theory

In this course we will deal with sets in an intuitive way. In particular, we allow sets to contain any object we can imagine (even Julian Assange).

This will be safe enough for this course. However, there are problems with unrestricted set formation. An important example is Bertrand Russell's set R, defined to be:

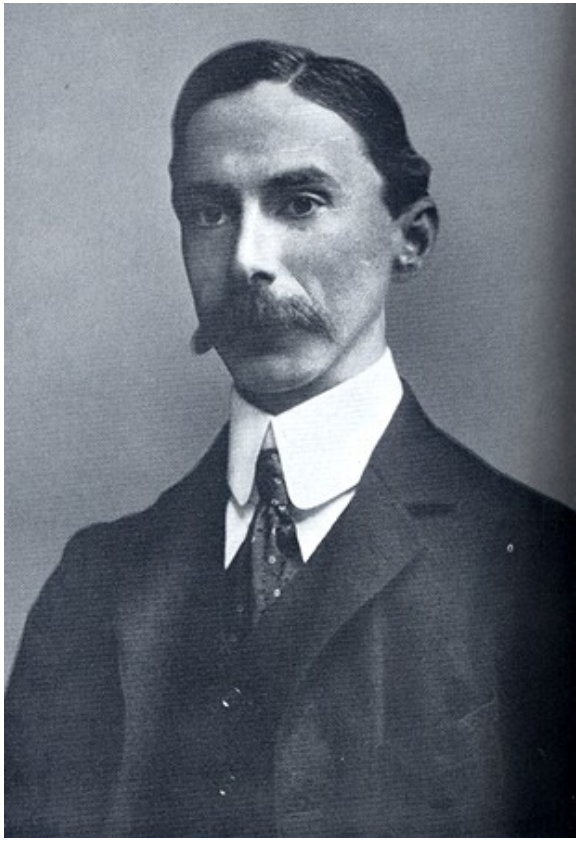
the set whose elements are
all sets X such that $X \notin X$.

Is R an element of R?



Aside on Set Theory

In this course we will deal with sets in an intuitive way. In particular, we allow sets to contain any object we can imagine (even Julian Assange).



This will be safe enough for this course. However, there are problems with unrestricted set formation. An important example is Bertrand Russell's set R, defined to be:

$$\text{the set whose elements are}$$
$$\text{all sets } X \text{ such that } X \notin X.$$

Is R an element of R? Either possibility leads to a contradiction!

Solution: put restrictions on the sets we are allowed to consider. Modern axiomatic set theory appears to be a sound foundation for mathematics.

Properties of complex numbers

Some motivation for the following definition will be given in lectures.

Definition 2.1

Given $z = a + bi \in \mathbb{C}$, we define

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

We call exp the *complex exponential function*.

Putting $z = i\theta$ in Definition 2.1 we get the **very useful** *Euler's formula*:

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

Lemma 2.2

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

$$\exp(z + w) = \exp z \exp w.$$

Trigonometric Identities

Putting $z = i\pi$ in Definition 2.1 (or $\theta = \pi$ in Euler's formula) gives

$$e^{i\pi} = -1.$$

In the form $e^{i\pi} + 1 = 0$, this identity unifies five fundamental mathematical constants.

Euler's formula gives quick proofs of the multiple-angle trigonometric identities.

Example 2.3

Take the special case of Euler's formula that

$$\cos 3\theta + i \sin 3\theta = e^{3i\theta}.$$

Rewrite the right-hand side as $(e^{i\theta})^3 = (\cos\theta + i \sin\theta)^3$, expand, and then compare real and imaginary parts to get

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

$$\sin 3\theta = -4\sin^3\theta + 3\sin\theta.$$

Exponential Form of a Complex Number and Roots

Let $z \in \mathbb{C}$. Suppose that z has polar form $z = r(\cos\theta + i\sin\theta)$ where $r = |z|$ and θ is an argument of z. Then $z = re^{i\theta}$. This is called the *exponential form* of z.

Exponential form is very useful for finding n-th roots of complex numbers.

Problem 2.5

Find the complex numbers z such that $z^3 = 8i$.

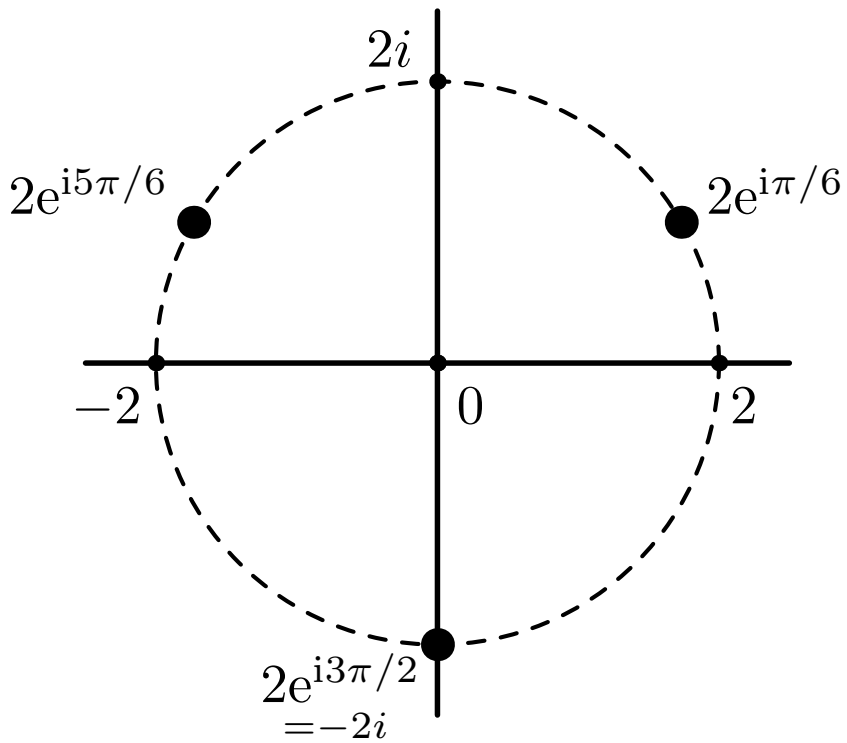
Exponential Form of a Complex Number and Roots

Let $z \in \mathbb{C}$. Suppose that z has polar form $z = r(\cos\theta + i\sin\theta)$ where $r = |z|$ and θ is an argument of z. Then $z = re^{i\theta}$. This is called the *exponential form* of z.

Exponential form is very useful for finding n-th roots of complex numbers.

Problem 2.5

Find the complex numbers z such that $z^3 = 8i$.



Log of a Complex Number

Let $z = re^{i\theta}$ be a complex number in exponential form. If $z = 0$ then there is no $w \in \mathbb{C}$ such that $e^w = z$. If $z \neq 0$ then the equation $e^w = z$ holds for all $w = a + bi \in \mathbb{C}$ such that $a = \log r$ and $b = \theta + 2\pi n$, for some $n \in \mathbb{Z}$.

For $z = re^{i\theta}$ with $z \neq 0$, we denote by $\log z$ any number of the form $w = \log r + i(\theta + 2\pi n)$ for some $n \in \mathbb{Z}$.

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 can be used to find the necessary square root.

Claim 2.6

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 $D^2 = b^2 - 4ac$.

Example 2.7

The equation $z^2 - 2z + (1 - i/2) = 0$ has solutions $3/2 + i/2$ and $1/2 - i/2$.

Fundamental Theorem of Algebra

The proof of this theorem is beyond the scope of this course.

Theorem 2.8 (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 $\mathbb{C}$.

We will see later in Part D of the course that it easily follows from the Fundamental Theorem of Algebra that there exist $w_1, w_2, \ldots, w_n \in \mathbb{C}$ such that

$$a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0 = a_n (z - w_1)(z - w_2) \ldots (z - w_n).$$

Exercise 2.9

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

Part B: Integers and Induction

§3 Induction and Sigma Notation

A proposition is a self-contained statement which is either true or false.

Example 3.1

Let P be the statement 'The integers are closed under addition'. Then P is a proposition and P is true. Let Q be the statement 'There is a real number x such that $x^2 + 1 = 0$. Then Q is a proposition and Q is false.

Some statements are too vague or subjective to be proposition. For example '3 is a pleasant sort of number' or 'houses in Englefield Green are too expensive'.

Predicates

Here is another statement which is not a proposition: '$n \geq 3$'. This statement is not a proposition because it is not self-contained: we cannot determine whether it is true or false without knowing n.

Definition 3.2

A *predicate* is a statement which depends on a variable n, and which becomes a proposition for each choice of n from a specified set.

Example 3.3

Let $P(n)$ denote the statement '$n^2 + n + 41$ is a prime number'. Then $P(n)$ is a predicate. Substituting particular natural numbers for n we get a sequence of propositions:

P(1): $1^2 + 1 + 41$ is a prime number,

P(2): $2^2 + 2 + 41$ is a prime number,

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

Quiz

Which of the following statements are propositions and which are predicates?

- $2^n \geq n^2 + 4$
- There are infinitely many primes
- If $n \in \mathbb{N}$ then there exist $r, s, t, u \in \mathbb{N}$ such that $n = r^2 + s^2 + t^2 + u^2$.
- Every number is the sum of m square numbers.

Quiz

Which of the following statements are propositions and which are predicates?

- $2^n \geq n^2 + 4$ **PREDICATE**
- There are infinitely many primes
- If $n \in \mathbb{N}$ then there exist $r, s, t, u \in \mathbb{N}$ such that $n = r^2 + s^2 + t^2 + u^2$.
- Every number is the sum of m square numbers.

Quiz

Which of the following statements are propositions and which are predicates?

- $2^n \geq n^2 + 4$ **PREDICATE**
- There are infinitely many primes **PROPOSITION**
- If $n \in \mathbb{N}$ then there exist $r, s, t, u \in \mathbb{N}$ such that $n = r^2 + s^2 + t^2 + u^2$.
- Every number is the sum of m square numbers.

Quiz

Which of the following statements are propositions and which are predicates?

- $2^n \geq n^2 + 4$ **PREDICATE**
- There are infinitely many primes **PROPOSITION**
- If $n \in \mathbb{N}$ then there exist $r, s, t, u \in \mathbb{N}$ such that $n = r^2 + s^2 + t^2 + u^2$. **PROPOSITION**
- Every number is the sum of m square numbers.

Quiz

Which of the following statements are propositions and which are predicates?

- $2^n \geq n^2 + 4$ **PREDICATE**
- There are infinitely many primes **PROPOSITION**
- If $n \in \mathbb{N}$ then there exist $r, s, t, u \in \mathbb{N}$ such that $n = r^2 + s^2 + t^2 + u^2$. **PROPOSITION**
- Every number is the sum of m square numbers. **PREDICATE**

The Principle of Mathematical Induction

Let $P(n)$ be a predicate defined for $n \in \mathbb{N}$, so $P(1)$, $P(2)$, ... are propositions. The Principle of Mathematical Induction states that if

- (i) $P(1)$ is true *and*
- (ii) for each $n \in \mathbb{N}$, if $P(n)$ is true then $P(n+1)$ is true;

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

Claim 3.5

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

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

Claim 3.6

For $n \in \mathbb{N}$ let $P(n)$ be the predicate

$$P(n): \ 2^{2n} - 1 \text{ is a multiple of 3.}$$

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

Base Case and Inductive Step

The case we prove to get the induction started is called the *base case*, and the argument to go from $P(n)$ to $P(n+1)$ is called the *inductive step*. In the statement of the Principle of Mathematical Induction above, the base case was the statement $P(1)$ for $n = 1$.

Sometimes it is necessary to take a different value of n for the base case.

Claim 3.7

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

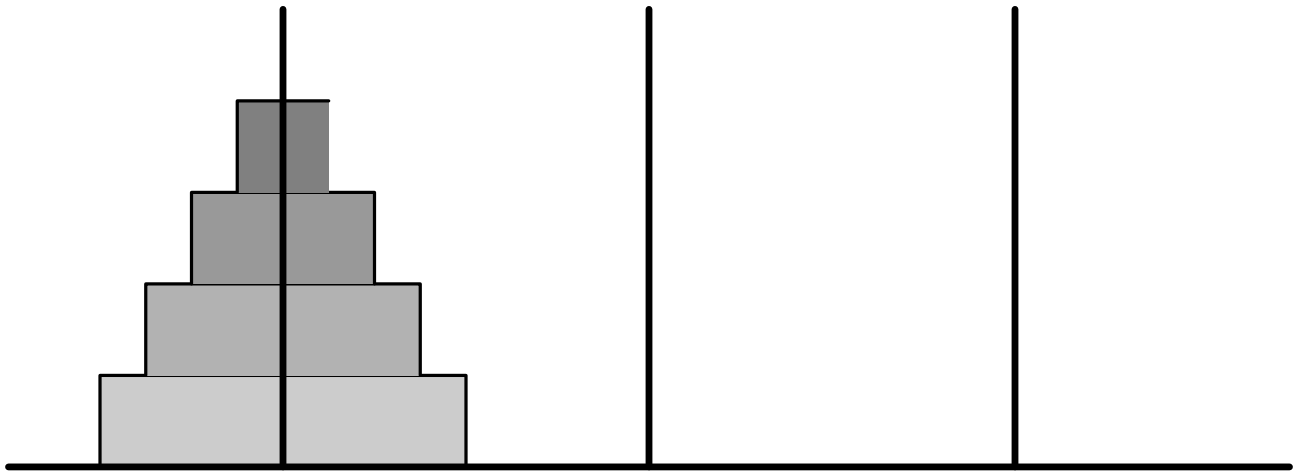
Problem Sheet 2

- If your surname starts with A to M your work is in the green folder. Otherwise it is in the blue folder. Please claim any older homework from the pink folder.
- Questions 4, 5 and 6 were marked. The main mark is out of 9, with a separate 0 or 1 mark for a reasonable attempt. (This becomes 1.25% of your final mark for this course.)
- On Moodle there is an extra file with some common errors. Please check your answer to Question 3 carefully: several people assumed that $\mathrm{Arg}(a+bi) = \tan^{-1}(b/a)$, but this only holds when $a, b > 0$.
- Please see the lecturer in an office hour to go through any of the questions.
- Problem Sheet 3 is due in this Thursday. Problem Sheet 4 will appear on Moodle by 5pm today.

Towers of Hanoi

Problem 3.8 (Towers of Hanoi)

You are given a board with three pegs. On peg number 1 *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 from 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 number 1 *to one of the other pegs. How many moves are required?*

Induction Exercises

Exercise 3.9

Prove by induction on n that no solution to the Towers of Hanoi Problem can use fewer moves than the solution found in lectures.

Exercise 3.10

Let $z \in \mathbb{C}$. Prove by induction on n that $\overline{z^n} = \overline{z}^n$ for all $n \in \mathbb{N}$. [*Hint:* for the inductive step, use that $\overline{zw} = \overline{z}\,\overline{w}$, as shown in Question 5 on Sheet 1.]

Sigma notation

If $a_1, a_2, \ldots a_n$ are complex numbers then we write their sum as $\sum_{k=1}^{n} a_k$. This may be read as

'the sum of a_k as k varies from 1 to n'

or 'sigma a_k for k from 1 to n'. we say that k is the *summation variable*. Here 1 is the *lower limit* and n is the *upper limit*.

Example 3.11

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) $\sum_{k=0}^{n} n = (n+1)n$.

Sigma Notation and Induction

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 $\sum_{j=1}^{n} j^2 - \sum_{k=2}^{n} (k-1)^2 =$

(A) 1 (B) n^2 (C) 42 (D) $n^2 - (n-1)^2$

Using Sigma notation, Claim 3.5 can be restated as

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

See Example 3.12 in the printed notes for a larger example.

Discussion on Induction

Is this argument valid? If not, where is the logical flaw?

(1) After dinner, a box of chocolates is passed clockwise around the table. Define

$P(n)$: *it is impolite to eat a chocolate when exactly n chocolates remain.*

Everyone knows it is impolite to eat the last chocolate, so $P(1)$ is true. Suppose $P(n)$ is true, and you are offered a choice of $n+1$ chocolates. If you eat a chocolate then

- *either* the person to your left eats a chocolate, which we know by induction is an impolite thing to do,
- *or* he or she goes hungry.

It would be impolite to put the person to your left in the position where he or she either had to be impolite or go hungry. Hence $P(n+1)$ is true.

Administration

- Please pass your answers to Sheet 3 to the person in your left. The person at the end of each row should put all work in the box and pass it down to the next row.
- Maths Soc talk by Laurence O'Toole, Cipher Systems. In Arts Building 021 at 6pm.
- **Please** collect unclaimed work at the end from the files at the front. These files are kept in the box outside my office (McCrea 240).

§4 Division and prime factorization

Theorem 4.1

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 q in Theorem 4.1 is called the *quotient* and the r the *remainder* when n is divided by m.

Example 4.2

(i) Let $n = 60$ and $m = 7$. Then $60/7 = 8\frac{4}{7}$ and correspondingly, $60 = 8 \times 7 + 4$. So we have $q = 8$ and $r = 4$.

(ii) Let $n = 63$ and $m = 7$. Then $63/7 = 9$ so we have $q = 9$ and $r = 0$.

(iii) Let $n = 44$ and $m = 6$. Then $44/6 = 7\frac{2}{6}$ so we have $q = 7$ and $r = 2$. (Note that it is more useful to leave the fractional part as $\frac{2}{6}$ than to simplify it to $\frac{1}{3}$.)

Exercise on division

Exercise 4.3

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) $n = -10$, $m = 7$.

It is useful to have some special notation to indicate the case where the remainder is 0 and n/m is an integer.

Definition 4.4

Let $n \in \mathbb{Z}$ and let $m \in \mathbb{N}$. We say that m *divides* n and write $m \mid n$ if $n/m \in \mathbb{Z}$.

Another way to say 'm divides n' is 'n is a multiple of m'.

Greatest common divisors

Definition 4.5

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 dividing both m and n.

Exercise 4.6

Find $\gcd(m, n)$ in each of these cases:

(i) $n = 310$, $m = 42$;

(ii) $n = 10$, $m = 21$;

(iii) $n = 23$, $m = 46$;

(iv) $n = 20475$, $m = 14025$.

Administration

- Spare copies of Sheet 4 and pages 15 to 18 of Part B handout at front.
- Answers to Sheet 3 are now on Moodle.
- Please see or email the lecturer if you need any hints for Sheet 4. Hints will be put up on an webpage or blog linked to from Moodle.
- **Please** collect unclaimed work at the end from the files at the front. These files are kept in the box outside my office (McCrea 240).

Revision Quiz on Sigma notation

(a) Let $t_m = 1 + 2 + 4 + 8 + \cdots + 2^m$. Then $t_3 =$

(A) 14 (B) 15 (C) 7 (D) 37

and in Sigma notation $t_m =$

(A) $\sum_{k=0}^{m} 2^m$ (B) $\sum_{k=0}^{m-1} 2^m$ (C) 2^m (D) $\sum_{k=1}^{m} 2^m$

(b) $\sum_{k=0}^{2} k^2 2^{k-1} =$

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

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

(A) 1 (B) n^2 (C) 42 (D) something else

Euclid's Algorithm

There is a very fast algorithm for finding greatest common divisors that is usually attributed to Euclid. The following lemma gives the key idea.

Lemma 4.7

Let $m, n \in \mathbb{N}$. *Let* $n = qm + r$ *where* $0 \leq r < m$. *Then*

$$\gcd(n, m) = \gcd(m, r).$$

Algorithm 4.8 (Euclid's Algorithm)

Let $m, n \in N$. *To find* $\gcd(n, m)$ *first 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* $\gcd(n, m) = \gcd(m, r)$. *Repeat the algorithm with* m *and* r.

Example of Euclid's Algorithm

Example 4.9

Let $n = 4452$ and let $m = 3402$. The equations below show the quotient and remainder at each step of Euclid's Algorithm:

$$\begin{aligned} 4452 &= 1 \times 3402 + 1050 \\ 3402 &= 3 \times 1050 + 252 \\ 1050 &= 4 \times 252 + 42 \\ 252 &= 5 \times 42. \end{aligned}$$

Hence $\gcd(4452, 3402) = 42$.

By working backwards through the steps in Euclid's Algorithm it is possible to find $s, t \in \mathbb{Z}$ such that $sm + tn = \gcd(m, n)$.

Linear Combinations

Example 4.10

By the penultimate line of Example 4.9 we have $42 = 1050 - 4 \times 252$. By finding the rows in which 1050 and 252 appear as remainders we get

$$\begin{aligned} 42 &= 1050 - 4 \times 252 \\ &= 1050 - 4 \times (3402 - 3 \times 1050) \\ &= 13 \times 1050 - 4 \times 3402 \\ &= 13 \times (4452 - 3402) - 4 \times 3402 \\ &= 13 \times 4452 - 17 \times 3402. \end{aligned}$$

Problem Sheet 3

- If your surname starts with A to M your work is in a green folder. Otherwise it is in a blue folder. Please claim any older homework from the pink folder.
- Questions 2 and 4 were marked. The total marks were 12, with 2 marks on Question 2 awarded for good mathematical style. A separate 0 or 1 mark (which becomes 1.25% of your final mark) was given for a reasonable attempt.
- The answers on Moodle have been updated with some common errors.
- Please see the lecturer in an office hour to go through any of the questions.
- Problem Sheet 4 is due in this Thursday. See Moodle link for hints.
- There are some examples and revision questions on complex numbers available from Moodle.

Factorization into Primes

Definition 4.11

A natural number $p > 1$ is said to be *prime* if the only natural numbers that divide it are 1 and p. A natural number $n > 1$ is said to be *composite* if it is not prime.

Theorem 4.12 (Fundamental Theorem of Arithmetic)

Let $n > 1$ be a natural number. There exists $k \in \mathbb{N}$ and primes $p_1, p_2, \ldots, p_k$ such that

$$n = p_1 p_2 \ldots p_k.$$

This expression of n as a product of primes is unique up to the order of the factors.

Example of Prime Factorization

Example 4.13

(i) Since 43 is prime, its unique factorization is $43 = 43$, with $k = 1$ and $p_1 = 43$.

(ii) Up to the order of the factors, the unique prime factorization of 572 is $2^2 \times 11 \times 13$. So $k = 4$ and we can take $p_1 = 2$, $p_2 = 2$, $p_3 = 11$, $p_4 = 13$.

(iii) The prime factorization of 7680 is ....

Example of Prime Factorization

Example 4.13

(i) Since 43 is prime, its unique factorization is $43 = 43$, with $k = 1$ and $p_1 = 43$.

(ii) Up to the order of the factors, the unique prime factorization of 572 is $2^2 \times 11 \times 13$. So $k = 4$ and we can take $p_1 = 2$, $p_2 = 2$, $p_3 = 11$, $p_4 = 13$.

(iii) The prime factorization of 7680 is ....

Quiz: Find the prime factorizations of the following numbers:

(a) 270 (b) 101 (c) 1001 (d) 123123.

Example of Prime Factorization

Example 4.13

(i) Since 43 is prime, its unique factorization is $43 = 43$, with $k = 1$ and $p_1 = 43$.

(ii) Up to the order of the factors, the unique prime factorization of 572 is $2^2 \times 11 \times 13$. So $k = 4$ and we can take $p_1 = 2$, $p_2 = 2$, $p_3 = 11$, $p_4 = 13$.

(iii) The prime factorization of 7680 is ....

Quiz: Find the prime factorizations of the following numbers:

(a) 270 (b) 101 (c) 1001 (d) 123123.

Claim 4.14

$\sqrt{3}$ is an irrational number.

Proof of the Existence of Prime Factorization

Strong Induction

In the inductive steps in the inductive proofs seen so far, we assumed $P(n)$ and used it to prove $P(n+1)$. To prove the existence of prime factorization, it will be useful to assume *all* the earlier cases, replacing (ii) in the Principle of Mathematical Induction with

(ii)$'$ for each $n \in \mathbb{N}$, if $P(1), \ldots, P(n-1), P(n)$ are true then $P(n+1)$ is true.

Proof of the Existence of Prime Factorization

Strong Induction

In the inductive steps in the inductive proofs seen so far, we assumed $P(n)$ and used it to prove $P(n+1)$. To prove the existence of prime factorization, it will be useful to assume *all* the earlier cases, replacing (ii) in the Principle of Mathematical Induction with

(ii)′ for each $n \in \mathbb{N}$, if $P(1), \ldots, P(n-1), P(n)$ are true then $P(n+1)$ is true.

Theorem 4.12 (Fundamental Theorem of Arithmetic)

Let $n > 1$ be a natural number. There exists $k \in \mathbb{N}$ and primes $p_1, p_2, \ldots, p_k$ such that

$$n = p_1 p_2 \ldots p_k.$$

This expression of n as a product of primes is unique up to the order of the factors.

Infinitely Many Primes

Theorem 4.15 (Euclid)

There are infinitely many primes.

Exercise 4.16

Let $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$, $p_6 = 13$ be the first six prime numbers. 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

$$\begin{aligned} p_1 p_2 p_3 p_4 p_5 p_6 + 1 &= 2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 \\ &= 300031 \\ &= 59 \times 509. \end{aligned}$$

This example shows that the second case in the proof of Euclid's theorem can arise!

Exercise on Claim 4.14

The line 'Let $n = 3^b \times N$ and let $m = 3^a \times M$' has caused some confusion. The purpose of this line is to define b, a, N and M.

So 3^a is the highest power of 3 dividing n and 3^b is the highest power of 3 dividing m, and $N = n/3^b$, $M = m/3^a$.

Exercise 4.17

A manufacturer of cheap pocket calculators claims to you that $\sqrt{3} = \frac{2148105}{1240209}$. Put $m = 2148105$ and $n = 1240209$ in the proof of Claim 4.14 and find b, a, N and M. (You can do this by repeated division by 3, even on one of his cheapest calculators.) Hence show the manufacturer that he is wrong.

Bases

Example 4.18

To write 144 in base 3:

Divide 144 by 3:	$144 = 48 \times 3 + 0$
Divide the quotient 48 by 3:	$48 = 16 \times 3 + 0$
Divide the quotient 16 by 3:	$16 = 5 \times 3 + 1$
Divide the quotient 5 by 3:	$5 = 1 \times 3 + 2$
Divide the quotient 1 by 3:	$1 = 0 \times 3 + 1$

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

$$144 = 1 \times 3^4 + 2 \times 3^3 + 1 \times 3^2 + 0 \times 3^1 + 0 \times 3^0.$$

Hence 144 is 12100 in base 3. We write this as $144 = 12100_3$.

Algorithm for Writing Numbers in Base b

Algorithm 4.19

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

The correctness of this algorithm can be proved by strong induction. This is left as an optional exercise.

Example of Algorithm 4.19

Example 4.20

To write 37 in base 2, following the algorithm:

Divide 37 by 2:	$37 = 18 \times 2 + 1$
Divide the quotient 18 by 2:	$18 = 9 \times 2 + 0$
Divide the quotient 9 by 2:	$9 = 4 \times 2 + 1$
Divide the quotient 4 by 2:	$4 = 2 \times 2 + 0$
Divide the quotient 2 by 2:	$2 = 1 \times 2 + 0$
Divide the quotient 1 by 2:	$2 = 0 \times 2 + 1$

The sequence of remainders is $1, 0, 1, 0, 0, 1$, so

$$r_0 = 1, r_1 = 0, r_2 = 1, r_3 = 0, r_4 = 0, r_5 = 1.$$

Hence $37 = (r_5 r_4 r_3 r_2 r_1 r_0)_2 = 100101_2$.

Exercise 4.21

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

Liar Game

Exercise 4.22

Form pairs. Person A should think of a number between 1 and 16 and write it down on a hidden piece of paper. Person B should now ask ask questions about the unknown number until it is discovered. Record how many questions you need.

Now repeat, with the change that person A is allowed to lie in at most one answer.

Administration

- If your surname begins with
  - A–F your work is in the red folder
  - H–M your work is in the blue folder
  - N–S your work is in the green folder
  - T–Z your work is in the yellow folder
- **Please** remember to put your name and student number on your work. Two people need to email me their name. If you have an unexpected gap in your submission record I may have asked you to confirm that no work has gone missing.
- **Remember a reasonable attempt at each of the 8 assessed sheets is worth 1.25% of your final mark.**
- The model answers on Moodle have been updated with some comments and common errors.
- See Moodle (week 3) for answers to the questions on the revision sheet on complex numbers.

Quiz: True or False?

- 3 divides 9
- 9 divides 3
- 3 is a multiple of 15
- 15 is a multiple of 3
- $3 \mid 21$
- $21 \mid 3$

Part C: Propositions, sets and relations

§5 Propositional Logic

Suppose that A and B are mathematical statements. **such** that if A is true then B is true. Then we say that A *implies* B, and write $A \implies B$.

So A and B could either be propositions, e.g. 'the morning is the best time of day', '$2 + 2 = 4$', or predicates e.g. '$2n + 1$ is odd', 'n is even'.

It is occasionally useful to write $A \implies B$ as $B \impliedby A$. This can be read as 'B is implied by A'.

If A implies B *and* B implies A then we write $A \iff B$. For the moment, please read this as 'A implies and is implied by B'.

Exercise

Exercise 5.1

Which of the following are correct:

(a) 3 divides 87 $\implies$ $87/3 \in \mathbb{Z}$;

(b) 5 divides 11 $\implies$ $11/5 \in \mathbb{Z}$;

(c) $x \geq 4 \implies x \geq 3$;

(d) $x \geq 3 \implies x \geq 4$;

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

(f) $x \geq 0$ and $x^2 - 2x - 3 = 0 \implies x = 3$.

(g) If x and y are real numbers then $x^2 = y^2 \implies x = y$.

(h) If r and s are distances in the plane then $r^2 = s^2 \implies r = s$.

(i) If x and y are real numbers then $x^3 = y^3 \implies x = y$;

(j) If z and w are complex numbers then $w^3 = z^3 \implies w = z$?

Administration

- Answers to Problem Sheet 5 will go up on Moodle shortly.
- Please make sure you get a copy of Problem Sheet 6. This will be marked as normal and **is worth** 1.25% **of your final mark for this course**. I will put up hints on my blog (see Moodle link).
- Does anyone know what happened to the work in red/blue/green/yellow files from Monday?

Double implication

Let A and B be mathematical statements. If A implies B *and* B implies A then we write $A \iff B$. For the moment, please read this as 'A implies and is implied by B'.

Quiz:

- Which of (a), (b), (c) and (d) are correct?
- In which can $\implies$ be replaced with $\iff$?

(a) $x^2 = 4 \implies x \in \{-2, 2\}$

(b) $x^2 = 4 \implies x \in \{-2, 2, 5\}$

(c) $x \in \{-2, 2\} \implies x \in \{-2, 2, 5\}$

(d) $x \geq 0$ and $x^2 = 4 \implies x = 2$

Double implication

Exercise 5.2

Define a predicate $P(n)$ *by*

$$P(n) : 2^n \geq 6n$$

If $n = 5$ *then* $P(5)$ *states that* $2^5 \geq 6 \times 5$*; this is true because* $32 \geq 30$*. Assume, by induction, that* $P(n)$ *is true. Then*

$$\begin{aligned} 2^{n+1} &\geq 6(n+1) \\ 2^{n+1} - 6(n+1) &\geq 0 \\ 2 \times 2^n - 6n - 6 &\geq 0 \\ 2(2^n - 6n) + 6n - 6 &\geq 0 \end{aligned}$$

which is true since $2^n \geq 6n$ *and* $6n \geq 6$*.*

Is this argument valid? How could it be clarified?

Double implication

Exercise 5.2

Define a predicate $P(n)$ *by*

$$P(n) : 2^n \geq 6n$$

If $n = 5$ *then* $P(5)$ *states that* $2^5 \geq 6 \times 5$*; this is true because* $32 \geq 30$*. Assume, by induction, that* $P(n)$ *is true. Then*

$$\begin{aligned} & 2^{n+1} \geq 6(n+1) \\ \iff & 2^{n+1} - 6(n+1) \geq 0 \\ \iff & 2 \times 2^n - 6n - 6 \geq 0 \\ \iff & 2(2^n - 6n) + 6n - 6 \geq 0 \end{aligned}$$

which is true since $2^n \geq 6n$ *and* $6n \geq 6$*.*

Is this argument valid? How could it be clarified?

Another Example on Double Implication

Example 5.3

Suppose we want to find all $x \in \mathbb{R}$ such that

$$\sqrt{x+3} = x+1.$$

The following chain of implications is correct:

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

But we cannot conclude that $x = -2$ and $x = 1$ are solutions. Putting $x = -2$ into $\sqrt{x+3} = x+1$ gives $\sqrt{-2+3} = -2+1$, which is false!

Logical Structure

Your arguments will be clearer if you use $\Longrightarrow$ and $\Longleftrightarrow$ to show their logical structure. Try to avoid lists of assertions whose relationship to one another is unclear.

Correct use of implication signs is helpful even in very simple arguments. For example, to find the prime factorization of 210 you could write:

$$\begin{aligned} 210/2 = 105 &\Longrightarrow 210 = 105 \times 2 \\ 105/5 = 21 &\Longrightarrow 105 = 5 \times 21 \\ 21/3 = 7 &\Longrightarrow 21 = 3 \times 7 \end{aligned}$$

hence $210 = 2 \times 105 = 2 \times 5 \times 21 = 2 \times 3 \times 5 \times 7$.

If, only if, necessary, sufficient

As before, let A and B be mathematical statements. The following are all different ways to write '$A \implies B$':

- if A then B;
- B if A;
- A only if B.
- A is sufficient for B;
- B is necessary for A.

The first often feels the most natural and is frequently used. (See, for instance, the statement of Claim 3.7.)

Administration

- Answers to Problem Sheet 5 are now on Moodle. This was a revision sheet and so will not be marked.
  - You are very welcome to ask me about it in office hours.
  - A few people handed work in to the maths office: please retrieve your work at the end.
- There will be four more problem sheets. Each will be marked as normal and **is worth** 1.25% **of your final mark for this course**. I will put up hints on my blog (see Moodle link). Problem Sheet 6 is due in next Thursday.
- Please aim to be in place by 9.04.59 am.

Exercise 5.4: 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?
Write down a letter $\iff$ it can be deduced.

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.

Exercise 5.4: 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?
Write down a letter $\Longleftrightarrow$ it can be deduced.

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.

Exercise 5.4: Assume P, Q, R.

P: If it is raining then the sky is cloudy.

$$\text{RAIN} \Longrightarrow \text{CLOUDY}$$

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?

A: A cloudy sky is a necessary condition for rain. $\text{RAIN} \Longrightarrow \text{CLOUDY}$

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.

Exercise 5.4: Assume P, Q, R.

P: If it is raining then the sky is cloudy.

$$\text{RAIN} \implies \text{CLOUDY}$$

Q: If it rains in the morning then Prof. X carries his umbrella all day.

$$\text{MORNING RAIN} \implies \text{UMBRELLA}$$

R: People who carry umbrellas never get soaked.

$$\text{UMBRELLA} \implies \text{NOT SOAKED}$$

Which of the following statements can be deduced from P, Q and R?

A: A cloudy sky is a necessary condition for rain. $\text{RAIN} \implies \text{CLOUDY}$

B: A cloudy sky is a sufficient condition for rain. $\text{CLOUDY} \not\implies \text{RAIN}$

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.

Exercise 5.4: Assume P, Q, R.

P: If it is raining then the sky is cloudy.

$$\text{RAIN} \implies \text{CLOUDY}$$

Q: If it rains in the morning then Prof. X carries his umbrella all day.

$$\text{MORNING RAIN} \implies \text{UMBRELLA}$$

R: People who carry umbrellas never get soaked.

$$\text{UMBRELLA} \implies \text{NOT SOAKED}$$

Which of the following statements can be deduced from P, Q and R?

A: A cloudy sky is a necessary condition for rain. $\text{RAIN} \implies \text{CLOUDY}$

B: A cloudy sky is a sufficient condition for rain. $\text{CLOUDY} \not\implies \text{RAIN}$

C: It is raining only if the sky is cloudy. $\text{RAIN} \implies \text{CLOUDY}$

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.

Exercise 5.4: Assume P, Q, R.

P: If it is raining then the sky is cloudy.
$$\text{RAIN} \implies \text{CLOUDY}$$

Q: If it rains in the morning then Prof. X carries his umbrella all day.
$$\text{MORNING RAIN} \implies \text{UMBRELLA}$$

R: People who carry umbrellas never get soaked.
$$\text{UMBRELLA} \implies \text{NOT SOAKED}$$

Which of the following statements can be deduced from P, Q and R?

A: A cloudy sky is a necessary condition for rain. $\text{RAIN} \implies \text{CLOUDY}$

B: A cloudy sky is a sufficient condition for rain. $\text{CLOUDY} \not\Longrightarrow \text{RAIN}$

C: It is raining only if the sky is cloudy. $\text{RAIN} \implies \text{CLOUDY}$

D: Rain in the morning is a necessary condition for Prof. X to carry his umbrella. $\text{UMBRELLA} \not\Longrightarrow \text{MORNING RAIN}$

E: Rain in the morning is a sufficient condition for Prof. X to carry his umbrella.

Exercise 5.4: Assume P, Q, R.

P: If it is raining then the sky is cloudy.
$$\text{RAIN} \implies \text{CLOUDY}$$

Q: If it rains in the morning then Prof. X carries his umbrella all day.
$$\text{MORNING RAIN} \implies \text{UMBRELLA}$$

R: People who carry umbrellas never get soaked.
$$\text{UMBRELLA} \implies \text{NOT SOAKED}$$

Which of the following statements can be deduced from P, Q and R?

A: A cloudy sky is a necessary condition for rain. $\text{RAIN} \implies \text{CLOUDY}$

B: A cloudy sky is a sufficient condition for rain. $\text{CLOUDY} \not\Longrightarrow \text{RAIN}$

C: It is raining only if the sky is cloudy. $\text{RAIN} \implies \text{CLOUDY}$

D: Rain in the morning is a necessary condition for Prof. X to carry his umbrella. $\text{UMBRELLA} \not\Longrightarrow \text{MORNING RAIN}$

E: Rain in the morning is a sufficient condition for Prof. X to carry his umbrella. $\text{MORNING RAIN} \implies \text{UMBRELLA}$

Exercise 5.4: 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?

F: Rain falling implies that the sky is cloudy. $\text{RAIN} \Longrightarrow \text{CLOUDY}$

G: The sky is cloudy implies that rain is falling.

H: If Prof. X is soaked then it did not rain this morning.

Exercise 5.4: 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?

F: Rain falling implies that the sky is cloudy. $\text{RAIN} \Longrightarrow \text{CLOUDY}$

G: The sky is cloudy implies that rain is falling. $\text{CLOUDY} \not\Longrightarrow \text{RAIN}$

H: If Prof. X is soaked then it did not rain this morning.

Exercise 5.4: Assume P, Q, R.

P: If it is raining then the sky is cloudy.

$$\text{RAIN} \implies \text{CLOUD}$$

Q: If it rains in the morning then Prof. X carries his umbrella all day.

$$\text{MORNING RAIN} \implies \text{UMBRELLA}$$

R: People who carry umbrellas never get soaked.

$$\text{UMBRELLA} \implies \text{NOT SOAKED}$$

Which of the following statements can be deduced from P, Q and R?

F: Rain falling implies that the sky is cloudy. $\text{RAIN} \implies \text{CLOUDY}$

G: The sky is cloudy implies that rain is falling. $\text{CLOUDY} \not\Longrightarrow \text{RAIN}$

H: If Prof. X is soaked then it did not rain this morning.

$$\text{SOAKED} \implies \text{NOT MORNING RAIN}$$

‘If and only if’ and logical equivalence

If $A \iff B$ holds we say that A and B are *logically equivalent*. We can rewrite

$B \implies A$ as ‘A if B’.

$A \implies B$ as ‘A only if B’.

This justifies reading $A \iff B$ as ‘A if and only if B’. Note that the ‘A if B’ part of this expression refers to the implication $B \implies A$.

Negation and the Contrapositive

If A is a mathematical statement we write $\neg A$ for the statement 'not A'. The *contrapositive* of an implication $A \implies B$ is $\neg B \implies \neg A$.

Exercise 5.5

Convince yourself that $A \implies B$ is true if and only if the contrapositive $\neg B \implies \neg A$ is true. In symbols

$$(A \implies B) \iff (\neg B \implies \neg A).$$

Switching to the contrapositive can be a useful first step in a proof, particularly when statements appear in negated form.

Claim 5.6

Let $x \in \mathbb{Q}$. If $y \notin \mathbb{Q}$ then $x + y \notin \mathbb{Q}$.

Quiz

(A) 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) E (b) D (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'?

Quiz

(A) 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) E (b) D (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'?

(B) Alcohol. In the far-off land of Erewhon, only people over the age of 21 are allowed to drink alcohol in public. If your job is to enforce this law, who of the following would you investigate further?

(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 18 with an unidentifiable drink

‘For all’ and ‘exists’

Let $P(x)$ be a predicate defined for elements 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 parentheses around $\forall x \in X$ and $\exists x \in X$ are often omitted.

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 on negation

Exercise 5.7

Sometimes the set X in $\forall x \in X$ is indicated by inequalities. For example,

$(\forall \epsilon > 0)\, Q(\epsilon)$ 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

$$(\exists \ell \in \mathbb{R})(\forall \epsilon > 0)(\exists N \in \mathbb{N})(\forall n \geq N)\ |a_n - \ell| < \epsilon.$$

Administration

- Answers to Problem Sheet 5 are now on Moodle. This was a revision sheet and so will not be marked.
  - You are very welcome to ask me about it in office hours.
  - A few people handed work in to the maths office: please retrieve your work at the end.
- There will be four more problem sheets. Each will be marked as normal and **is worth** 1.25% **of your final mark for this course**. I will put up hints on my blog (see Moodle link). Problem Sheet 6 is due in next Thursday.
- Please aim to be in place by 9.04.59 am. Of course the worst offenders won't be reading this.
- Please take pages 27 and 28 of the printed notes. Spare copies of Sheet 6 and last installment at front.

Conjunction and disjunction

Let A and B be mathematical statements.

- The *conjunction* of A and B, written $A \wedge B$ and read 'A and B', is true if A and B are both true, and false otherwise.
- The *disjunction* of A and B, written $A \vee B$ and read 'A or B' is true if one or both of A and B is true, and false otherwise.

Truth tables

Consider the disjunction $A \vee B$. This is true if one of A and B is true, and false otherwise. The *truth table* below shows this by going through all possibilities for A and B.

A	B	$A \vee B$
T	T	T
T	F	T
F	T	T
F	F	F

Administration

- Please pass your answers to Sheet 3 to the person in your left. The person at the end of each row should put all work in the box and pass it down to the next row.
- Please take pages 29 and 30 of the printed notes.
- Library: some more copies of Liebeck, *A concise introduction to pure mathematics*, Chapman & Hall (2011) should arrive soon. If you can't get hold of this or *How to think like a mathematician*, you can borrow my copy and photocopy the bits you need.

Truth table for implication

Exercise 5.8

Fill in the $\Longrightarrow$ column of the following truth table.

A	B	$A \Longrightarrow B$	$\neg B$	$\neg A$	$\neg B \Longrightarrow \neg A$
T	T				
T	F				
F	T				
F	F				

Truth table for implication

Exercise 5.8

Fill in the $\Longrightarrow$ column of the following truth table.

A	B	$A \Longrightarrow B$	$\neg B$	$\neg A$	$\neg B \Longrightarrow \neg A$
T	T				
T	F				
F	T				
F	F				

Now fill in the remaining columns. Are they consistent with the logical equivalence of $A \Longrightarrow B$ and $\neg B \Longrightarrow \neg A$?

Remember: $A \Longrightarrow B$ means that if A is true then B is true. If A is false . . .

Truth table for implication

Exercise 5.8

Fill in the $\Longrightarrow$ column of the following truth table.

A	B	$A \Longrightarrow B$	$\neg B$	$\neg A$	$\neg B \Longrightarrow \neg A$
T	T				
T	F				
F	T				
F	F				

Now fill in the remaining columns. Are they consistent with the logical equivalence of $A \Longrightarrow B$ and $\neg B \Longrightarrow \neg A$?

Remember: $A \Longrightarrow B$ means that if A is true then B is true. If A is false . . . then B is allowed to be anything . . .

Truth table for implication

Exercise 5.8

Fill in the $\Longrightarrow$ column of the following truth table.

A	B	$A \Longrightarrow B$	$\neg B$	$\neg A$	$\neg B \Longrightarrow \neg A$
T	T				
T	F				
F	T				
F	F				

Now fill in the remaining columns. Are they consistent with the logical equivalence of $A \Longrightarrow B$ and $\neg B \Longrightarrow \neg A$?

Remember: $A \Longrightarrow B$ means that if A is true then B is true. If A is false . . . then B is allowed to be anything . . . so $A \Longrightarrow B$ is true.

Exercise 5.9

By definition, $A \iff B$ is true if and only if $A \implies B$ and $B \implies A$ both hold. So $A \iff B$ is logically equivalent to

$$(A \implies B) \wedge (B \implies A).$$

Use this to find the truth table for $A \iff B$.

Example 5.10

Let A and B be propositions. The *exclusive or* of A and B is true if exactly one of A and B is true.

A	B	A xor B
T	T	F
T	T	T
T	F	T
T	F	F

To express A xor B in terms of the usual logical connectives $\wedge$ and $\vee$, we write down a proposition that says 'A and B have the truth values of one of the rows for which A xor B is true'. There are two such rows in the truth table, so we want to say

'(A is true and B is false) or (A is false and B is true)'.

In symbols this is

$$\big(A \wedge (\neg B)\big) \vee \big((\neg A) \wedge B\big).$$

§6 More about Sets

Let X be a set. If $P(x)$ is a predicate defined for elements of X then we denote by

$$\{x \in X : P(x)\}$$

the set of all elements of X for which $P(x)$ is true.

Example 6.1

(a) $\{m \in \mathbb{Z} : 2 \mid m\}$ is the set of even integers.

(b) $\{x \in \mathbb{R} : x > 0\}$ is the set of positive real numbers.

(c) $\{z \in \mathbb{C} : z^5 = 1\}$ is the set of fifth roots of 1 in $\mathbb{C}$.

Definition 6.2

(i) A set X is said to be a *subset* of a set Y if $x \in X$ implies $x \in Y$. If X is a subset of Y we write $X \subseteq Y$.

(ii) The set with no elements is called the *empty set* and is denoted $\varnothing$.

(ii) A set is said to be *finite* if it has finitely many elements. The *size* of a finite set is its number of elements. We denote the size of a set X by $|X|$, read 'mod X'.

Exercise 6.3 (True or False?)

(a) the empty set is a subset of every set;

(b) the empty set is an element of every set;

(c) $\{0, 1\}$ is a subset of $\{\{0, 1\}, 1, 3\}$;

(d) $\{0, 1\}$ is an element of $\{\{0, 1\}, 1, 3\}$;

(e) the size of $\varnothing$ is 0;

(f) $|\{\{0, 1\}, 1, 3\}| = 4$;

(g) $|\{z \in \mathbb{C} : z^3 = 1\}| = 3$.

Exercise 6.3 (True or False?)

(a) the empty set is a subset of every set;

(b) the empty set is an element of every set;

(c) $\{0, 1\}$ is a subset of $\{\{0, 1\}, 1, 3\}$;

(d) $\{0, 1\}$ is an element of $\{\{0, 1\}, 1, 3\}$;

(e) the size of $\varnothing$ is 0;

(f) $|\{\{0, 1\}, 1, 3\}| = 4$;

(g) $|\{z \in \mathbb{C} : z^3 = 1\}| = 3$.

Exercise 6.3 (True or False?)

(a) the empty set is a subset of every set; TRUE

For any set Y, $x \in \varnothing \implies x \in Y$ (nothing to check!)

(b) the empty set is an element of every set;

(c) $\{0, 1\}$ is a subset of $\{\{0, 1\}, 1, 3\}$;

(d) $\{0, 1\}$ is an element of $\{\{0, 1\}, 1, 3\}$;

(e) the size of $\varnothing$ is 0;

(f) $|\{\{0, 1\}, 1, 3\}| = 4$;

(g) $|\{z \in \mathbb{C} : z^3 = 1\}| = 3$.

Exercise 6.3 (True or False?)

(a) the empty set is a subset of every set; TRUE

For any set Y, $x \in \varnothing \implies x \in Y$ (nothing to check!)

(b) the empty set is an element of every set; FALSE

For example, $\varnothing \notin \{1\}$, or $\varnothing \notin \mathbb{R}$, or ...

(c) $\{0, 1\}$ is a subset of $\{\{0, 1\}, 1, 3\}$;

(d) $\{0, 1\}$ is an element of $\{\{0, 1\}, 1, 3\}$;

(e) the size of $\varnothing$ is 0;

(f) $|\{\{0, 1\}, 1, 3\}| = 4$;

(g) $|\{z \in \mathbb{C} : z^3 = 1\}| = 3$.

Exercise 6.3 (True or False?)

(a) the empty set is a subset of every set; TRUE

For any set Y, $x \in \varnothing \implies x \in Y$ (nothing to check!)

(b) the empty set is an element of every set; FALSE

For example, $\varnothing \notin \{1\}$, or $\varnothing \notin \mathbb{R}$, or ...

(c) $\{0, 1\}$ is a subset of $\{\{0, 1\}, 1, 3\}$; FALSE

(d) $\{0, 1\}$ is an element of $\{\{0, 1\}, 1, 3\}$;

(e) the size of $\varnothing$ is 0;

(f) $|\{\{0, 1\}, 1, 3\}| = 4$;

(g) $|\{z \in \mathbb{C} : z^3 = 1\}| = 3$.

Exercise 6.3 (True or False?)

(a) the empty set is a subset of every set; TRUE

For any set Y, $x \in \varnothing \implies x \in Y$ (nothing to check!)

(b) the empty set is an element of every set; FALSE

For example, $\varnothing \notin \{1\}$, or $\varnothing \notin \mathbb{R}$, or ...

(c) $\{0,1\}$ is a subset of $\{\{0,1\},1,3\}$; FALSE

This is false because $0 \in \{0,1\}$ but $0 \notin \{\{0,1\},1,3\}$.

(d) $\{0,1\}$ is an element of $\{\{0,1\},1,3\}$;

(e) the size of $\varnothing$ is 0;

(f) $|\{\{0,1\},1,3\}| = 4$;

(g) $|\{z \in \mathbb{C} : z^3 = 1\}| = 3$.

Exercise 6.3 (True or False?)

(a) the empty set is a subset of every set; TRUE

For any set Y, $x \in \varnothing \implies x \in Y$ (nothing to check!)

(b) the empty set is an element of every set; FALSE

For example, $\varnothing \notin \{1\}$, or $\varnothing \notin \mathbb{R}$, or ...

(c) $\{0,1\}$ is a subset of $\{\{0,1\},1,3\}$; FALSE

This is false because $0 \in \{0,1\}$ but $0 \notin \{\{0,1\},1,3\}$.

(d) $\{0,1\}$ is an element of $\{\{0,1\},1,3\}$; TRUE

(e) the size of $\varnothing$ is 0;

(f) $|\{\{0,1\},1,3\}| = 4$;

(g) $|\{z \in \mathbb{C} : z^3 = 1\}| = 3$.

Exercise 6.3 (True or False?)

(a) the empty set is a subset of every set; TRUE

For any set Y, $x \in \varnothing \implies x \in Y$ (nothing to check!)

(b) the empty set is an element of every set; FALSE

For example, $\varnothing \notin \{1\}$, or $\varnothing \notin \mathbb{R}$, or ...

(c) $\{0,1\}$ is a subset of $\{\{0,1\},1,3\}$; FALSE

This is false because $0 \in \{0,1\}$ but $0 \notin \{\{0,1\},1,3\}$.

(d) $\{0,1\}$ is an element of $\{\{0,1\},1,3\}$; TRUE

(e) the size of $\varnothing$ is 0; TRUE

(f) $|\{\{0,1\},1,3\}| = 4$;

(g) $|\{z \in \mathbb{C} : z^3 = 1\}| = 3$.

Exercise 6.3 (True or False?)

(a) the empty set is a subset of every set; TRUE

For any set Y, $x \in \varnothing \implies x \in Y$ (nothing to check!)

(b) the empty set is an element of every set; FALSE

For example, $\varnothing \notin \{1\}$, or $\varnothing \notin \mathbb{R}$, or ...

(c) $\{0,1\}$ is a subset of $\{\{0,1\},1,3\}$; FALSE

This is false because $0 \in \{0,1\}$ but $0 \notin \{\{0,1\},1,3\}$.

(d) $\{0,1\}$ is an element of $\{\{0,1\},1,3\}$; TRUE

(e) the size of $\varnothing$ is 0; TRUE

(f) $|\{\{0,1\},1,3\}| = 4$; FALSE (size is 3)

(g) $|\{z \in \mathbb{C} : z^3 = 1\}| = 3$.

Exercise 6.3 (True or False?)

(a) the empty set is a subset of every set; TRUE

For any set Y, $x \in \varnothing \implies x \in Y$ (nothing to check!)

(b) the empty set is an element of every set; FALSE

For example, $\varnothing \notin \{1\}$, or $\varnothing \notin \mathbb{R}$, or ...

(c) $\{0,1\}$ is a subset of $\{\{0,1\},1,3\}$; FALSE

This is false because $0 \in \{0,1\}$ but $0 \notin \{\{0,1\},1,3\}$.

(d) $\{0,1\}$ is an element of $\{\{0,1\},1,3\}$; TRUE

(e) the size of $\varnothing$ is 0; TRUE

(f) $|\{\{0,1\},1,3\}| = 4$; FALSE (size is 3)

(g) $|\{z \in \mathbb{C} : z^3 = 1\}| = 3$. TRUE

Subsets

Recall that a set X is said to be a *subset* of a set Y if $x \in X$ implies $x \in Y$.

Example 6.4

Let $m \in \mathbb{N}$. Then

(i) $\{n \in \mathbb{N} : m^2 \mid n\} \subseteq \{n \in \mathbb{N} : m \mid n\}$

(ii) $\{n \in \mathbb{N} : 6 \mid n\} = \{n \in \mathbb{N} : 2 \mid n \text{ and } 3 \mid n\}$.

Intersection, Union and Complement

Let X and Y be sets.

- We define the *intersection* $X \cap Y$ to be the set of elements that are in both X and Y.
- We define the *union* $X \cup Y$ to be the set of elements that are in at least one of X and Y.

If X is a subset of a 'universe set' U then we define the *complement of U with respect to U* by

$$X' = \{z \in U : z \notin X\}.$$

Claim 6.5 (De Morgan's Laws)

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

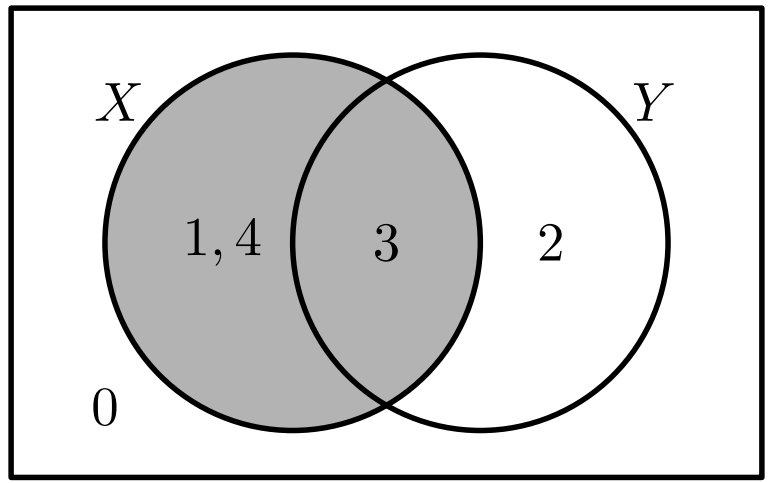
(i) $(X \cup Y)' = X' \cap Y'$,

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

Venn Diagrams

Example 6.6

Let $U = \{0, 1, 2, 3, 4\}$. Define subsets X and Y of U by $X = \{1, 3, 4\}$ and $Y = \{2, 3\}$. We can represent U, X and Y pictorially by a *Venn diagram*, as shown below.



In this diagram U is represented by the rectangular region. The region representing X is shaded.

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

$$|X \cup Y| = |X| + |Y| - |X \cap Y|.$$

Exercise 6.7

Show that if X, Y and Z are finite sets then

$$|X \cup Y \cup Z| = |X| + |Y| + |Z| - |X \cap Y| - |Y \cap Z| - |Z \cap X| + |X \cap Y \cap Z|.$$

Administration

- If your surname begins with
  - A–G your work is in the red folder
  - H–M your work is in the blue folder
  - N–S your work is in the green folder
  - T–Z your work is in the yellow folder
- **Please** remember to put your full name and/or student number on your work.
- **Remember a reasonable attempt at each of the 8 assessed sheets is worth 1.25% of your final mark.**
- The model answers on Moodle for Sheet 6 have been updated with some comments and common errors.
- There is a hint for Question 6 on Sheet 7 on the blog (see link at top of Moodle page). Email or see the lecturer if you want any more hints.

Cartesian Products

If X and Y are sets then we denote by $X \times Y$ the set of all *ordered pairs* (x, y) with $x \in X$ and $y \in Y$. It is usual to write X^2 for $X \times X$. Thus the plane is the set $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$.

Quiz: Decide whether the following are True or False. Let

$$X = \{x \in \mathbb{R} : 1 \leq x \leq 3\}$$
$$Y = \{y \in \mathbb{R} : 1 \leq y \leq 2\}.$$

(a) $(1, 2) = (2, 1)$;

(b) $\{1, 2\} = \{2, 1\}$.

(c) $(\frac{5}{2}, \frac{3}{2}) \in X \times Y$;

(d) $(\frac{3}{2}, \frac{5}{2}) \in X \times Y$;

(e) $Y \times Y \subseteq X \times Y$;

(f) $X \subseteq Y$;

(g) $\varnothing \times X \subseteq \varnothing \times Y$;

(h) Every subset of $\mathbb{R}^2$ is of the form $A \times B$ for suitable subsets $A \subseteq \mathbb{R}$, $B \subseteq \mathbb{R}$.

Cartesian Products

If X and Y are sets then we denote by $X \times Y$ the set of all *ordered pairs* (x, y) with $x \in X$ and $y \in Y$. It is usual to write X^2 for $X \times X$. Thus the plane is the set $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$.

Quiz: Decide whether the following are True or False. Let

$$X = \{x \in \mathbb{R} : 1 \leq x \leq 3\}$$
$$Y = \{y \in \mathbb{R} : 1 \leq y \leq 2\}.$$

(a) $(1, 2) = (2, 1)$;

(b) $\{1, 2\} = \{2, 1\}$.

(c) $(\frac{5}{2}, \frac{3}{2}) \in X \times Y$; TRUE

(d) $(\frac{3}{2}, \frac{5}{2}) \in X \times Y$;

(e) $Y \times Y \subseteq X \times Y$;

(f) $X \subseteq Y$;

(g) $\varnothing \times X \subseteq \varnothing \times Y$;

(h) Every subset of $\mathbb{R}^2$ is of the form $A \times B$ for suitable subsets $A \subseteq \mathbb{R}$, $B \subseteq \mathbb{R}$.

Cartesian Products

If X and Y are sets then we denote by $X \times Y$ the set of all *ordered pairs* (x, y) with $x \in X$ and $y \in Y$. It is usual to write X^2 for $X \times X$. Thus the plane is the set $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$.

Quiz: Decide whether the following are True or False. Let

$$X = \{x \in \mathbb{R} : 1 \leq x \leq 3\}$$
$$Y = \{y \in \mathbb{R} : 1 \leq y \leq 2\}.$$

(a) $(1, 2) = (2, 1)$;

(b) $\{1, 2\} = \{2, 1\}$.

(c) $(\frac{5}{2}, \frac{3}{2}) \in X \times Y$; TRUE

(d) $(\frac{3}{2}, \frac{5}{2}) \in X \times Y$; FALSE

(e) $Y \times Y \subseteq X \times Y$;

(f) $X \subseteq Y$;

(g) $\varnothing \times X \subseteq \varnothing \times Y$;

(h) Every subset of $\mathbb{R}^2$ is of the form $A \times B$ for suitable subsets $A \subseteq \mathbb{R}$, $B \subseteq \mathbb{R}$.

Cartesian Products

If X and Y are sets then we denote by $X \times Y$ the set of all *ordered pairs* (x, y) with $x \in X$ and $y \in Y$. It is usual to write X^2 for $X \times X$. Thus the plane is the set $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$.

Quiz: Decide whether the following are True or False. Let

$$X = \{x \in \mathbb{R} : 1 \leq x \leq 3\}$$
$$Y = \{y \in \mathbb{R} : 1 \leq y \leq 2\}.$$

(a) $(1, 2) = (2, 1)$;

(b) $\{1, 2\} = \{2, 1\}$.

(c) $(\frac{5}{2}, \frac{3}{2}) \in X \times Y$; TRUE

(d) $(\frac{3}{2}, \frac{5}{2}) \in X \times Y$; FALSE

(e) $Y \times Y \subseteq X \times Y$; TRUE

(f) $X \subseteq Y$;

(g) $\varnothing \times X \subseteq \varnothing \times Y$;

(h) Every subset of $\mathbb{R}^2$ is of the form $A \times B$ for suitable subsets $A \subseteq \mathbb{R}$, $B \subseteq \mathbb{R}$.

Cartesian Products

If X and Y are sets then we denote by $X \times Y$ the set of all *ordered pairs* (x, y) with $x \in X$ and $y \in Y$. It is usual to write X^2 for $X \times X$. Thus the plane is the set $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$.

Quiz: Decide whether the following are True or False. Let

$$X = \{x \in \mathbb{R} : 1 \leq x \leq 3\}$$
$$Y = \{y \in \mathbb{R} : 1 \leq y \leq 2\}.$$

(a) $(1, 2) = (2, 1)$;

(b) $\{1, 2\} = \{2, 1\}$.

(c) $(\frac{5}{2}, \frac{3}{2}) \in X \times Y$; TRUE

(d) $(\frac{3}{2}, \frac{5}{2}) \in X \times Y$; FALSE

(e) $Y \times Y \subseteq X \times Y$; TRUE

(f) $X \subseteq Y$; FALSE

(g) $\varnothing \times X \subseteq \varnothing \times Y$;

(h) Every subset of $\mathbb{R}^2$ is of the form $A \times B$ for suitable subsets $A \subseteq \mathbb{R}$, $B \subseteq \mathbb{R}$.

Cartesian Products

If X and Y are sets then we denote by $X \times Y$ the set of all *ordered pairs* (x, y) with $x \in X$ and $y \in Y$. It is usual to write X^2 for $X \times X$. Thus the plane is the set $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$.

Quiz: Decide whether the following are True or False. Let

$$X = \{x \in \mathbb{R} : 1 \leq x \leq 3\}$$
$$Y = \{y \in \mathbb{R} : 1 \leq y \leq 2\}.$$

(a) $(1, 2) = (2, 1)$;

(b) $\{1, 2\} = \{2, 1\}$.

(c) $(\frac{5}{2}, \frac{3}{2}) \in X \times Y$; TRUE

(d) $(\frac{3}{2}, \frac{5}{2}) \in X \times Y$; FALSE

(e) $Y \times Y \subseteq X \times Y$; TRUE

(f) $X \subseteq Y$; FALSE

(g) $\varnothing \times X \subseteq \varnothing \times Y$; TRUE

(h) Every subset of $\mathbb{R}^2$ is of the form $A \times B$ for suitable subsets $A \subseteq \mathbb{R}$, $B \subseteq \mathbb{R}$.

Cartesian Products

If X and Y are sets then we denote by $X \times Y$ the set of all *ordered pairs* (x, y) with $x \in X$ and $y \in Y$. It is usual to write X^2 for $X \times X$. Thus the plane is the set $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$.

Quiz: Decide whether the following are True or False. Let

$$X = \{x \in \mathbb{R} : 1 \leq x \leq 3\}$$
$$Y = \{y \in \mathbb{R} : 1 \leq y \leq 2\}.$$

(a) $(1, 2) = (2, 1)$; FALSE

(b) $\{1, 2\} = \{2, 1\}$.

(c) $(\frac{5}{2}, \frac{3}{2}) \in X \times Y$; TRUE

(d) $(\frac{3}{2}, \frac{5}{2}) \in X \times Y$; FALSE

(e) $Y \times Y \subseteq X \times Y$; TRUE

(f) $X \subseteq Y$; FALSE

(g) $\varnothing \times X \subseteq \varnothing \times Y$; TRUE

(h) Every subset of $\mathbb{R}^2$ is of the form $A \times B$ for suitable subsets $A \subseteq \mathbb{R}$, $B \subseteq \mathbb{R}$. FALSE

Cartesian Products

If X and Y are sets then we denote by $X \times Y$ the set of all *ordered pairs* (x, y) with $x \in X$ and $y \in Y$. It is usual to write X^2 for $X \times X$. Thus the plane is the set $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$.

Quiz: Decide whether the following are True or False. Let

$$X = \{x \in \mathbb{R} : 1 \leq x \leq 3\}$$
$$Y = \{y \in \mathbb{R} : 1 \leq y \leq 2\}.$$

(a) $(1, 2) = (2, 1)$; FALSE

(b) $\{1, 2\} = \{2, 1\}$. TRUE

(c) $(\frac{5}{2}, \frac{3}{2}) \in X \times Y$; TRUE

(d) $(\frac{3}{2}, \frac{5}{2}) \in X \times Y$; FALSE

(e) $Y \times Y \subseteq X \times Y$; TRUE

(f) $X \subseteq Y$; FALSE

(g) $\varnothing \times X \subseteq \varnothing \times Y$; TRUE

(h) Every subset of $\mathbb{R}^2$ is of the form $A \times B$ for suitable subsets $A \subseteq \mathbb{R}$, $B \subseteq \mathbb{R}$. FALSE

Duality

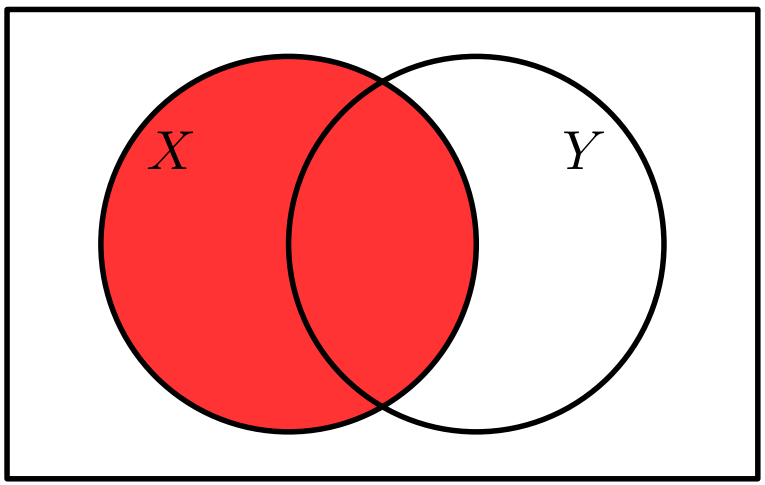
Given any equation involving subsets of a universe set U, the principle of *duality* says that if you swap $\cup$ and $\cap$ and replace every set with its complement in U, then the new equation still holds.

For example, suppose that X, Y, Z are subsets of U and $X \cup Y = Z$. Then by duality, $X' \cap Y' = Z'$. *Exercise:* What happens when $X' \cap Y' = Z'$ is dualized?

Duality

Given any equation involving subsets of a universe set U, the principle of *duality* says that if you swap $\cup$ and $\cap$ and replace every set with its complement in U, then the new equation still holds.

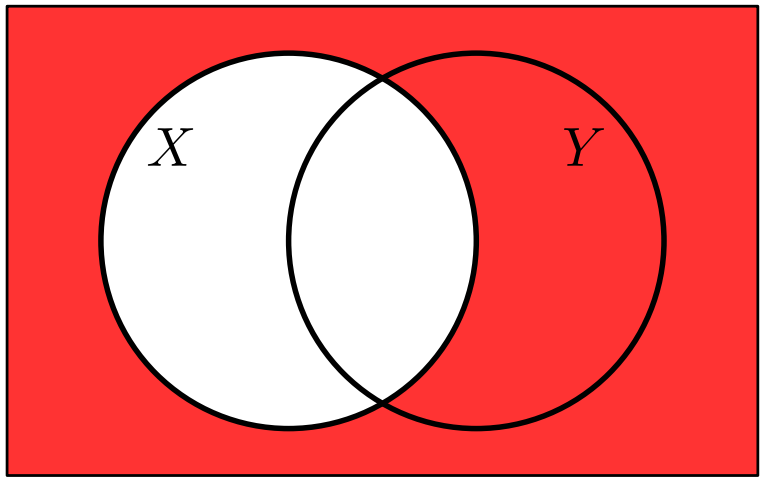
For example, suppose that X, Y, Z are subsets of U and $X \cup Y = Z$. Then by duality, $X' \cap Y' = Z'$. *Exercise:* What happens when $X' \cap Y' = Z'$ is dualized?



Duality

Given any equation involving subsets of a universe set U, the principle of *duality* says that if you swap $\cup$ and $\cap$ and replace every set with its complement in U, then the new equation still holds.

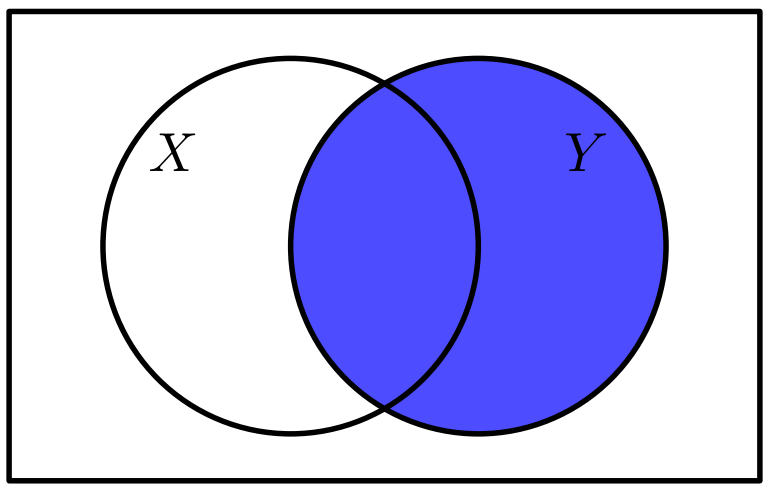
For example, suppose that X, Y, Z are subsets of U and $X \cup Y = Z$. Then by duality, $X' \cap Y' = Z'$. *Exercise:* What happens when $X' \cap Y' = Z'$ is dualized?



Duality

Given any equation involving subsets of a universe set U, the principle of *duality* says that if you swap $\cup$ and $\cap$ and replace every set with its complement in U, then the new equation still holds.

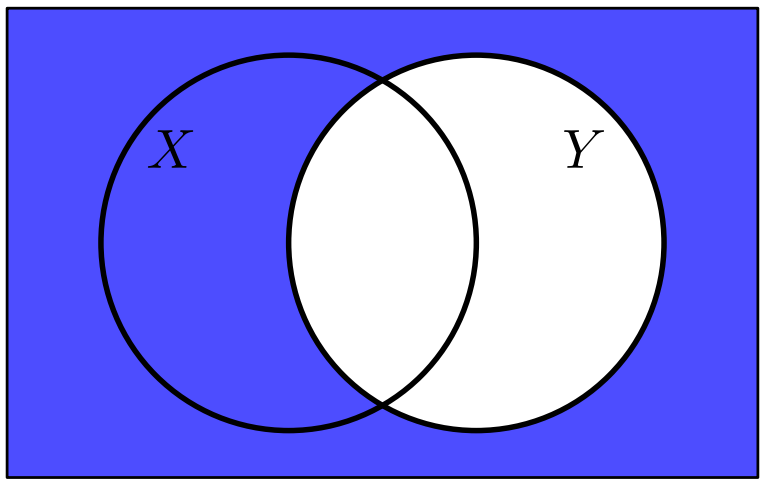
For example, suppose that X, Y, Z are subsets of U and $X \cup Y = Z$. Then by duality, $X' \cap Y' = Z'$. *Exercise:* What happens when $X' \cap Y' = Z'$ is dualized?



Duality

Given any equation involving subsets of a universe set U, the principle of *duality* says that if you swap $\cup$ and $\cap$ and replace every set with its complement in U, then the new equation still holds.

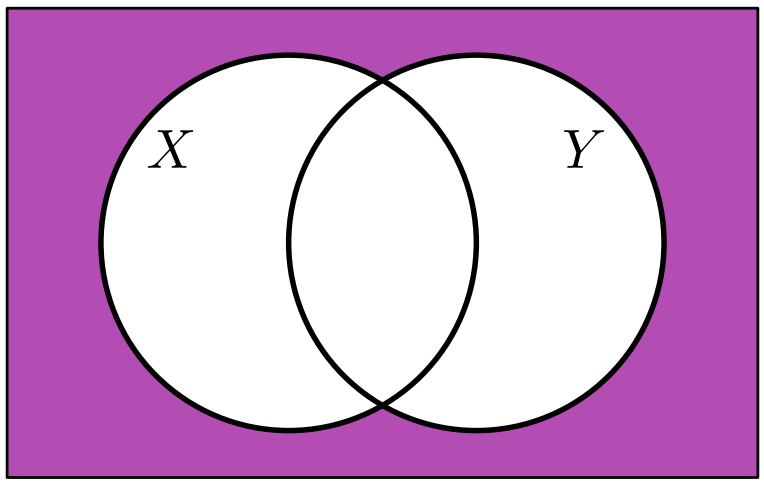
For example, suppose that X, Y, Z are subsets of U and $X \cup Y = Z$. Then by duality, $X' \cap Y' = Z'$. *Exercise:* What happens when $X' \cap Y' = Z'$ is dualized?



Duality

Given any equation involving subsets of a universe set U, the principle of *duality* says that if you swap $\cup$ and $\cap$ and replace every set with its complement in U, then the new equation still holds.

For example, suppose that X, Y, Z are subsets of U and $X \cup Y = Z$. Then by duality, $X' \cap Y' = Z'$. *Exercise:* What happens when $X' \cap Y' = Z'$ is dualized?



Common Errors on Sheet 6: Question 4

Write A for $(P \implies Q) \wedge (Q \implies R)$. To show that $A \implies (P \implies Q)$ is a tautology, you need to show that

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

holds for all truth values of P, Q and R.

Common Errors on Sheet 6: Question 4

Write A for $(P \implies Q) \wedge (Q \implies R)$. To show that $A \implies (P \implies Q)$ is a tautology, you need to show that

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

holds for all truth values of P, Q and R.

This is **not** the same as showing that A and $P \implies R$ always have the same truth value. If you did this, you were testing whether $A \iff (P \implies R)$ is a tautology. (It is not.)

Common Errors on Sheet 6: Question 4

Write A for $(P \Longrightarrow Q) \wedge (Q \Longrightarrow R)$. To show that $A \Longrightarrow (P \Longrightarrow Q)$ is a tautology, you need to show that

$$\big((P \Longrightarrow Q) \wedge (Q \Longrightarrow R)\big) \Longrightarrow (P \Longrightarrow R)$$

holds for all truth values of P, Q and R.

This is **not** the same as showing that A and $P \Longrightarrow R$ always have the same truth value. If you did this, you were testing whether $A \Longleftrightarrow (P \Longrightarrow R)$ is a tautology. (It is not.)

P	Q	R	$P \Longrightarrow Q$	$Q \Longrightarrow R$	A	$P \Longrightarrow R$	$A \Longrightarrow (P \Longrightarrow R)$
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	T
T	F	T	F	T	F	T	T
T	F	F	F	T	F	F	T
F	T	T	T	T	T	T	T
F	T	F	T	F	F	T	T
F	F	T	F	T	F	T	T
F	F	F	F	T	F	T	T

Common Errors on Sheet 6: Question 5

(a) Let P be the proposition $(\forall x \in \mathbb{R})(x^2 > 0)$. Write $\neg P$ without using '$\neg$'. Is P true? Explain your answer.

(b) Let Q be the proposition $(\forall m \in \mathbb{N})(\exists n \in \mathbb{N})(m \text{ divides } n)$. Write $\neg Q$ without using '$\neg$'. Is Q true? Explain your answer.

(c) Let R be the proposition $(\exists n \in \mathbb{N})(\forall m \in \mathbb{N})(m \text{ divides } n)$. Write $\neg R$ without using '$\neg$'. Is R true? Explain your answer.

Common Errors on Sheet 6: Question 5

(a) Let P be the proposition $(\forall x \in \mathbb{R})(x^2 > 0)$. Write $\neg P$ without using '$\neg$'. Is P true? Explain your answer.

(b) Let Q be the proposition $(\forall m \in \mathbb{N})(\exists n \in \mathbb{N})(m \text{ divides } n)$. Write $\neg Q$ without using '$\neg$'. Is Q true? Explain your answer.

(c) Let R be the proposition $(\exists n \in \mathbb{N})(\forall m \in \mathbb{N})(m \text{ divides } n)$. Write $\neg R$ without using '$\neg$'. Is R true? Explain your answer.

For (a), $\neg P$ is

$$(\exists x \in \mathbb{R})(x^2 \leq 0).$$

Many people dealt with the quantifier correctly, but then negated $x^2 > 0$ as $x^2 < 0$. This is wrong: if $x^2 \not> 0$ then $x^2 \leq 0$.

In (b) several people seemed to misinterpret the meaning of $(\forall m \in \mathbb{N})(\exists n \in \mathbb{N})(m \text{ divides } n)$. It means that for each $m \in \mathbb{N}$, there exists *some* $n \in \mathbb{N}$, such that m divides n. So for each m you need to find one n that works.

Many people wrote down $\neg Q$ then 'True'. I hope you all meant that Q was True, not that $\neg Q$ was True. Some words would help!

§7 Functions

Let X and Y be sets. A *function*

$$f : X \to Y$$

assigns to each $x \in X$ a unique element $f(x) \in Y$. If $f(x) = y$ then we say that y is the *image* of x under f. We say that X is the *domain* of f and Y is the *codomain* of f.

Example 7.1

(a) Define $f : \mathbb{Z} \to \mathbb{Z}$ by $f(x) = x + 1$. Then f is a function with domain $\mathbb{Z}$ and codomain $\mathbb{Z}$.

(b) Let $X = \{1, 2, 3\}$ and let $Y = \{1, 2, 3, 4\}$. Define $t : X \to Y$ by $t(1) = 2$, $t(2) = 1$, $t(3) = 4$. Then t is a function with domain X and codomain Y.

(c) Define $g : \mathbb{R} \to \mathbb{R}$ by $f(x) = x^2$. Then g is a function with domain $\mathbb{R}$ and codomain $\mathbb{R}$.

(d) Define $h : \mathbb{C} \to \mathbb{C}$ by $g(z) = z^2$. Then h is a function with domain $\mathbb{C}$ and codomain $\mathbb{C}$.

Injective, Surjective, Bijective

Definition 7.2

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

(i) We say that f is *injective* if for each $y \in Y$ there exists *at most one* $x \in X$ such that $f(x) = y$.

(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.

Example 7.3

(a) The function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = x + 1$ is bijective.

(b) The function $t : \{1, 2, 3\} \to \{1, 2, 3, 4\}$ defined in Example 7.1 is injective but not surjective.

(c) The function $g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = x^2$ is neither injective nor surjective.

(d) The function $h : \mathbb{C} \to \mathbb{C}$ defined by $h(z) = z^2$ is surjective but not injective.

Administration

- Please pass your answers to Sheet 3 to the person in your left. The person at the end of each row should put all work in the box and pass it down to the next row.
- Please correct a nasty typo: in last paragraph of §6

  'Yet another equivalent setting is digitial electonics: NOT gates correspond to negation $\neg$ *(or complement), AND gates to* **conjunction** $\wedge$ **(or intersection** $\cap$**)**, *and so on.'*

- Change of office hours: from Wednesday 2pm to Wednesday 11am. Tuesday 10am and Friday 3pm continue as before.
- Please take Problem Sheet 8 and pages 33 and 34 of the printed notes.

Real-Valued Functions

To give another example, we need some notation for intervals in $\mathbb{R}$. Given a, $b \in \mathbb{R}$, let

$$[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$$

Similarly $[a, \infty) = \{x \in \mathbb{R} : a \leq x\}$, and so on. (Please *do not* take this to mean that ∞ is a real number: this is not the case.)

Example 7.4

Let $f : [1, \infty) \to [0, \infty)$ be defined by $f(x) = x^2 + 2x - 3$. Then f is bijective.

To show that f is injective, we suppose that $f(x) = f(x')$, and show that $x = x'$. This is usually the most elegant way to present this sort of argument. Please use it for Question 5 on Sheet 7.

Administration

- Answers to Problem Sheet 7 will appear on Moodle later today.
- Hints for Question 2 and 4 on Problem Sheet 8 will appear on my blog shortly.
- There was a request for some extra questions on recent parts of the course. I will put up something on Moodle by Monday.

  Another good source for questions is textbooks, in particular Martin Liebeck's book *A concise introduction to pure mathematics*, which has the answers to odd-numbered questions at the back.

  You can also see me in office hours to get answers.

Inverse functions

Definition 7.5

Let $f : X \to Y$ be bijective. The *inverse function* to f is the function $g : Y \to X$ defined, for each $y \in Y$, by $g(y) = x$ where x is the unique element of X such that $f(x) = y$.

We denote the inverse function to f by f^{-1}. You may have seen this notation used for the inverses of the sine, cosine and tangent functions, which are bijective when defined with suitable domain and codomain.

Exercise 7.6

(a) Show, by sketching the graph, that if we define sine as a function $\sin : [-\pi/2, \pi/2] \to [-1, 1]$ then sin is bijective. Draw the inverse function on the same set of axes.

(b) Repeat (a) for cosine. (You should keep $[-1, 1]$ as the codomain but change the domain.)

More inverse functions

Example 7.7

(a) Define $f : [0, \infty) \to [0, \infty)$ by $f(x) = x^2$. Then f is bijective with inverse function $g(y) = \sqrt{y}$.

(b) Define $f : \mathbb{R} \to \mathbb{R}^{>0}$ by $f(x) = \mathrm{e}^x$. Then f is bijective with inverse function $g(y) = \log y$.

Quiz: True or False?

(a) $f(x) = x^2 + 1 : [0, \infty) \to [0, \infty)$ is injective;
(b) $g(x) = x^2 + 1 : [0, \infty) \to [0, \infty)$ is surjective;
(c) $h(x) = x^2 + 1 : [0, \infty) \to [1, \infty)$ is injective;
(d) $h(x) = x^2 + 1 : [0, \infty) \to [1, \infty)$ is surjective;
(e) The inverse of h is $h^{-1}(y) = \sqrt{y - 1}$;
(f) The codomain of h^{-1} is $[0, \infty)$;
(g) There is a function $\varnothing \to \{1, 2, 3\}$;
(h) There is a function $\{1, 2, 3\} \to \varnothing$.
(i) The unique function $\varnothing \to \varnothing$ is (1) injective (2) surjective

More inverse functions

Example 7.7

(a) Define $f : [0, \infty) \to [0, \infty)$ by $f(x) = x^2$. Then f is bijective with inverse function $g(y) = \sqrt{y}$.

(b) Define $f : \mathbb{R} \to \mathbb{R}^{>0}$ by $f(x) = \mathrm{e}^x$. Then f is bijective with inverse function $g(y) = \log y$.

Quiz: True or False?

(a) $f(x) = x^2 + 1 : [0, \infty) \to [0, \infty)$ is injective; TRUE
(b) $g(x) = x^2 + 1 : [0, \infty) \to [0, \infty)$ is surjective;
(c) $h(x) = x^2 + 1 : [0, \infty) \to [1, \infty)$ is injective;
(d) $h(x) = x^2 + 1 : [0, \infty) \to [1, \infty)$ is surjective;
(e) The inverse of h is $h^{-1}(y) = \sqrt{y - 1}$;
(f) The codomain of h^{-1} is $[0, \infty)$;
(g) There is a function $\varnothing \to \{1, 2, 3\}$;
(h) There is a function $\{1, 2, 3\} \to \varnothing$.
(i) The unique function $\varnothing \to \varnothing$ is (1) injective (2) surjective

More inverse functions

Example 7.7

(a) Define $f : [0, \infty) \to [0, \infty)$ by $f(x) = x^2$. Then f is bijective with inverse function $g(y) = \sqrt{y}$.

(b) Define $f : \mathbb{R} \to \mathbb{R}^{>0}$ by $f(x) = \mathrm{e}^x$. Then f is bijective with inverse function $g(y) = \log y$.

Quiz: True or False?

(a) $f(x) = x^2 + 1 : [0, \infty) \to [0, \infty)$ is injective; TRUE
(b) $g(x) = x^2 + 1 : [0, \infty) \to [0, \infty)$ is surjective; FALSE
(c) $h(x) = x^2 + 1 : [0, \infty) \to [1, \infty)$ is injective;
(d) $h(x) = x^2 + 1 : [0, \infty) \to [1, \infty)$ is surjective;
(e) The inverse of h is $h^{-1}(y) = \sqrt{y - 1}$;
(f) The codomain of h^{-1} is $[0, \infty)$;
(g) There is a function $\varnothing \to \{1, 2, 3\}$;
(h) There is a function $\{1, 2, 3\} \to \varnothing$.
(i) The unique function $\varnothing \to \varnothing$ is (1) injective (2) surjective

More inverse functions

Example 7.7

(a) Define $f : [0, \infty) \to [0, \infty)$ by $f(x) = x^2$. Then f is bijective with inverse function $g(y) = \sqrt{y}$.

(b) Define $f : \mathbb{R} \to \mathbb{R}^{>0}$ by $f(x) = \mathrm{e}^x$. Then f is bijective with inverse function $g(y) = \log y$.

Quiz: True or False?

(a) $f(x) = x^2 + 1 : [0, \infty) \to [0, \infty)$ is injective; TRUE
(b) $g(x) = x^2 + 1 : [0, \infty) \to [0, \infty)$ is surjective; FALSE
(c) $h(x) = x^2 + 1 : [0, \infty) \to [1, \infty)$ is injective; TRUE
(d) $h(x) = x^2 + 1 : [0, \infty) \to [1, \infty)$ is surjective;
(e) The inverse of h is $h^{-1}(y) = \sqrt{y - 1}$;
(f) The codomain of h^{-1} is $[0, \infty)$;
(g) There is a function $\varnothing \to \{1, 2, 3\}$;
(h) There is a function $\{1, 2, 3\} \to \varnothing$.
(i) The unique function $\varnothing \to \varnothing$ is (1) injective (2) surjective

More inverse functions

Example 7.7

(a) Define $f : [0, \infty) \to [0, \infty)$ by $f(x) = x^2$. Then f is bijective with inverse function $g(y) = \sqrt{y}$.

(b) Define $f : \mathbb{R} \to \mathbb{R}^{>0}$ by $f(x) = \mathrm{e}^x$. Then f is bijective with inverse function $g(y) = \log y$.

Quiz: True or False?

(a) $f(x) = x^2 + 1 : [0, \infty) \to [0, \infty)$ is injective; TRUE
(b) $g(x) = x^2 + 1 : [0, \infty) \to [0, \infty)$ is surjective; FALSE
(c) $h(x) = x^2 + 1 : [0, \infty) \to [1, \infty)$ is injective; TRUE
(d) $h(x) = x^2 + 1 : [0, \infty) \to [1, \infty)$ is surjective; TRUE
(e) The inverse of h is $h^{-1}(y) = \sqrt{y - 1}$;
(f) The codomain of h^{-1} is $[0, \infty)$;
(g) There is a function $\varnothing \to \{1, 2, 3\}$;
(h) There is a function $\{1, 2, 3\} \to \varnothing$.
(i) The unique function $\varnothing \to \varnothing$ is (1) injective (2) surjective

More inverse functions

Example 7.7

(a) Define $f : [0, \infty) \to [0, \infty)$ by $f(x) = x^2$. Then f is bijective with inverse function $g(y) = \sqrt{y}$.

(b) Define $f : \mathbb{R} \to \mathbb{R}^{>0}$ by $f(x) = \mathrm{e}^x$. Then f is bijective with inverse function $g(y) = \log y$.

Quiz: True or False?

(a) $f(x) = x^2 + 1 : [0, \infty) \to [0, \infty)$ is injective; TRUE
(b) $g(x) = x^2 + 1 : [0, \infty) \to [0, \infty)$ is surjective; FALSE
(c) $h(x) = x^2 + 1 : [0, \infty) \to [1, \infty)$ is injective; TRUE
(d) $h(x) = x^2 + 1 : [0, \infty) \to [1, \infty)$ is surjective; TRUE
(e) The inverse of h is $h^{-1}(y) = \sqrt{y - 1}$; TRUE
(f) The codomain of h^{-1} is $[0, \infty)$;
(g) There is a function $\varnothing \to \{1, 2, 3\}$;
(h) There is a function $\{1, 2, 3\} \to \varnothing$.
(i) The unique function $\varnothing \to \varnothing$ is (1) injective (2) surjective

More inverse functions

Example 7.7

(a) Define $f : [0, \infty) \to [0, \infty)$ by $f(x) = x^2$. Then f is bijective with inverse function $g(y) = \sqrt{y}$.

(b) Define $f : \mathbb{R} \to \mathbb{R}^{>0}$ by $f(x) = \mathrm{e}^x$. Then f is bijective with inverse function $g(y) = \log y$.

Quiz: True or False?

(a) $f(x) = x^2 + 1 : [0, \infty) \to [0, \infty)$ is injective; TRUE
(b) $g(x) = x^2 + 1 : [0, \infty) \to [0, \infty)$ is surjective; FALSE
(c) $h(x) = x^2 + 1 : [0, \infty) \to [1, \infty)$ is injective; TRUE
(d) $h(x) = x^2 + 1 : [0, \infty) \to [1, \infty)$ is surjective; TRUE
(e) The inverse of h is $h^{-1}(y) = \sqrt{y - 1}$; TRUE
(f) The codomain of h^{-1} is $[0, \infty)$; TRUE
(g) There is a function $\varnothing \to \{1, 2, 3\}$;
(h) There is a function $\{1, 2, 3\} \to \varnothing$.
(i) The unique function $\varnothing \to \varnothing$ is (1) injective (2) surjective

More inverse functions

Example 7.7

(a) Define $f : [0, \infty) \to [0, \infty)$ by $f(x) = x^2$. Then f is bijective with inverse function $g(y) = \sqrt{y}$.

(b) Define $f : \mathbb{R} \to \mathbb{R}^{>0}$ by $f(x) = \mathrm{e}^x$. Then f is bijective with inverse function $g(y) = \log y$.

Quiz: True or False?

(a) $f(x) = x^2 + 1 : [0, \infty) \to [0, \infty)$ is injective; TRUE
(b) $g(x) = x^2 + 1 : [0, \infty) \to [0, \infty)$ is surjective; FALSE
(c) $h(x) = x^2 + 1 : [0, \infty) \to [1, \infty)$ is injective; TRUE
(d) $h(x) = x^2 + 1 : [0, \infty) \to [1, \infty)$ is surjective; TRUE
(e) The inverse of h is $h^{-1}(y) = \sqrt{y - 1}$; TRUE
(f) The codomain of h^{-1} is $[0, \infty)$; TRUE
(g) There is a function $\varnothing \to \{1, 2, 3\}$; TRUE
(h) There is a function $\{1, 2, 3\} \to \varnothing$.
(i) The unique function $\varnothing \to \varnothing$ is (1) injective (2) surjective

More inverse functions

Example 7.7

(a) Define $f : [0, \infty) \to [0, \infty)$ by $f(x) = x^2$. Then f is bijective with inverse function $g(y) = \sqrt{y}$.

(b) Define $f : \mathbb{R} \to \mathbb{R}^{>0}$ by $f(x) = \mathrm{e}^x$. Then f is bijective with inverse function $g(y) = \log y$.

Quiz: True or False?

(a) $f(x) = x^2 + 1 : [0, \infty) \to [0, \infty)$ is injective; TRUE
(b) $g(x) = x^2 + 1 : [0, \infty) \to [0, \infty)$ is surjective; FALSE
(c) $h(x) = x^2 + 1 : [0, \infty) \to [1, \infty)$ is injective; TRUE
(d) $h(x) = x^2 + 1 : [0, \infty) \to [1, \infty)$ is surjective; TRUE
(e) The inverse of h is $h^{-1}(y) = \sqrt{y - 1}$; TRUE
(f) The codomain of h^{-1} is $[0, \infty)$; TRUE
(g) There is a function $\varnothing \to \{1, 2, 3\}$; TRUE
(h) There is a function $\{1, 2, 3\} \to \varnothing$. FALSE
(i) The unique function $\varnothing \to \varnothing$ is (1) injective (2) surjective

More inverse functions

Example 7.7

(a) Define $f : [0, \infty) \to [0, \infty)$ by $f(x) = x^2$. Then f is bijective with inverse function $g(y) = \sqrt{y}$.

(b) Define $f : \mathbb{R} \to \mathbb{R}^{>0}$ by $f(x) = \mathrm{e}^x$. Then f is bijective with inverse function $g(y) = \log y$.

Quiz: True or False?

(a) $f(x) = x^2 + 1 : [0, \infty) \to [0, \infty)$ is injective; TRUE
(b) $g(x) = x^2 + 1 : [0, \infty) \to [0, \infty)$ is surjective; FALSE
(c) $h(x) = x^2 + 1 : [0, \infty) \to [1, \infty)$ is injective; TRUE
(d) $h(x) = x^2 + 1 : [0, \infty) \to [1, \infty)$ is surjective; TRUE
(e) The inverse of h is $h^{-1}(y) = \sqrt{y - 1}$; TRUE
(f) The codomain of h^{-1} is $[0, \infty)$; TRUE
(g) There is a function $\varnothing \to \{1, 2, 3\}$; TRUE
(h) There is a function $\{1, 2, 3\} \to \varnothing$. FALSE
(i) The unique function $\varnothing \to \varnothing$ is (1) injective (2) surjective T

More inverse functions

Example 7.7

(a) Define $f : [0, \infty) \to [0, \infty)$ by $f(x) = x^2$. Then f is bijective with inverse function $g(y) = \sqrt{y}$.

(b) Define $f : \mathbb{R} \to \mathbb{R}^{>0}$ by $f(x) = \mathrm{e}^x$. Then f is bijective with inverse function $g(y) = \log y$.

Quiz: True or False?

(a) $f(x) = x^2 + 1 : [0, \infty) \to [0, \infty)$ is injective; TRUE
(b) $g(x) = x^2 + 1 : [0, \infty) \to [0, \infty)$ is surjective; FALSE
(c) $h(x) = x^2 + 1 : [0, \infty) \to [1, \infty)$ is injective; TRUE
(d) $h(x) = x^2 + 1 : [0, \infty) \to [1, \infty)$ is surjective; TRUE
(e) The inverse of h is $h^{-1}(y) = \sqrt{y - 1}$; TRUE
(f) The codomain of h^{-1} is $[0, \infty)$; TRUE
(g) There is a function $\varnothing \to \{1, 2, 3\}$; TRUE
(h) There is a function $\{1, 2, 3\} \to \varnothing$. FALSE
(i) The unique function $\varnothing \to \varnothing$ is (1) injective (2) surjective T T

Composition

Definition 7.8

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

Note that gf means 'do f then do g'. So one has to get used to reading function compositions from right to left. In the special case where $Y = X$ and $g = f$ we write f^2 for ff, f^3 for fff and so on.

Theorem 7.9

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

(i) *If f and g are injective then $gf : X \to Z$ is injective.*

(ii) *If f and g are surjective then $gf : X \to Z$ is surjective.*

(iii) *If f and g are bijective then $gf : X \to Z$ is bijective.*

Administration

- If your surname begins with
  - A–M your work is probably the red folder
  - N–Z your work is probably in the blue folder
- **Please** remember to put your full name and/or student number on your work.
- **Remember a reasonable attempt at each of the 8 assessed sheets is worth 1.25% of your final mark.**
- There are model answers on Moodle for Sheet 7.
- There are some revision examples and questions on Part C of the course on Moodle (see week 9).
- There are hints for Questions 2 and 4 on Sheet 8 on the blog (see link at top of Moodle page). Email or see the lecturer if you want any more hints.
- Office hours: the Wednesday hour has moved from 2pm to 11am. Tuesday 11am, Friday 3pm as before.

Quiz on Inverse Functions

Definition 7.5

Let X and Y be sets and let $f : X \to Y$ be a bijective function. Recall that the *inverse function* $f^{-1} : Y \to X$ is the function defined by

$f^{-1}(y) = x \iff x$ is the unique element of X such that $f(x) = y$.

Quiz: For each of the functions drawn on the board, decide whether they are bijective. Which two bijective functions are inverse to one another?

Inverses on One Side

Theorem 7.10

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

(i) *f is injective $\iff$ there exists a function $g : Y \to X$ such that $gf = i_X$.*

(ii) *f is surjective $\iff$ there exists a function $h : Y \to X$ such that $fh = i_Y$.*

Administration

- Please pass your answers to Sheet 8 to the person in your left. The person at the end of each row should put all work in the box and pass it down to the next row.
- Please take Problem Sheet 9. This is the final problem sheet that will be marked this term. (Problem Sheet 10 will be issued next week for the vacation.)
- Spare copies of pages 35 to 36 and diagrams issued on Monday.

§8 Relations

Let X be a set. A *relation* on X is a subset of $X \times X$. If (x, y) is in the subset, then we say that x and y are *related*. More informally, a relation is a true-or-false statement that depends on two elements of X.

Example 8.1

(i) Let $X = \mathbb{R}$. Then '$x < y$' is a relation on X.

(ii) Let $X = \mathbb{Z}$. Then '$m - n$ is even' is a relation on X.

(iii) Let X be the set of all subsets of $\{1, 2, 3\}$. Then $A \subseteq B$ is a relation on X.

(iv) Let X be the set of people in this room. Then $x \sim y$ if x can see y is a relation on X.

Formally, the relation in (i) is the subset

$$\{(x, y) \in \mathbb{R} \times \mathbb{R} : x < y\}.$$

Usually it is clearer to specify relations more informally, as in Example 8.1.

Diagrams

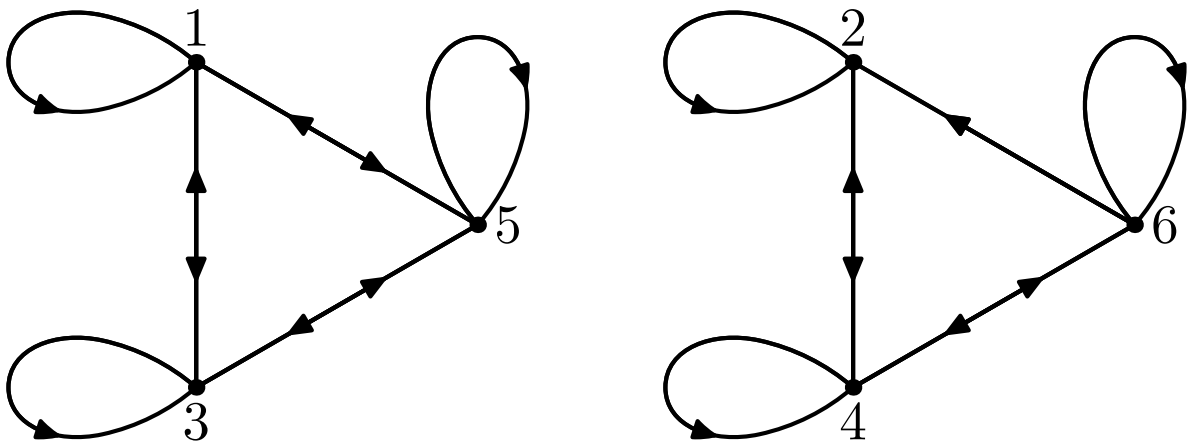
Let X be a set and let $\equiv$ be a relation defined on X. To represent $\equiv$ on a diagram, draw a dot for each element of X. Then for each x, $y \in X$ such that $x \equiv y$, draw an arrow *from* x *to* y. If $x \equiv x$ draw a loop from x to itself.

Example 8.2

Let $X = \{1, 2, 3, 4, 5, 6\}$ and let $\equiv$ be the relation defined on X by

$$x \equiv y \iff x - y \text{ is even.}$$

The diagram for X is shown below.



Definition 8.4

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 $x, y, z \in X$

$$x \sim y \text{ and } y \sim z \Longrightarrow x \sim z.$$

Exercise 8.5

Let X be the set of people sitting in this lecture room. For each of the following relations, decide whether it is (1) reflexive, (2) symmetric and (3) transitive.

(a) $x \sim y$ if x is sitting in a strictly higher row than y;

(b) $x \sim y$ if x and y are in the same row, or x is higher than y;

(c) $x \sim y$ if x and y are sitting in the same row;

(d) $x \sim y$ if x and y are friends.

(e) $x \sim y$ if x is not y.

Answers to Exercise 8.5

	Reflexive	Symmetric	Transitive
(a) x is sitting in a strictly higher row than y			
(b) x and y are in the same row, or x is higher than y			
(c) x and y are sitting in the same row			
(d) x and y are friends			
(e) x is not y			

Answers to Exercise 8.5

	Reflexive	Symmetric	Transitive
(a) x is sitting in a strictly higher row than y	False	False	True
(b) x and y are in the same row, or x is higher than y			
(c) x and y are sitting in the same row			
(d) x and y are friends			
(e) x is not y			

Answers to Exercise 8.5

	Reflexive	Symmetric	Transitive
(a) x is sitting in a strictly higher row than y	False	False	True
(b) x and y are in the same row, or x is higher than y	True	False	True
(c) x and y are sitting in the same row			
(d) x and y are friends			
(e) x is not y			

Answers to Exercise 8.5

	Reflexive	Symmetric	Transitive
(a) x is sitting in a strictly higher row than y	False	False	True
(b) x and y are in the same row, or x is higher than y	True	False	True
(c) x and y are sitting in the same row	True	True	True
(d) x and y are friends			
(e) x is not y			

[1]We will suppose that a person is well-disposed towards themselves.

Answers to Exercise 8.5

	Reflexive	Symmetric	Transitive
(a) x is sitting in a strictly higher row than y	False	False	True
(b) x and y are in the same row, or x is higher than y	True	False	True
(c) x and y are sitting in the same row	True	True	True
(d) x and y are friends	True[1]	True	False
(e) x is not y			

[1]We will suppose that a person is well-disposed towards themselves.

Answers to Exercise 8.5

	Reflexive	Symmetric	Transitive
(a) x is sitting in a strictly higher row than y	False	False	True
(b) x and y are in the same row, or x is higher than y	True	False	True
(c) x and y are sitting in the same row	True	True	True
(d) x and y are friends	True[1]	True	False
(e) x is not y	False	True	False[2]

[1] We will suppose that a person is well-disposed towards themselves.

[2] Take two different people x and y. Then x is not y so $x \sim y$ and y is not x so $y \sim x$. But $x \not\sim x$ so the relation $\sim$ is not transitive.

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

$$[x]_\sim = \{z \in X : z \sim x\}.$$

So the equivalence class of x consists of all the elements of X that relate to x.

If the relation will be clear we may write $[x]$ rather than $[x]_\sim$.

Example 8.6

Define a relation $\sim$ on $\mathbb{C}$ by $z \equiv w$ if $|z| = |w|$. Then $\sim$ is an equivalence relation. The equivalence classes are the circles centred on 0, together with $[0]_\sim = \{0\}$.

Congruences

Example 8.7

Let $n \in \mathbb{N}$. Define a relation on the set of integers $\mathbb{Z}$ by $a \equiv b$ if n divides $b - a$. [**changed from a-b to be consistent with Definition 9.1**] Then $\equiv$ is an equivalence relation. The different equivalence class are

$$\begin{aligned} [0] &= \{qn : q \in \mathbb{Z}\} \\ [1] &= \{1 + qn : q \in \mathbb{Z}\} \\ &\vdots \\ [n-1] &= \{(n-1) + qn : q \in \mathbb{Z}\} \end{aligned}$$

Quiz: True or false?

(a) $2 \equiv -1$

(b) $[2] = [-1]$

(c) $6 \in [2]$

(d) $6 \equiv 2$

(e) $-37 \equiv 2$

(f) $[-37] = [-2]$

Congruences

Example 8.7

Let $n \in \mathbb{N}$. Define a relation on the set of integers $\mathbb{Z}$ by $a \equiv b$ if n divides $b - a$. [**changed from a-b to be consistent with Definition 9.1**] Then $\equiv$ is an equivalence relation. The different equivalence class are

$$\begin{aligned} [0] &= \{qn : q \in \mathbb{Z}\} \\ [1] &= \{1 + qn : q \in \mathbb{Z}\} \\ &\vdots \\ [n-1] &= \{(n-1) + qn : q \in \mathbb{Z}\} \end{aligned}$$

Quiz: True or false?

(a) $2 \equiv -1$ TRUE

(b) $[2] = [-1]$

(c) $6 \in [2]$

(d) $6 \equiv 2$

(e) $-37 \equiv 2$

(f) $[-37] = [-2]$

Congruences

Example 8.7

Let $n \in \mathbb{N}$. Define a relation on the set of integers $\mathbb{Z}$ by $a \equiv b$ if n divides $b - a$. [**changed from a-b to be consistent with Definition 9.1**] Then $\equiv$ is an equivalence relation. The different equivalence class are

$$\begin{aligned} [0] &= \{qn : q \in \mathbb{Z}\} \\ [1] &= \{1 + qn : q \in \mathbb{Z}\} \\ &\vdots \\ [n-1] &= \{(n-1) + qn : q \in \mathbb{Z}\} \end{aligned}$$

Quiz: True or false?

(a) $2 \equiv -1$ TRUE

(b) $[2] = [-1]$ TRUE

(c) $6 \in [2]$

(d) $6 \equiv 2$

(e) $-37 \equiv 2$

(f) $[-37] = [-2]$

Congruences

Example 8.7

Let $n \in \mathbb{N}$. Define a relation on the set of integers $\mathbb{Z}$ by $a \equiv b$ if n divides $b - a$. [**changed from a-b to be consistent with Definition 9.1**] Then $\equiv$ is an equivalence relation. The different equivalence class are

$$\begin{aligned} [0] &= \{qn : q \in \mathbb{Z}\} \\ [1] &= \{1 + qn : q \in \mathbb{Z}\} \\ &\vdots \\ [n-1] &= \{(n-1) + qn : q \in \mathbb{Z}\} \end{aligned}$$

Quiz: True or false?

(a) $2 \equiv -1$	TRUE	(d) $6 \equiv 2$
(b) $[2] = [-1]$	TRUE	(e) $-37 \equiv 2$
(c) $6 \in [2]$	FALSE	(f) $[-37] = [-2]$

Congruences

Example 8.7

Let $n \in \mathbb{N}$. Define a relation on the set of integers $\mathbb{Z}$ by $a \equiv b$ if n divides $b - a$. [**changed from a-b to be consistent with Definition 9.1**] Then $\equiv$ is an equivalence relation. The different equivalence class are

$$\begin{aligned} [0] &= \{qn : q \in \mathbb{Z}\} \\ [1] &= \{1 + qn : q \in \mathbb{Z}\} \\ &\vdots \\ [n-1] &= \{(n-1) + qn : q \in \mathbb{Z}\} \end{aligned}$$

Quiz: True or false?

(a) $2 \equiv -1$ TRUE

(b) $[2] = [-1]$ TRUE

(c) $6 \in [2]$ FALSE

(d) $6 \equiv 2$ FALSE

(e) $-37 \equiv 2$

(f) $[-37] = [-2]$

Congruences

Example 8.7

Let $n \in \mathbb{N}$. Define a relation on the set of integers $\mathbb{Z}$ by $a \equiv b$ if n divides $b - a$. [**changed from a-b to be consistent with Definition 9.1**] Then $\equiv$ is an equivalence relation. The different equivalence class are

$$\begin{aligned} [0] &= \{qn : q \in \mathbb{Z}\} \\ [1] &= \{1 + qn : q \in \mathbb{Z}\} \\ &\vdots \\ [n-1] &= \{(n-1) + qn : q \in \mathbb{Z}\} \end{aligned}$$

Quiz: True or false?

(a) $2 \equiv -1$ TRUE

(b) $[2] = [-1]$ TRUE

(c) $6 \in [2]$ FALSE

(d) $6 \equiv 2$ FALSE

(e) $-37 \equiv 2$ TRUE

(f) $[-37] = [-2]$

Congruences

Example 8.7

Let $n \in \mathbb{N}$. Define a relation on the set of integers $\mathbb{Z}$ by $a \equiv b$ if n divides $b - a$. [**changed from a-b to be consistent with Definition 9.1**] Then $\equiv$ is an equivalence relation. The different equivalence class are

$$\begin{aligned} [0] &= \{qn : q \in \mathbb{Z}\} \\ [1] &= \{1 + qn : q \in \mathbb{Z}\} \\ &\vdots \\ [n-1] &= \{(n-1) + qn : q \in \mathbb{Z}\} \end{aligned}$$

Quiz: True or false?

(a) $2 \equiv -1$ TRUE

(b) $[2] = [-1]$ TRUE

(c) $6 \in [2]$ FALSE

(d) $6 \equiv 2$ FALSE

(e) $-37 \equiv 2$ TRUE

(f) $[-37] = [-2]$ TRUE

Administration

- If your surname begins with
  - A–F your work is in the red folder
  - G–M your work is in the blue folder
  - N–S your work is in the green folder
  - S–Z your work is in the yellow folder
- **Please** remember to put your full name and/or student number on your work.
- **Remember a reasonable attempt at each of the 8 assessed sheets is worth 1.25% of your final mark.**
- There are model answers on Moodle for Sheet 8 along with a wide selection of common errors.
- There are some revision examples and questions on Part C of the course on Moodle (see week 9). Please see the lecturer to go through these. I will put up answers at the end of term.
- Email or see the lecturer if you want any hints for Problem Sheet 8.
- Office hours: the Wednesday hour moved last week from 2pm to 11am. Tuesday 11am, Friday 3pm as before.

Example 8.7 (Special case $n = 3$)

Define a relation on the set of integers $\mathbb{Z}$ by $a \equiv b$ if 3 divides $b - a$. Then $\equiv$ is an equivalence relation. The different equivalence class are

$$[0] = \{3q : q \in \mathbb{Z}\}$$
$$[1] = \{1 + qn : q \in \mathbb{Z}\}$$
$$[2] = \{2 + qn : q \in \mathbb{Z}\}$$

Here is the argument from the end of last lecture that $[n] = [0]$, in the special case $n = 3$:

$$[3] = \{3+qn : q \in \mathbb{Z}\} = \{3+(p-1)n : p \in \mathbb{Z}\} = \{pn : p \in \mathbb{Z}\} = [0].$$

Quiz: True or false?

(a) $5 \equiv 8$

(b) $5 \in [8]$

(c) $8 \in [5]$

(d) $[5] = [8]$

(e) $5 \equiv [9]$

(f) $[5] = [9]$

Example 8.7 (Special case $n = 3$)

Define a relation on the set of integers $\mathbb{Z}$ by $a \equiv b$ if 3 divides $b - a$. Then $\equiv$ is an equivalence relation. The different equivalence class are

$$[0] = \{3q : q \in \mathbb{Z}\}$$
$$[1] = \{1 + qn : q \in \mathbb{Z}\}$$
$$[2] = \{2 + qn : q \in \mathbb{Z}\}$$

Here is the argument from the end of last lecture that $[n] = [0]$, in the special case $n = 3$:

$$[3] = \{3+qn : q \in \mathbb{Z}\} = \{3+(p-1)n : p \in \mathbb{Z}\} = \{pn : p \in \mathbb{Z}\} = [0].$$

Quiz: True or false?

(a) $5 \equiv 8$ TRUE

(b) $5 \in [8]$

(c) $8 \in [5]$

(d) $[5] = [8]$

(e) $5 \equiv [9]$

(f) $[5] = [9]$

Example 8.7 (Special case $n = 3$)

Define a relation on the set of integers $\mathbb{Z}$ by $a \equiv b$ if 3 divides $b - a$. Then $\equiv$ is an equivalence relation. The different equivalence class are

$$[0] = \{3q : q \in \mathbb{Z}\}$$
$$[1] = \{1 + qn : q \in \mathbb{Z}\}$$
$$[2] = \{2 + qn : q \in \mathbb{Z}\}$$

Here is the argument from the end of last lecture that $[n] = [0]$, in the special case $n = 3$:

$$[3] = \{3+qn : q \in \mathbb{Z}\} = \{3+(p-1)n : p \in \mathbb{Z}\} = \{pn : p \in \mathbb{Z}\} = [0].$$

Quiz: True or false?

(a) $5 \equiv 8$ TRUE

(b) $5 \in [8]$ TRUE

(c) $8 \in [5]$

(d) $[5] = [8]$

(e) $5 \equiv [9]$

(f) $[5] = [9]$

Example 8.7 (Special case $n = 3$)

Define a relation on the set of integers $\mathbb{Z}$ by $a \equiv b$ if 3 divides $b - a$. Then $\equiv$ is an equivalence relation. The different equivalence class are

$$[0] = \{3q : q \in \mathbb{Z}\}$$
$$[1] = \{1 + qn : q \in \mathbb{Z}\}$$
$$[2] = \{2 + qn : q \in \mathbb{Z}\}$$

Here is the argument from the end of last lecture that $[n] = [0]$, in the special case $n = 3$:

$$[3] = \{3+qn : q \in \mathbb{Z}\} = \{3+(p-1)n : p \in \mathbb{Z}\} = \{pn : p \in \mathbb{Z}\} = [0].$$

Quiz: True or false?

(a) $5 \equiv 8$ TRUE

(b) $5 \in [8]$ TRUE

(c) $8 \in [5]$ TRUE

(d) $[5] = [8]$

(e) $5 \equiv [9]$

(f) $[5] = [9]$

Example 8.7 (Special case $n = 3$)

Define a relation on the set of integers $\mathbb{Z}$ by $a \equiv b$ if 3 divides $b - a$. Then $\equiv$ is an equivalence relation. The different equivalence class are

$$[0] = \{3q : q \in \mathbb{Z}\}$$
$$[1] = \{1 + qn : q \in \mathbb{Z}\}$$
$$[2] = \{2 + qn : q \in \mathbb{Z}\}$$

Here is the argument from the end of last lecture that $[n] = [0]$, in the special case $n = 3$:

$$[3] = \{3+qn : q \in \mathbb{Z}\} = \{3+(p-1)n : p \in \mathbb{Z}\} = \{pn : p \in \mathbb{Z}\} = [0].$$

Quiz: True or false?

(a) $5 \equiv 8$ TRUE

(b) $5 \in [8]$ TRUE

(c) $8 \in [5]$ TRUE

(d) $[5] = [8]$ TRUE

(e) $5 \equiv [9]$

(f) $[5] = [9]$

Example 8.7 (Special case $n = 3$)

Define a relation on the set of integers $\mathbb{Z}$ by $a \equiv b$ if 3 divides $b - a$. Then $\equiv$ is an equivalence relation. The different equivalence class are

$$[0] = \{3q : q \in \mathbb{Z}\}$$
$$[1] = \{1 + qn : q \in \mathbb{Z}\}$$
$$[2] = \{2 + qn : q \in \mathbb{Z}\}$$

Here is the argument from the end of last lecture that $[n] = [0]$, in the special case $n = 3$:

$$[3] = \{3+qn : q \in \mathbb{Z}\} = \{3+(p-1)n : p \in \mathbb{Z}\} = \{pn : p \in \mathbb{Z}\} = [0].$$

Quiz: True or false?

(a) $5 \equiv 8$ TRUE

(b) $5 \in [8]$ TRUE

(c) $8 \in [5]$ TRUE

(d) $[5] = [8]$ TRUE

(e) $5 \equiv [9]$ FALSE

(f) $[5] = [9]$

Example 8.7 (Special case $n = 3$)

Define a relation on the set of integers $\mathbb{Z}$ by $a \equiv b$ if 3 divides $b - a$. Then $\equiv$ is an equivalence relation. The different equivalence class are

$$[0] = \{3q : q \in \mathbb{Z}\}$$
$$[1] = \{1 + qn : q \in \mathbb{Z}\}$$
$$[2] = \{2 + qn : q \in \mathbb{Z}\}$$

Here is the argument from the end of last lecture that $[n] = [0]$, in the special case $n = 3$:

$$[3] = \{3+qn : q \in \mathbb{Z}\} = \{3+(p-1)n : p \in \mathbb{Z}\} = \{pn : p \in \mathbb{Z}\} = [0].$$

Quiz: True or false?

(a) $5 \equiv 8$	TRUE	(d) $[5] = [8]$	TRUE
(b) $5 \in [8]$	TRUE	(e) $5 \equiv [9]$	FALSE
(c) $8 \in [5]$	TRUE	(f) $[5] = [9]$	TRUE

Partitions

Definition 8.8

Let X be a set.

(i) We say that subsets $A, B \subseteq X$ are *disjoint* if $A \cap B = \varnothing$.

(ii) A *partition* of X is a collection of non-empty subsets of X such that any element of X is in one of the subsets, and any two subsets are either equal or disjoint.

For instance, in Example 8.7 the equivalence classes

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

partition $\mathbb{Z}$ since they are disjoint and

$$[0] \cup [1] \cup \cdots \cup [n-1] = \mathbb{Z}.$$

Theorem 8.9

Let $\sim$ be an equivalence relation on a set X. Then the equivalence classes $[x]_\sim$ for $x \in X$ partition X.

Equivalence Relations and Partitions

By Theorem 8.9, an equivalence relation on a set X gives a partition of X. Conversely, given a partition of X we can define the corresponding equivalence relation by defining

$$x \sim y \iff x \text{ and } y \text{ are in the same subset in the partition.}$$

Hence there is a bijective correspondence between equivalence relations on a set X and partitions of X.

Example 8.10

An alternative way to define the equivalence relation $\sim$ in Example 8.6 would be to start with the partition of $\mathbb{C}$, and define $z \sim w$ if and only if z and w are in the same subset in this partition. Equivalently,

$$z \sim w \iff \begin{array}{l}\text{either } z = w = 0 \text{ or } z \text{ and } w \text{ are on the same circle} \\ \text{centred on } 0.\end{array}$$

Sheet 8 Question 6

6. For each of the relations $\sim$ below on a set X, decide whether it is (1) reflexive, (2) symmetric, (3) transitive. [**Note that each relation could have several of these properties!**] Give brief explanations or counterexamples as appropriate.

(a) X is the set of people taking MT181, $x \sim y$ if x and y were either both present or both absent at the MT181 lecture on Thursday 22nd November.

(b) X is the set of people taking MT181, $x \sim y$ if x and y were both present at the same MT181 lecture in the week this sheet was issued.

(c) X is the set of people in a lecture room, $x \sim y$ if x can see the eyes of y.

How to Show that a Function is Injective

It might help to first look at the definition of injective!

Definition 7.2

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

(i) We say that f is *injective* if for each $y \in Y$ there exists *at most one* $x \in X$ such that $f(x) = y$.

(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.

How to Show that a Function is Injective

It might help to first look at the definition of injective!

Definition 7.2

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

(i) We say that f is *injective* if for each $y \in Y$ there exists *at most one* $x \in X$ such that $f(x) = y$.

(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.

So $f(x)$ is injective if and only if there do not exist $x, x' \in X$ such that $x \neq x'$ and $f(x) = f(x')$.

How to Show that a Function is Injective

It might help to first look at the definition of injective!

Definition 7.2

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

(i) We say that f is *injective* if for each $y \in Y$ there exists *at most one* $x \in X$ such that $f(x) = y$.

(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.

So $f(x)$ is injective if and only if there do not exist $x, x' \in X$ such that $x \neq x'$ and $f(x) = f(x')$.

Almost always the most elegant way to show that f is injective is to suppose that $f(x) = f(x')$ and use the definition of f to show that $x = x'$.

Example of Contrapositive

Example A. The strategy for showing that a function is injective recommended in lectures uses the contrapositive. We agreed that $f : X \to Y$ is injective if and only if

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

This is equivalent, by taking the contrapositive, to

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

(Compare Claim 5.6: taking the contrapositive often helps when you are trying to prove a statement with one or more negatives.)

Example of Contrapositive

Example A. The strategy for showing that a function is injective recommended in lectures uses the contrapositive. We agreed that $f : X \to Y$ is injective if and only if

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

This is equivalent, by taking the contrapositive, to

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

(Compare Claim 5.6: taking the contrapositive often helps when you are trying to prove a statement with one or more negatives.)

Example B. The Prime Minister is on record as saying that he would implement the recommendations of the Leveson Report, 'as long as they are not bonkers'

Example of Contrapositive

Example A. The strategy for showing that a function is injective recommended in lectures uses the contrapositive. We agreed that $f : X \to Y$ is injective if and only if

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

This is equivalent, by taking the contrapositive, to

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

(Compare Claim 5.6: taking the contrapositive often helps when you are trying to prove a statement with one or more negatives.)

Example B. The Prime Minister is on record as saying that he would implement the recommendations of the Leveson Report, 'as long as they are not bonkers'

$$\text{REPORT NOT BONKERS} \implies \text{WILL IMPLEMENT}.$$

Example of Contrapositive

Example A. The strategy for showing that a function is injective recommended in lectures uses the contrapositive. We agreed that $f : X \to Y$ is injective if and only if

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

This is equivalent, by taking the contrapositive, to

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

(Compare Claim 5.6: taking the contrapositive often helps when you are trying to prove a statement with one or more negatives.)

Example B. The Prime Minister is on record as saying that he would implement the recommendations of the Leveson Report, 'as long as they are not bonkers'

$$\text{REPORT NOT BONKERS} \implies \text{WILL IMPLEMENT}.$$

He has now made it clear that he does not intend to implement the report. What can you conclude?

Example of Contrapositive

Example A. The strategy for showing that a function is injective recommended in lectures uses the contrapositive. We agreed that $f : X \to Y$ is injective if and only if

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

This is equivalent, by taking the contrapositive, to

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

(Compare Claim 5.6: taking the contrapositive often helps when you are trying to prove a statement with one or more negatives.)

Example B. The Prime Minister is on record as saying that he would implement the recommendations of the Leveson Report, 'as long as they are not bonkers'

$$\text{REPORT NOT BONKERS} \implies \text{WILL IMPLEMENT}.$$

He has now made it clear that he does not intend to implement the report. What can you conclude? (Assume for the next 30 seconds that our elected representatives are completely logical.)

Questionnaires

The batch number is 965003.

The additional questions from the college are:

17. For this course, Library study space met my needs.
18. The course books in the Library met my needs for this course.
19. The online Library resources met my needs for this course.
20. I was satisfied with the Moodle elements of this course.
21. I received feedback on my work within the 4 week norm specified by College.

Please think seriously about your responses and comments: useful feedback works both ways!

Write any further comments on the back of the form. In particular, please answer the old version of Q17: whether you found the speed too fast, too slow, or about right.

Please leave the form on the desk at the front. If you do not want it to pass through my hands (so I may not see your comments for six months) return it directly to the Maths Office, McCrea 243.

Administration

- Please pass your answers to Sheet 9 to the person in your left. The person at the end of each row should put all work in the box and pass it down to the next row.
- Problem Sheet 10 will be issued tomorrow. Answers to Sheet 9 will be put on Moodle later today.
- Please take pages 39 and 40 of the printed notes.

Part D: Rings and fields

§9 Introduction to Rings: Integers Modulo n

We begin with a formal definition of the relation introduced in Example 8.7.

Definition 9.1

Let $n \in \mathbb{N}$. Given $a, b \in \mathbb{Z}$, we say that a is *congruent to b modulo n*, and write

$$a \equiv b \bmod n$$

if n divides $b - a$. Let $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$ be the set of equivalence classes under this relation, so

$$[r] = \{r + qn : q \in \mathbb{Z}\}.$$

If $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$ then

$$a \equiv b \bmod n \iff [a] = [b].$$

Examples of Congruences

Since the distinct equivalence classes in $\mathbb{Z}_n$ are $[0], [1], \ldots, [n-1]$, any integer is congruent to one of $0, 1, \ldots, n-1 \bmod n$.

Exercise 9.2

Recall that a square number is a number of the form n^2 where $n \in \mathbb{N}_0$.

(i) Calculate $0, 1, 4, 9, 16, 25, 36, \ldots$ modulo 4. State and prove a conjecture on the pattern you observe.

(ii) Is 2015 the sum of two square numbers?

Exercise 9.3

Find the following:

(i) $27 \times 33 \bmod 10$;

(ii) $7 \times 33 \bmod 10$;

(iii) $27 \times 3 \bmod 10$;

(iv) $7 \times 3 \bmod 10$.

Addition and Multiplication in $\mathbb{Z}_n$

Lemma 9.4

Let $n \in \mathbb{N}$ and let $r, r', s, s' \in \mathbb{Z}$. If $r \equiv r' \bmod n$ and $s \equiv s' \bmod n$ then $r + s \equiv r' + s' \bmod n$ and $rs \equiv r's' \bmod n$.

Definition 9.5

Let $n \in \mathbb{N}$. Given $[r], [s] \in \mathbb{Z}_n$ we define

$$[r] + [s] = [r + s]$$

and

$$[r][s] = [rs].$$

Lemma 9.6

The definitions of addition and multiplication in Definition 9.5 are well-defined.

Example 9.7

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 [2] 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]

Exercise 9.2 Revisited

Exercise 9.2

Recall that a square number is a number of the form n^2 where $n \in \mathbb{N}_0$.

(i) Calculate $0, 1, 4, 9, 16, 25, 36, \ldots$ modulo 4. State and prove a conjecture on the pattern you observe.

(ii) Is 2015 the sum of two square numbers?

Working in $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$ we can give an alternative solution. Let $r \in \mathbb{N}_0$. Then

- $[r] = [0] \implies [r]^2 = [0]^2 = [0]$
- $[r] = [1] \implies [r]^2 = [1]^2 = [1]$
- $[r] = [2] \implies [r]^2 = [2]^2 = [4] = [0]$
- $[r] = [3] \implies [r]^2 = [3]^2 = [9] = [1]$

Administration

- If your surname begins with
  - A–F your work is in the red folder
  - G–M your work is in the blue folder
  - N–S your work is in the green folder
  - T–Z your work is in the yellow folder
- **Please** remember to put your full name and/or student number on your work.
- There are model answers on Moodle for Sheet 9.
- Answers to Sheet 10 and to the sheet of revision questions on Part C of the course will be put on Moodle on Monday 17 December.
- Office hours: Tuesday 11am, Wednesday 11am, Thursday 2pm (no office hour on Friday).

Definition 9.8

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. We say that R is a *ring* if the following properties hold:

(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 $x, y, z \in R$.

Rings and Fields

Claim 9.9

The number systems $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ and $\mathbb{Z}_n$ for $n \in \mathbb{N}$ are rings.

Definition 9.10

A ring R is *commutative* if $xy = yx$ for all $x, y \in R$. 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 $y = x^{-1}$.

For example, $\mathbb{Z}_5$ is a field. The inverses of the non-zero elements can be found from the multiplication table in Example 9.7. They are

$$[1]^{-1} = [1], \quad [2]^{-1} = [3], \quad [3]^{-1} = [2], \quad [4]^{-1} = [4].$$

Theorem 9.11

If p is prime then $\mathbb{Z}_p$ is a field.

More Examples of Fields

Some further examples of fields are $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$. Example 1.14 gives a more unusual example of a field.

Example 9.12

Let K be the subset of $\mathbb{R}$ defined by

$$K = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}.$$

Then K is a ring. Properties (1), (4), (6) and (7) in Definition 9.8 hold because K is closed under addition and multiplication and these properties are known to hold for $\mathbb{R}$. Properties (2) and (5) hold because $0, 1 \in K$. Property (3) holds because if $a + b\sqrt{2} \in K$ then $-a - b\sqrt{2} \in K$. Finally the inverse of the non-zero element $a + b\sqrt{2} \in K$ is

$$(a + b\sqrt{2})^{-1} = \frac{a - b\sqrt{2}}{a^2 - 2b^2}.$$

So K is a field.

General Properties of Rings

Claim 9.13

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).*

Let 0 be the unique zero element in R and let 1 be the unique one element.

(iii) *For each $x \in R$ there exists a unique $y \in R$ such that* $y + x = x + y = 0$.

(iv) *We have $0x = 0 = x0$ for all $x \in R$.*

(v) *We have $-x = (-1)x = x(-1)$ for all $x \in R$.*

(vi) *For each $x \in X$, $-(-x) = x$.*

(vii) *For all x, $y \in R$ we have $-(xy) = (-x)y = y(-x)$ and* $(-x)(-y) = xy$.

(viii) $0 = 1$ *if and only if* $R = \{0\}$.

Administration

- Please take the final installment of the lecture notes.
- Please also take and complete a questionnaire about the course.
- Please collect previous homework! (The box outside my office is almost full.)

ISBNs: An Application of Congruences

All recent books have an International Standard Book Number (ISBN) assigned by the publisher. In the system used before 2007, each book is given a sequence of length 10 with entries from $\{1, 2, 3, 4, 5, 6, 7, 8, 9, \mathrm{X}\}$. For example *A Concise Introduction to Pure Mathematics* has ISBN

1-4398-3598-5

- 1 identifies the country of publication;
- 4398 identifies the publisher (Productivity Press, an imprint of CRC Press);
- 3598 is the item number assigned by the publisher
- 5 is the *check digit*.

The check digit is chosen 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

$$\sum_{j=1}^{10} (11 - j) u_j = 10u_1 + 9u_2 + \cdots + 2u_9 + u_{10} \equiv 0 \bmod 11.$$

If a single digit is miscopied, this will be revealed by the check digit.

It might be necessary to take 10 as a check digit. In this case the letter X is used to stand for 10.

§10 Polynomial rings

We will define polynomials rings over arbitrary fields. The main examples of fields to bear in mind are $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ and $\mathbb{Z}_p$ for a prime p.

Definition 10.1

Let F be a field. Let $F[x]$ denote the set of all polynomials

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d$$

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 we say that $f(x)$ is a *constant polynomial*. If $a_d \neq 0$ then we say that a_d is the *leading coefficient* of $f(x)$.

- If $a_i = 1$ we write x^i rather than $1x^i$.
- If $a_i = 0$ we omit the term x^i rather than writing $0x^i$.

For example, in $\mathbb{Q}[x]$, we write $x^2 + 1$ rather than $1x^2 + 0x + 1$.

Polynomial rings

Polynomials are added and multiplied in the natural way.

Example 10.2

In $\mathbb{Z}_3[x]$, we have

$$\begin{aligned}(x^4 + [2]x^3 + [1]) + ([2]x^4 + x^2 + [1]) \\ &= ([1] + [2])x^4 + [2]x^3 + x^2 + ([1] + [1]) \\ &= [2]x^3 + x^2 + [2]\end{aligned}$$

and

$$(x + [1])(x + [2]) = x^2 + ([1] + [2])x + [1][2] = x^2 + [2].$$

Theorem 10.3

Let F be a field. Then $F[x]$ is a ring with zero the constant polynomial 0 and one the constant polynomial 1.

Polynomial Division

Definition 10.4

If $f(x) = a_0 + a_1x + a_2 + \cdots + a_dx^d$ where $a_d \neq 0$, then we say that d is the *degree* of the polynomial $f(x)$, and write $\deg f = d$.

Theorem 10.5 (Division Algorithm)

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 $\deg r(x) < \deg f(x)$.

We say that $q(x)$ is the *quotient* and $r(x)$ is the *remainder* when $g(x)$ is divided by $f(x)$.

Example 10.6

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.

Example 10.7

Working in $\mathbb{Z}_3[x]$, let $g(x) = x^3 + x^2 + [2]$ and let $f(x) = x^2 + [2]x + [1]$. Then

$$g(x) = (x + [2])f(x) + x$$

so the quotient when $g(x)$ is divided by $f(x)$ is $x + [2]$ and the remainder is x.

Administration

- Spare copies of the final installment of the lecture notes.
- Please also take and complete a questionnaire about the course.
- Please collect previous homework! (The box outside my office is almost full.)

Factor Theorem

Theorem 10.8

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 $r = 0$.

This theorem is very useful when solving polynomial equations.

Example 10.9

Let $f(x) = x^3 - 3x^2 + 7x - 5 \in \mathbb{C}[x]$. The sum of the coefficients is $1 - 3 + 7 - 5 = 0$ so $f(1) = 0$. Dividing $f(x)$ by $x - 1$ gives

$$f(x) = (x - 1)(x^2 - 2x + 5).$$

Hence the roots of $f(x)$ are 1, $1 + 2i$ and $1 - 2i$.

We end with a corollary of Theorem 10.8 that gives a stronger version of the Fundamental Theorem of Algebra (Theorem 2.9).

Corollary 10.10

Let F be a field and let $f(x) \in \mathbb{C}[x]$ be a polynomial of degree n. Then f has at most n roots in F. Moreover if $F = \mathbb{C}$ then f has exactly n roots in $\mathbb{C}$.

We end with a corollary of Theorem 10.8 that gives a stronger version of the Fundamental Theorem of Algebra (Theorem 2.9).

Corollary 10.10

Let F be a field and let $f(x) \in \mathbb{C}[x]$ be a polynomial of degree n. Then f has at most n roots in F. Moreover if $F = \mathbb{C}$ then f has exactly n roots in $\mathbb{C}$.

Theorem 2.9 (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 $\mathbb{C}$.

Questionnaires

You must return a quesionnaire. Unless 15 more are returned, the response rate will be less than the 75% required by the college.

The batch number is 965003.

The additional questions are:

17. For this course, Library study space met my needs.
18. The course books in the Library met my needs for this course.
19. The online Library resources met my needs for this course.
20. I was satisfied with the Moodle elements of this course.
21. I received feedback on my work within the 4 week norm specified by College.

Please write any further comments on the back of the form. (In particular, please answer the old version of Q17: whether you found the speed too fast, too slow, or about right.)

Questionnaires

You must return a quesionnaire. Unless 15 more are returned, the response rate will be less than the 75% required by the college.

The batch number is 965003.

The additional questions are:

17. For this course, Library study space met my needs.
18. The course books in the Library met my needs for this course.
19. The online Library resources met my needs for this course.
20. I was satisfied with the Moodle elements of this course.
21. I received feedback on my work within the 4 week norm specified by College.

Please write any further comments on the back of the form. (In particular, please answer the old version of Q17: whether you found the speed too fast, too slow, or about right.)

Comments so far: (1) BLT1 is too cold. There is a thermostat at the front. Or close the door at the back. (2) More examples.