MT181 NUMBER SYSTEMS

MARK WILDON

These notes are intended to give the logical structure of the course; proofs and further examples and remarks will be given in lectures. Further installments will be issued as they are ready. All handouts and problem sheets will be put on Moodle.

These notes are based on earlier notes by Prof. Ruediger Schack. I would very much appreciate being told of any corrections or possible improvements to these notes.

You are warmly encouraged to ask questions in lectures, and to talk to me after lectures and in my office hours. I am also happy to answer questions about the lectures or problem sheets by email. My email address is `mark.wildon@rhul.ac.uk`.

Lectures in BLT1: Monday 9am, Thursday 9am and Friday 9am.

Office hours in McCrea 240: Tuesday 11am, Wednesday 2pm and Friday 3pm.

Date: First term 2012/13.

Number systems

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.

Outline.

(A) Complex numbers: Complex numbers and calculations with them. Argand diagram. Polar form. Complex exponential function and $e^{i\theta} = \cos\theta + i\sin\theta$. Roots and quadratic equations.

(B) The integers and induction: Induction and Σ notation. Division algorithm: $n = qa + r$. Euclidean algorithm and greatest common divisors. Prime factorization and the Fundamental Theorem of Arithmetic. Binary and other bases.

(C) Propositions, sets and relations: Propositions and truth tables. Sets: union, intersection, complement, product. Venn diagrams. de Morgan's laws. Injective, surjective and bijective maps. Compositions. Inverses. Relations and equivalence relations.

(D) Groups, rings and fields: Modular arithmetic and $\mathbb{Z}_n$. The field $\mathbb{Z}_p$ for a prime p. The ring $F[x]$ of polynomials over a field F. Analogy with $\mathbb{Z}$: division algorithm, remainder theorem, greatest common divisors. The ring of 2×2-matrices over a field.

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.

As part of problem sheets you will be asked to do some reading from *How to think like a mathematician.* The library has copies of this book on short-term loan.

Problem sheets. There will be 8 marked problem sheets; the first will be due in on Thursday 11th October. To encourage you to work hard throughout the term, each problem sheet is worth 1.25% of your overall grade. Note that this mark is awarded for *any reasonable attempt* at the sheet. (There is a link on Moodle to the document explaining this policy in more detail.)

Exercises in these notes. Exercises set in these notes are mostly simple tests that you are following the material. (Any harder exercises will be clearly indicated.) Some will be used for quizzes in lectures. Doing the others will help you to review your notes.

Optional questions. The 'Bonus question' at the end of each problem sheet, and any other optional questions, are for interest and to give you practice in problem solving. You should not worry if you find them difficult.

If you can do the compulsory questions on problem sheets, know the definitions and main results from lectures, and can prove the theorems whose proofs are marked as examinable, then you should do very well in the examination.

Part A

1. Introduction: sets and numbers

Sets. The course begins with its least respectable definition.[1]

Definition 1.1. A *set* is any collection of objects. These objects are called the *elements* of the set.

The italics indicate that it is the technical terms 'set' and 'elements' that are being defined above.

One way to specify a set is to put a list of its elements inside a pair of curly braces. For example $\{1, 4, 9, 16, 25\}$ is a set. Alternatively we may describe a set in words. For example,

the set of square numbers that are less than or equal to 25

is another way to specify $\{1, 4, 9, 16, 25\}$.

If X is a set and x is an element of X then we write $x \in X$. When speaking this is usually read as 'x is in X'. If y is not an element of X then we write $y \notin X$. For example, $9 \in \{1, 4, 9, 16, 25\}$ and $8 \notin \{1, 4, 9, 16, 25\}$.

We will look at sets in more detail in Part C of the course.

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.

The natural numbers. 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 $m + n \in \mathbb{N}$ and $mn \in \mathbb{N}$. Because of this we say that $\mathbb{N}$ is closed under addition and multiplication.

More generally, we make the following definition.

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 $y \neq 0$.

[1] If most mathematicians were put in charge of building a skyscraper, they would put the foundations in last.

Exercise 1.4. Is the set $\mathbb{N}$ of natural numbers closed under (i) multiplication; (ii) subtraction; (iii) division?

INTEGERS, RATIONAL NUMBERS AND REAL NUMBERS. 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 $q \neq 0$.

For example, $0 \in \mathbb{Q}$, $1/2 \in \mathbb{Q}$, $-3 \in \mathbb{Q}$. In Part B we will show that $\sqrt{2} \notin \mathbb{Q}$. In words: $\sqrt{2}$ is *irrational*.

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. If $x \in \mathbb{R}$ then $x^2 \geq 0$. So the equation $x^2 = -1$ has no solutions in $\mathbb{R}$. To solve this equation we must pass to the larger set of complex numbers.

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*. We write $\mathbb{C}$ for the set of complex numbers.

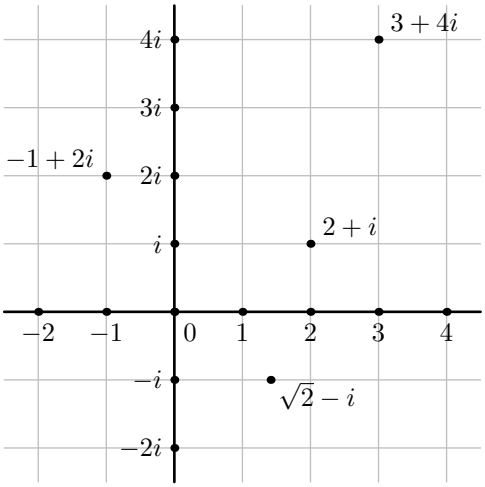
For example, $3 - 2i$ and $1 + i\sqrt{2}$ are complex numbers. (It is fine to write $a + ib$ instead of $a + bi$.) It is usual to write bi, or ib, instead of $0 + bi$, and a instead of $a + 0i$. So real numbers are just a special sort of complex number.

All the usual rules for adding, subtracting, multiplying and dividing complex numbers follow from the property that $i^2 = -1$. For instance, if $a + bi$ and $c + di$ are complex numbers then

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$
$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i.$$

The analogous formula for subtraction should be clear. For division see Exercise 1.8. Therefore the complex numbers are closed under addition, subtraction, multiplication and division.

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



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

When speaking, it is usual to read $|z|$ as 'mod z', Please do not use this in writing: write '$|z|$' or 'the modulus of z' instead. The plural of modulus is 'moduli'.

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 1.8(i), 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 non-zero 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 $\theta = \arg(z)$.

Suppose that θ is an argument of $z \in \mathbb{C}$. Then, since sin and cos are periodic with period 2π, $\theta + 2n\pi$ is also an argument for any $n \in \mathbb{Z}$. In fact, the set of angles that are arguments of θ is

$$\{\ldots, \theta - 4\pi, \theta - 2\pi, \theta, \theta + 2\pi, \theta + 4\pi, \ldots\}.$$

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 $z = 2(\cos\pi/3 + i\sin\pi/3)$.

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.

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.

2. Properties of complex numbers

Exponential function. 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.*

The e^x in Definition 2.1 is an instance of the the usual real exponential function. Often we will write e^z instead of $\exp z$.

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

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

We immediately prove the most important property of the complex exponential function.[2]

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.[3]

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

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

Exercise 2.4. Use Euler's formula for $e^{i\theta}$ to show that

$$\cos\theta = \frac{1}{2}\big(e^{i\theta} + e^{-i\theta}\big)$$
$$\sin\theta = \frac{1}{2i}\big(e^{i\theta} - e^{-i\theta}\big).$$

---

[2]This property is needed to justify writing $\exp z$ as e^z, since from the e^z form, it certainly seems reasonable to expect that $e^{z+w} = e^z e^w$ will hold. Note that the previous sentence is **not** a proof of Lemma 2.2: for a proof we have to use the definition of $\exp z$, as given Definition 2.1.

[3]According to a survey in 1988 of 68 readers of *The Mathematical Intelligencer*, this is the most beautiful result in mathematics. The close runner-up was Euclid's theorem that there are infinitely many primes.

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 $z^3 = 8i$. *Solution:* the argument of $8i$ is $\pi/2$, so in exponential form we have $8i = 8e^{i\pi/2}$. If $z = re^{i\theta}$ then $z^3 = r^3e^{i3\theta}$. So we need to solve

$$r^3e^{i3\theta} = 8e^{i\pi/2}$$

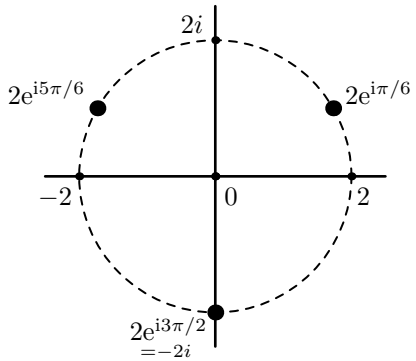
for r and θ. Comparing moduli, we get $r = 2$. Comparing arguments, using the discussion after Definition 1.9, we see that

$$3\theta = \pi/2 + 2n\pi$$

for some $n \in \mathbb{Z}$. Hence $\theta = \pi/6 + 2n\pi/3$. Since $e^{i2n\pi/3} = 1$ if n is a multiple of 3, only three of these solutions are different. Taking $n = 0, 1, 2$ gives the three solutions

$$z = 2e^{i\pi/6}, \quad 2e^{i5\pi/6}, \quad 2e^{i3\pi/2}.$$

shown below on an Argand diagram.



You should draw a diagram whenever you do a problem of this sort. The rotational symmetry in the roots helps to check that your answer is correct, and that no roots have been overlooked.

In general, a non-zero complex number has n distinct n-th roots.

Exercise 2.6.[4] A particle starts at $1 \in \mathbb{C}$ and moves vertically upwards, parallel to the imaginary axis, so that its position at time t is $z(t) = 1 + i2\pi t$. The exponential function is applied to the particle, so that its transformed position at time t is $\exp\big(z(t)\big) = \exp(1 + i2\pi t)$. What shape does the transformed particle trace out?

[4]You should find ten minutes to work on this exercise, even if you have ignored all the others.

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 2.7. *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 2.8. 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.[5]

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 $\mathbb{C}$.

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

[5] A fairly elementary (in the sense of not needing too much background knowledge, not in the sense of being easy) was given by D'Alembert in 1746 and simplified by Argand in 1804. A good account is available online here: `www.cs.amherst.edu/~djv/FTAp.pdf`. There are now many other proofs, using ideas from every branch of pure mathematics.

Part B

3. Induction and Sigma Notation

Propositions. 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 what n is.

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,

P(3): $3^2 + 3 + 41$ 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.[6]

[6]For expression $n^2 + n + 41$ continues to generate prime numbers with an unusually high frequency for larger n. For reasons that are beyond the scope of this course, this is related to the fact that the discriminant of the polynomial $x^2 + x + 41$ is $1^2 - 4 \times 41 = -163$ and $e^{\pi\sqrt{163}} = 262537412640768743.99999999999925\ldots$ is exceptionally close to an integer.

Example 3.4. Some more examples of predicates are

$$P(n) : 1 + 2 + \cdots + n = \frac{n(n+1)}{2};$$
$$Q(x) : x + 1 \geq x;$$
$$T(n) : 4^n \geq 4n.$$

For $Q(x)$ the intended values for x are all real numbers. For the others, the intended values for n are all natural numbers.

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 $n \in \mathbb{N}$.

EXAMPLES. Here are three examples of how to use the Principle of Mathematical Induction to prove results about the natural numbers. Please fill in the gaps in the proof of Claim 3.5.

Claim 3.5. *For all $n \in \mathbb{N}$ we have*

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

Proof. Let $P(n)$ be the predicate

$$P(n) :$$

The proposition $P(1)$ is '$1 = \frac{1(1+1)}{2}$'. Clearly this is .
We now assume that the proposition $P(2)$ is true. So, by assumption

$$1 + 2 + \cdots + n =$$

Adding we get

$$1 + 2 + \cdots + n + 1 =$$

Hence is true. We have shown that $P(1)$ is true, and that $P(n)$ implies $P(n+1)$ for each $n \in \mathbb{N}$. So by the Principle of Mathematical Induction, $P(n)$ is true for all n, as required. □

You may prefer to abbreviate the final two sentences, and write: 'Hence by induction, $P(n)$ is true for all n'. Do not write 'and so on' as a substitute for 'by induction on n'.

Claim 3.6. *For $n \in \mathbb{N}$ let $P(n)$ be the predicate*

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

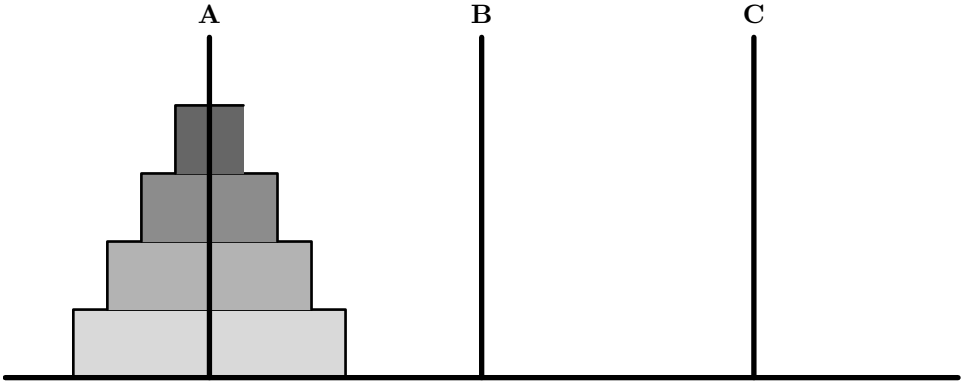
Then $P(n)$ is true for all $n \in \mathbb{N}$.

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 $2^n \geq 4n$.*

Here is a more substantial example of induction.

Problem 3.8 (Towers of Hanoi)**.** You are given a board with three pegs. On peg **A** there are n discs of strictly increasing radius. The starting position for a four disc game is shown below.



A *move* consists of taking a single disc 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 **A** to one of the other pegs. How many moves are required?

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 $a_1, \dots a_n$ are complex numbers then we write their sum as

$$a_1 + \cdots + a_n = \sum_{k=1}^{n} a_k.$$

The right-hand side 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*. At A-level you might have written $\sum_1^n a_k$ for this sum. This can be ambiguous. For example, if $m, n \in \mathbb{N}$ then

$$1^m + 2^m + \cdots + n^m = \sum_{k=1}^{n} k^m.$$

If instead we write $\sum_1^n k^m$ for the sum then it is no longer clear that k should vary while m is fixed.

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

RULES FOR MANIPULATING SIGMA NOTATION.

(1) The summation variable can be renamed: $\sum_{k=0}^{n} 2^k = \sum_{j=0}^{n} 2^j$.
(2) In a product, expressions not involving the summation variable can be taken outside the sum:

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

and

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

(3) Sums can be split up:

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

and terms taken out: $\sum_{k=0}^{n} a_k = a_0 + \sum_{k=1}^{n} a_k$.
(4) The limits can be shifted. For example, if $x \in \mathbb{R}$ then

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

We replaced every k with $r+1$. The original sum has k varying from 1 to n. Hence $r+1$ should also vary from 1 to n, and so r should vary from 0 to $n-1$.

Here is a final example involving both induction and Sigma notation. If you get stuck on Question 2(b) on Sheet 4, try going through this example first.

Example 3.12. We shall show that if $n \in \mathbb{N}$ then $\sum_{k=1}^{n} k^2 = \frac{1}{6}n(n+1)(2n+1)$. Define a predicate $P(n)$ by

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

In the case $n = 1$, the proposition $P(1)$ is

$$\text{`}\textstyle\sum_{k=1}^{1} k^2 = \frac{1}{6}1(1+1)(2\times 1+1)\text{'}.$$

This is true, because the left-hand side is $1^2 = 1$ and the right-hand side is $\frac{1}{6}(1 \times 2 \times 3) = 1$.

Assume that $P(n)$ is true. So, by assumption

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

We want to prove that $P(n+1)$ is true. We obtain $P(n+1)$ by replacing n with $n+1$ in the statement of $P(n)$ above. So the statement we want to prove is

$$\begin{aligned}\sum_{k=1}^{n+1} k^2 &= \tfrac{1}{6}(n+1)(n+2)(2(n+1)+1)\\ &= \tfrac{1}{6}(n+1)(n+2)(2n+3).\end{aligned}$$

Note we have not proved it yet! Splitting off the final summand of $\sum_{k=1}^{n+1} k^2$ we get

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

Now using the inductive assumption and some algebraic manipulation we get

$$\begin{aligned}\sum_{k=1}^{n+1} k^2 &= \tfrac{1}{6}n(n+1)(2n+1) + (n+1)^2\\ &= \tfrac{1}{6}(n+1)\big(n(2n+1) + 6(n+1)\big)\\ &= \tfrac{1}{6}(n+1)\big(2n^2+7n+6\big)\\ &= \tfrac{1}{6}(n+1)\big((n+2)(2n+3)\big).\end{aligned}$$

Hence $P(n+1)$ holds.

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

STRONG INDUCTION. In the inductive steps in the inductive proofs seen so far, we assumed $P(n)$ and used it to prove $P(n+1)$. Sometimes it is 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.

A proof using (ii)′ is said to be a proof by *strong induction*. In this course we take it for granted that strong induction is a valid methods of proof.[7]

4. Division and prime factorization

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

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.

Theorem 4.1 can be proved by strong induction on n, but the proof is not especially illuminating, so it will not be given in lectures. It is much more important that you understand the statement of Theorem 4.1 and can find q and r in specific cases. This is done by dividing n 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 $\frac{1}{3}$.)

[7]It can be proved, using the ordinary Principle of Mathematical Induction that proof by strong induction is valid. So anyone who accepts the Principle of Mathematical Induction should also accept proof by strong induction.

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

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.*

Euclid's Algorithm always finishes because the numbers get smaller at each step. Lemma 4.7 implies that the final output of the algorithm is $\gcd(m, n)$. So Euclid's Algorithm has the two key properties of a good algorithm: it always finishes, and it always finishes with the right answer.

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 $sm + tn = \gcd(m, n)$.

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

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

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.

The first few primes are

$$2, 3, 5, 7, 11, 13, 17, 21, 23, 29, 31, 37, 41, 43, 47, \ldots.$$

By Definition 4.11, 1 is neither prime nor composite.

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.

The existence of prime factorizations can be proved fairly easily using strong induction. The uniqueness is a bit trickier and will not be proved in lectures.[8]

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 ....

The reason why 1 is not defined to be a prime number, even though it is not divisible by any numbers except itself, is because this would destroy unique factorization. For instance, $5 = 5 \times 1 = 1 \times 5 \times 1 = 1 \times 5 \times 1 \times 1 = \ldots$ would all be different prime factorizations of 5.

Unique factorization can be used to show that some numbers are irrational. As an example we will show that $\sqrt{3}$ is irrational. The proof goes through with very minor changes to show that $\sqrt{p}$ is irrational for any prime p.

Claim 4.14. *$\sqrt{3}$ is an irrational number.*

Proof. Suppose, for a contradiction that $\sqrt{3} \in \mathbb{Q}$. Then there exist $m, n \in \mathbb{Z}$ with $n \neq 0$ such that $\sqrt{3} = m/n$. Multiply through by n and square both sides to get

$$3n^2 = m^2.$$

Let $n = 3^b \times N$ and let $m = 3^a \times M$, where N and M are not divisible by 3. Substituting into $3n^2 = m^2$ we get

$$3^{2b+1} \times N = 3^{2a} \times M.$$

The highest power of 3 dividing the left-hand side is 3^{3b+1}, and the highest power of 3 dividing the right-hand side is 3^{2a}. But $2b + 1 \neq 2a$. This contradicts unique factorization. Hence $\sqrt{3}$ is irrational. □

For Quesion 6 on Sheet 4, try cubing instead of squaring!

[8] See the lecturer in an office hour, or Proposition 10.6 and Theorem 11.1 in *A concise introduction to pure mathematics* by Martin Liebeck (CRC Press, 2011).

INFINITELY MANY PRIMES. According to the poll of readers of *The Mathematical Intelligencer* mentioned on page 8, the following theorem is the second most beautiful result in mathematics.

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_1p_2+1, $p_1p_2p_3+1$, $p_1p_2p_3p_4+1$ and $p_1p_2p_3p_4p_5+1$ are all prime, but

$$\begin{aligned} p_1p_2p_3p_4p_5p_6 + 1 &= 2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 \\ &= 300031 \\ &= 59 \times 509. \end{aligned}$$

To show that a number is prime you could use Question 5 on Sheet 4, or the MATHEMATICA command `PrimeQ`. This example shows that the second case in the proof of Euclid's theorem can arise!

TWO THINGS TO THINK ABOUT.

(1) It is quite easy to generate large primes, and easy to multiply them together. Any modern desktop computer can generate primes of about 300 decimal digits almost instantly. But given only the product of two primes, it appears to be a hard problem to find the prime factors.

For example, given only

$$31485923544937$$

and a pocket calculator, you would probably have a hard time finding its prime factors. But on the other hand, given the primes 1282817 and 24544361, you could verify that

$$1282817 \times 24544361 = 31485923544937$$

quite easily.

The algorithms used to make secure connections on the internet, for for internet banking etc., would all be useless if there was a quick way to factorize large composite numbers. To learn more, search for 'Public Key Cryptography' on the web, or wait until your 3rd / 4th year and do one of the cryptography courses here.

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

REMARK 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.

BINARY AND OTHER 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 $144 = 12100_3$.

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

The example above should suggest a general algorithm.

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

Base 2 is known as *binary*. Binary is particularly important because computers store and process data as sequences of the *bi*nary digi*ts* 0, 1, also known as *bits*. For a nice introduction to programming at the level of bits, see `pleasingfungus.com/Manufactoria/`.

Exercise 4.21. Show that $21 = 10101_2$ and write 63, 64 and 65 in binary.

Part C

5. Propositional Logic

Implication. Suppose that A and B are mathematical statements[9] such that if A is true then B is true. Then we say that A *implies* B, and write $A \implies B$.

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 $w^3 = z^3 \implies w = z$?

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 5.2. Question 4(b) on Sheet 3 asked for a proof, using the Principle of Mathematical Induction (see page 12) that $2^n \geq 6n$ for all $n \geq 5$. Here is a slightly tidied-up version of one argument that was submitted.[10]

> 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
>
> $$2^{n+1} \geq 6(n+1)$$
> $$2^{n+1} - 6(n+1) \geq 0$$
> $$2 \times 2^n - 6n - 6 \geq 0$$
> $$2(2^n - 6n) + 6n - 6 \geq 0$$
>
> which is true since $2^n \geq 6n$ and $6n \geq 6$.

Is this argument valid? How could it be clarified?

[9] So A and B could be either propositions or predicates (see page 11). Some non-mathematical statements will be used in quizzes.

[10] Dubious parts of arguments are marked with bars: these are reproduced so you can think about them, not so you can use them as model examples!

It is often tempting to start with the statement we are trying to prove, and manipulate it until it becomes obviously true. **But this is only valid if every step is reversible**. The following example should make this point.

Example 5.3. Suppose we want to find all $x \in \mathbb{R}$ such that

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

It might be tempting to write something like this:

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

hence $x = -2$ or $x = 1$. But something is definitely wrong: if we substitute $x = -2$ into the original equation, we get $\sqrt{-2+3} = -2+1$, which is false!

Your arguments will be clearer if you use $\implies$ and $\iff$ 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:

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

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.)

Exercise 5.4. Please assume that the following statements are true.

- 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?

- 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 from the sky 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.

'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 $x + y \notin \mathbb{Q}$.*

For example, Claim 5.6 implies that $n + \sqrt{2}$ is not a rational number for any $n \in \mathbb{Z}$.

'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 $(\forall x \in X)\, \neg P(x)$.

Once you have understood the meaning of the $\forall$ and $\exists$ symbols, these rules should seem fairly obvious to you. Negating long compound statements becomes routine if you apply these rules step-by-step.

Exercise 5.7. Sometimes the set X in $\forall x \in X$ is indicated by inequalities. For example,

$(\forall \varepsilon > 0)\, Q(\varepsilon)$ means that $Q(\varepsilon)$ 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

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

Those doing MT194 Numbers and Functions will notice that a logically equivalent statement is 'the sequence (a_n) converges'. Using the two rules above, everyone should be able to get the correct negation.

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

Exercise 5.8. Fill in the $\Longrightarrow$ column of the following truth table. (Unless you are very confident, use pencil.)

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 $\neg B \Longrightarrow \neg A$?

Exercise 5.9. By definition, $A \Longleftrightarrow B$ is true if and only if $A \Longrightarrow B$ and $B \Longrightarrow A$ both hold. So $A \Longleftrightarrow B$ is logically equivalent to

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

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

For Question 2(c) on Sheet 6 you will need a truth table with eight rows, corresponding to the eight possibilities for the truth or falsity of the statements A, B and C.

The final example below may give you a hint for Question 6 on Sheet 6.

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. The truth table of exclusive or is shown below. [**Corrected 16th November.**]

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

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

As an *exercise* you should find a different, but logically equivalent, way to express A xor B.

Propositional and predicate logic is a much deeper subject than this introduction might suggest. It underpins Gödel's famous incompleteness theorem on the limits of formal mathematical proofs and Turing's equally important work on the relationship between mathematical truth and computability.

There are many good books on these subjects written for the non-expert. For example, *Gödel's Proof* by Ernest Nagel and James Newman, NYU Press (2001).

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) $\{m \in \mathbb{Z} : 2 \mid n\}$ 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'.

A good way to show that two sets X and Y are equal is to show that $X \subseteq Y$ and $Y \subseteq X$. If this holds then X and Y have the same elements, so are equal.

Exercise 6.3. Decide whether each of the following statements are 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) $|\{z \in \mathbb{C} : z^3 = 1\}| = 3$.

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. 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

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

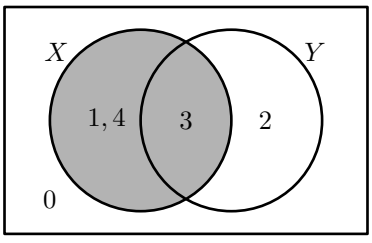
Claim 6.5 (De Morgan's Laws)**.** *Let X and Y be subsets of a universe set U. Then*

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

The proof of (ii) is left to you: see Question 4(a) on Sheet 7.

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.

Venn diagrams are a useful way of picturing the unions and intersections of two or three sets. It is possible to draw a Venn diagram for 4 sets with 16 different regions, but Venn diagrams for 5 sets cannot be drawn in the plane.

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

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

The Principle of Inclusion and Exclusion generalizes these formulae to any number of sets. (Most textbooks on combinatorics in the library will have a proof.)

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 $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$.

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?

BOOLEAN LOGIC (NON-EXAMINABLE). If A and B are mathematical statements then you showed in Question 2(b) of Sheet 6

that $\neg(A \vee B)$ and $\neg A \wedge \neg B$ are logically equivalent. This might remind you of the first De Morgan's Law in Claim 6.5(i), that

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

In fact, any pair of logically equivalent propositions corresponds to an identity in set theory: replace $\wedge$ with $\cap$, replace $\vee$ with $\cup$, replace $\neg$ with complement, and interpret the letters A, B, etc. as sets to get the two sides of the identity.[11]

Exercise 6.8 (Optional)**.** By Question 2(c) on Sheet 6, the propositions $(A \vee B) \wedge C$ and $(A \wedge C) \vee (B \wedge C)$ are logically equivalent. What is the corresponding identity in set theory?

Yet another equivalent setting is digital electronics: NOT gates correspond to negation $\neg$ (or complement), AND gates to conjunction $\wedge$ (or intersection $\cap$) [**sorry, there was a nasty typo here, where I switched from AND / conjunction / $\wedge$ / $\cap$ to OR / disjunction / $\vee$ / $\cup$ in mid-sentence**.] Try searching the web for 'Boolean algebra' to learn more about these ideas.

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 $g(x) = x^2$. Then g is a function with domain $\mathbb{R}$ and codomain $\mathbb{R}$.

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

[11] To see why this correspondence should work, let U be a universe set and suppose that $A(x)$ and $B(x)$ are predicates defined for $x \in U$. Define $X = \{x \in U : A(x)\}$ and $Y = \{x \in U : B(x)\}$. Then

$$X \cap Y = \{x \in U : A(x) \wedge B(x)\}$$
$$X' = \{x \in U : \neg A(x)\}$$

and so on. So $\cap$ corresponds to $\wedge$, and set complement correspond to negation of propositions.

Note that g and h are different functions, according to the definition at the start of this section, because they have different domains (and different codomains).

If $f : X \to Y$ is a function then $f(x)$ must be defined for each $x \in X$. There is no requirement that there is some 'uniform rule' giving the values of $f(x)$. For example, in Example 7.1(b) the values $f(x)$ were specified one-by-one for each $x \in X$.

Functions are also called *mappings*.

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(b) 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.

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.

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.)

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 $g(y) = \log y$.

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.[12]

The proof of (i) in the following theorem is left to you on Question 5(a) of Sheet 8. You should be able to do it in a fairly similar way to (ii).

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.*

[12]There is a nasty notational clash with the trigonometric functions, where $\sin^2 x$ means $(\sin x)^2$ rather than $\sin(\sin x)$. This is a historical accident. Fortunately it is rarely useful to compose trigonometric functions.

By Theorem 7.9(iii), if $f : X \to Y$ and $g : Y \to Z$ are both bijective then $gf : X \to Z$ is bijective, and so has an inverse function. To undo gf we need to first undo g then undo f, so

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

For an application of this result, see Question 8 on Sheet 8.

If X is a set then the function $i_X : X \to X$ such that $i_X(x) = x$ for all $x \in X$ is called the *identity function on* X. For example, if $f : X \to Y$ is bijective then $f^{-1}f = i_X$ and $ff^{-1} = i_Y$.

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 $fh = i_Y$.*

For some other results on compositions of functions see Question 5 on Sheet 8.

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

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

Usually it is clearer to specify relations more informally, as in this example.

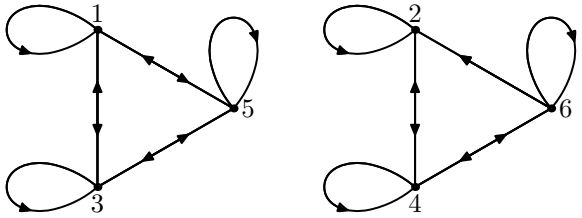
In Example 8.1(iii) the subset relation was shown with the usual symbol $\subseteq$. Other symbols that are commonly used to denote relations are $\equiv$, read 'is equivalent to', and $\sim$, read 'is related to' or 'twiddles'.

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.



Exercise 8.3. Let $X = \{1, 2, 3, 4, 5, 6\}$ as in Example 8.2. Draw a diagram for the relation on X defined by

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

PROPERTIES OF RELATIONS.

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 $x, y \in X$,

$$x \sim y \implies y \sim x;$$

(iii) *transitive* if for all $x, y, z \in X$,

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

A relation that is reflexive, symmetric and transitive is said to be an *equivalence relation*.

The following exercise will be used as part of a quiz in lectures.

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.

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 $[0]_\sim = \{0\}$.

The next example will be important in Part D of the course.

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 $a - b$. Then $\equiv$ is an equivalence relation. The different equivalence class are

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

Observe that $[r]$ is the set of integers that leave a remainder r on division by n.

Examples 8.2, 8.5(c), 8.6 and 8.7 illustrate an important general result on equivalence relations. To state it we need the following definition.

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.*

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,

$$z \sim w \iff \begin{array}{l}\text{either } z = w = 0 \text{ or } z \text{ and } w \text{ are on the same} \\ \text{circle centred on } 0.\end{array}$$

Part D

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

$$a \equiv b \bmod n \iff [a] = [b].$$

Working with integers, as on the left-hand side, is usually easiest for calculations. For more theoretical results it is better to work with the equivalence classes in $\mathbb{Z}_n$, as on the right-hand side.[13]

Since the distinct equivalence classes in $\mathbb{Z}_n$ are $[0], [1], \ldots, [n-1]$, any integer is congruent to one of 0, 1, …, $n-1$ mod 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) $7 \times 3 \bmod 10$.

The next lemma states the result that was hopefully suggested by Exercise 9.3.

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 $rs \equiv r's' \bmod n$.*

[13] You might see other notations for $\mathbb{Z}_n$ such as $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}/n$ in textbooks or online.

We now use modular arithmetic to define addition and multiplication on $\mathbb{Z}_n$.

Definition 9.5. Let $n \in \mathbb{N}$. Given $[r], [s] \in \mathbb{Z}_n$ we define

$$[r] + [s] = [r + s]$$

and

$$[r][s] = [rs].$$

There is one subtle point that has to be checked about this definition. We have defined addition and multiplication on equivalence classes by choosing particular representatives r and s within each class. We must check that these operations are *well-defined*, that is, they do not depend on the choice of representatives.

For example, take $n = 5$. According to Definition 9.5 we have $[1] + [2] = [3]$. But $[1] = [6]$, so we should also have

$$[1] + [2] = [6] + [2] = [8].$$

Since $[3] = [8]$ these answers are consistent. The next lemma shows that is the case in general.

Lemma 9.6. *The definitions of addition and multiplication in Definition 9.5 are well-defined.*

We can record the addition and multiplication operations on $\mathbb{Z}_n$ by tables as in the next example.

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]

The addition and multiplication operations on $\mathbb{Z}_n$ have all the properties you would expect. Formally this is expressed by saying that $\mathbb{Z}_n$ is a ring, as defined in the next definition.

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 $x, y, z \in R$.

Claim 9.9. *The number systems $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ and $\mathbb{Z}_n$ for $n \in \mathbb{N}$ are rings.*

For $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{C}$ the properties in Definition 9.8 (if not their official names) should be familiar to you. Some of them will be checked for $\mathbb{Z}_n$ in lectures.

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.*

Note that the proof of this theorem gives an effective way to find the inverse of a non-zero element $[x] \in \mathbb{Z}_p$: use Euclid's Algorithm to find $r, s \in \mathbb{Z}$ such that

$$rx + sp = 1;$$

then $[x]^{-1} = [r]$.

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.

Here are some properties that hold for all rings. Some of the proofs are left to you on Question 8 of Problem Sheet 10.

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 $R = \{0\}$.*

In (v) and (vi) you should bear in mind that $-x$ means the element of R given by Property (3) satisfying $-x + x = 0$. So it is a non-trivial result that $-x = (-1)x$.

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 $f(x)$.

When writing polynomials we usually omit coefficients of 1, and do not include powers of x whose coefficient is 0. For example, in $\mathbb{Q}[x]$, we write $x^2 + 1$ rather than $1x^2 + 0x + 1$.

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

$$(x + [1])(x + [2]) = x^2 + ([1] + [2])x + [1][2] = x^2 + [2].$$

It is routine to verify that each of the properties in Definition 9.8 holds for $F[x]$. We will assume this result in this course.

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.*

There is a remarkable analogy between the ring of integers $\mathbb{Z}$ and polynomial rings. For example, polynomials can be divided with remainder in a similar way to integers (see Theorem 4.1).

Definition 10.4. If $f(x) = a_0 + a_1 x + a_2 + \cdots + a_d x^d$ where $a_d \neq 0$, then we say that d is the *degree* of the polynomial $f(x)$, and write $\deg f = d$.

We leave the degree of zero polynomial $f(x) = 0$ undefined.

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.

There is a MATHEMATICA notebook on Moodle you can use to check calculations with polynomials.

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.

The next theorem is sometimes called the Remainder Theorem, or 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 $\mathbb{C}$.*

11. Integral Domains and Matrix Rings

This final section is non-examinable and is included for interest only. Let R be a ring. If $a, b, c, d \in R$ then we say that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is a 2×2-*matrix* over R. The set of all such matrices forms a ring, with addition and multiplication defined by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix}.$$

and

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix}$$

The zero element is $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ and the one element is $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. The reason why matrices are multiplied in this way will be seen in MT182 Matrix Algebra.

One interesting property of the ring of 2×2-matrices is that, unlike all the rings seen so far, multiplication is not commutative.

Exercise 11.1. Compute the matrix products

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

and deduce that multiplication of matrices is not commutative.

An important property of the integers $\mathbb{Z}$ is that the product of two non-zero integers is always non-zero.

Definition 11.2. Let R be a ring and suppose that $x, y \in R$. If $xy = 0$ implies that either $x = 0$ or $y = 0$ then we say that R is an *integral domain*.

Thus $\mathbb{Z}$ is an integral domain. However, the ring of 2×2-matrices is not an integral domain. For example, the second product in Example 11.1 is the zero matrix. By Question 4(a) on Sheet 10, $\mathbb{Z}_n$ is not an integral domain if n is composite.

Theorem 11.3. *If F is a field then F is an integral domain*

Proof. Suppose that $x, y \in F$ are such that $xy = 0$. If $x \neq 0$ then x has an inverse, $x^{-1} \in F$. Multiplying by x^{-1} we get

$$0 = x^{-1}0 = x^{-1}(xy) = (x^{-1}x)y = 1y = y$$

using Claim 3.13(iv) and the ring properties in Definition 9.8. Hence if $x \neq 0$ then $y = 0$, and so either $x = 0$ or $y = 0$. □