WMS

MA132

Foundations Revision Guide

Written by David McCormick
Amended by Matthew Lee

Contents

Introduction

This revision guide for MA132 Foundations has been designed as an aid to revision, not a substitute for it. Foundations is about introducing you to the style of university mathematics. There aren't as many confusing definitions in this course as there are in MA131A Analysis I, but definitions are important, so learn them. Also, while proofs are important, it's far more important to understand what the theorems say and how you can use them. For more questions, try the book *The Foundations of Mathematics* by Stewart and Tall.

Disclaimer: Use at your own risk. No guarantee is made that this revision guide is accurate or complete, or that it will improve your exam performance.

Authors

Written by D. S. McCormick (d.s.mccormick@warwick.ac.uk).
Updated based upon lecture notes by D. Mond and S. Siksek, at the University of Warwick, 2011.
Any corrections or improvements should be reported by email to comms@warwickmaths.org.

1 Numbers

We first define what we mean by numbers:

Definition 1.1. The set of *natural numbers* is defined as $\mathsf{N} = \{0, 1, 2, 3, \dots\}$, and the set of *integers* is defined as $\mathsf{Z} = \{\dots, -2, -1, 0, 1, 2, 3, \dots\}$.

The fundamental question about numbers we are interested in is that of division with remainder: if $m, n \in \mathsf{N}$ with $n > 0$, then there exist $q, r \in \mathsf{N}$ such that $m = qn + r$ with $0 \leq r < n$. Why does this work? We first define divisibility without remainder: $a \mid b$ if a divides b exactly with no remainder; thus 6 divides 42, as does 7, but 9 does not; we write $6 \mid 42$ but $9 \nmid 42$.

Proposition 1.2. Divisibility is transitive: if $a, b, c \in \mathsf{N}$ and if $a \mid b$ and $b \mid c$, then $a \mid c$.

A prime number is one which is divisible only by itself and 1. (By convention, 1 is *not* a prime number.)

Lemma 1.3. Every natural number greater than 1 is divisible by some prime number.

Throughout foundations you will use the well ordering principle which is stated below.

Theorem 1.4. There are infinitely many prime numbers.

To nail down these properties, we consider a fundamental property of the natural numbers:

Well-Ordering Principle. Every non-empty subset of N has a least element.

The Well-Ordering Principle is at the root of the form of proof known as induction, which we first state as a bland statement on subsets of N:

Principle of Induction. Suppose that $T \subseteq \mathsf{N}$, that $0 \in T$, and that for any $n \in N$, if $n - 1 \in T$ then $n \in T$. Then $T = \mathsf{N}$.

By letting $T = \{n \in \mathsf{N} : \text{property } P(n) \text{ holds}\}$, where $P(n)$ is some proposition relating to n, we get the much more useful form of induction used for proving things:

Principle of Induction. A proposition $P(n)$ relating to a natural number n is valid for all natural numbers n if

1. $P(1)$ is true, i.e. the proposition is valid for $n = 1$; and
2. $P(n) \implies P(n+1)$, i.e. the proposition for n implies the proposition for $n + 1$.

Example 1.5. We prove by induction that for any $n \in \mathsf{N}$, $1^2 + 2^2 + \cdots + n^2 = \frac{1}{6}n(n+1)(2n+1)$.

- First, when $n = 1$, the statement simply reads $1 = \frac{1}{6} \cdot 1 \cdot 2 \cdot 3 = 1$, so it is certainly true in this case.
- Assume that $1^2 + 2^2 + \cdots + k^2 = \frac{1}{6}k(k+1)(2k+1)$ for some specific $k \in \mathsf{N}$. Adding $(k+1)^2$ to both sides we obtain

$$\begin{aligned} 1^2 + 2^2 + \cdots + k^2 + (k+1)^2 &= \tfrac{1}{6}k(k+1)(2k+1) + (k+1)^2 \\ &= \tfrac{1}{6}(k+1)\left[k(2k+1) + 6(k+1)\right] \\ &= \tfrac{1}{6}(k+1)(2k^2 + 7k + 6) \\ &= \tfrac{1}{6}(k+1)(k+2)(2k+3) \\ &= \tfrac{1}{6}(k+1)((k+1)+1)(2(k+1)+1). \end{aligned}$$

  This is simply our required statement with $n = k + 1$. Thus if it holds for $n = k$, it must hold for $n = k + 1$.

Hence by induction, the statement is true for all $n \in \mathsf{N}$.

A slightly different principle of induction is given as follows:

Principle of Induction. Suppose that $T \subseteq \mathsf{N}$, that $0 \in T$, and that for any $n \in N$, if $0, 1, \dots, n-1 \in T$ then $n \in T$. Then $T = \mathsf{N}$.

We can use this principle of induction to prove:

Theorem 1.6 (The Fundamental Theorem of Arithmetic)**.**

1. Every natural number greater than 1 can be written as a product of prime numbers.
2. Such a factorisation is unique, except for the order of the terms.

This gives us a very useful corollary:

Corollary 1.7. If p is a prime number with $p \mid mn$, then either $p \mid m$ or $p \mid n$.

Definition 1.8. Let m and n be natural numbers. The *highest common factor* of m and n, denoted $\text{hcf}\{m, n\}$, is the largest number which divides both m and n. The *lowest common multiple* of m and n, denoted $\text{lcm}\{m, n\}$, is the least number divisible by both m and n.

1.1 The Euclidean Algorithm

We say that two numbers are *coprime* if their highest common factor is 1.

However, *finding* the hcf and lcm of two numbers is not always easy. Fortunately, there is an algorithm which allows us to do so. It depends on the following key lemma:

Lemma 1.9. If $m = qn + r$, then $\text{hcf}\{n, m\} = \text{hcf}\{n, r\}$.

Proof. If d divides m and n, then as $m = qn + r$, we must have $d \mid r$; conversely if d divides n and r, we must have that $d \mid m$. □

Example 1.10. Let us find $\text{hcf}\{345, 780\}$:

$$\begin{aligned} 780 &= 2 \times 345 + 90 & \text{hcf}\{780, 345\} &= \text{hcf}\{345, 90\} \\ 345 &= 3 \times 90 + 75 & \text{hcf}\{345, 90\} &= \text{hcf}\{90, 75\} \\ 90 &= 1 \times 75 + 15 & \text{hcf}\{90, 75\} &= \text{hcf}\{75, 15\} \\ 75 &= 5 \times 15 + 0 & \text{hcf}\{75, 15\} &= 15 \end{aligned}$$

2 Integers and Modular Arithmetic

Now bizarrely in the Foundations course you consider subgroups but not groups themselves, even though subgroups are groups in their own right. But we shall not digress, so for now let us forget about groups.

Definition 2.1. A subset of Z is called a *subgroup* if it is nonempty, and the sum and difference of any two of its members is also a member.

From definition it follows that for any subgroup S:

1. $0 \in S$
2. If $a \in S$ then $-a \in S$
3. If $a \in S$ then every multiple of a is in S. That is $a\mathsf{Z} \subseteq S$

Proposition 2.2. Every subgroup of Z is of the form $n\mathsf{Z}$ for some natural number $n \in \mathsf{N}$.

Proposition 2.3. For any two integers m and n, $m \mid n$ if and only if $m\mathsf{Z} \supseteq n\mathsf{Z}$.

Proposition 2.4.

1. If G_1 and G_2 are subgroups of Z then so is
   $G_1 \cap G_2 := \{n \in \mathsf{Z} : n \in G_1\}$ and
   $G_1 + G_2 := \{m + n : m \in G_1, n \in G_2$.
2. $G_1 \cap G_2$ contains every subgroup contained in both G_1 and G_2
   $G_1 + G_2$ is contained in every subgroup containing both G_1 and G_2

In fact, this is what lies behind finding the hcf and lcm:

Theorem 2.5. For $m, n \in \mathsf{Z}$, $m\mathsf{Z}+n\mathsf{Z} = h\mathsf{Z}$ and $m\mathsf{Z}\cap n\mathsf{Z} = \ell\mathsf{Z}$, where $h = \text{hcf}\{m, n\}$ and $\ell = \text{lcm}\{m, n\}$.

Corollary 2.6. For any $m, n \in \mathsf{Z}$, there exist $a, b \in \mathsf{Z}$ such that $am + bn = \text{hcf}\{m, n\}$. In particular, m and n are coprime if and only if there exist $a, b \in \mathsf{Z}$ such that $am + bn = 1$.

Finding these a and b is a matter of running the Euclidean algorithm in reverse, as we demonstrate now:

Example 2.7. Let $m = 780$, $n = 345$. We know that $h = \text{hcf}\{345, 780\} = 15$. We take our stack of equations and read from the bottom up. The last equation says that $h = 15$. We use step 3 to replace 15 by $90 - (1 \times 75)$, to give $h = 90 - (1 \times 75)$. Then we use step 2 to write $75 = 345 - (3 \times 90)$, and replace this to get

$$h = 90 - 345 + (3 \times 90) = (4 \times 90) - 345.$$

Finally we use step 1 to write $90 = 780 - 2 \times 345$, and we get

$$h = 4(780 - 2 \times 345) - 345 = 4 \times 780 - 9 \times 345.$$

So $a = 4$, $b = -9$.

2.1 Modular Arithmetic

Let $n \in \mathsf{N}$. We define binary operations on $\{0, 1, \ldots, n-1\}$ by

$$r +_n s = r + s \mod n \qquad r \times_n s = rs \mod n$$

where $\mod n$ means take the remainder on dividing by n. These binary operations are easily seen to be associative and commutative. $\{0, 1, \ldots, n-1\}$ with the operation $+_n$ is a group under addition, denoted Z/n or $\mathsf{Z}/n\mathsf{Z}$. We call it the *cyclic group of order* n.

Proposition 2.8 (Subgroups of Z/n)**.** If m divides n, then $m\mathsf{Z}/n$ is a subgroup of Z/n, and every subgroup of Z/n is of this form except $\{0\}$.

Corollary 2.9. If p is a prime number then Z/p has no proper subgroups.

The following proposition allows us to carry out useful calculations in Z/n:

Proposition 2.10. If $a_1 = b_1 \mod n$ and $a_2 = b_2 \mod n$, then $a_1+a_2 = b_1+b_2 \mod n$ and $a_1a_2 = b_1b_2 \mod n$.

Example 2.11. As $5 = -2 \mod 7$, we have $5^4 = (-2)^4 \mod 7 = 16 \mod 7 = 2 \mod 7$.

Example 2.12 (Other incarnations)**.** Consider the set of complex n^{th} roots of unity (i.e. of 1), that is

$$G_n = \{1, e^{2\pi i/n}, e^{4\pi i/n}, \ldots, e^{2(n-1)\pi i/n}\}.$$

This is a group under multiplication of complex numbers:

- If $z^n = 1$ and $w^n = 1$, then $(zw)^n = z^n w^n = 1$, so closure holds;
- Associativity follows from associativity of complex multiplication;
- 1 is an n^{th} root of unity, so we have an identity element;
- If $z^n = 1$ then $\left(\frac{1}{z}\right)^n = 1$ as well, so we have inverses.

In fact, there is a bijection $\phi\colon \mathsf{Z}/n \to G_n$ given by $k \mapsto e^{2k\pi i/n}$; moreover, ϕ transforms addition in Z/n into multiplication in G_n; that is,

$$\phi(k +_n l) = e^{2(k+l)\pi i/n} = e^{2k\pi i/n} \cdot e^{2l\pi i/n} = \phi(k) \cdot \phi(l).$$

This is an example of an isomorphism. Let us celebrate by making a definition:

Definition 2.13. Let G and G' be groups, and let $\phi\colon G \to G'$ be a map. Then ϕ is an *isomorphism* if it is a bijection, and for any $g_1, g_2 \in G$, $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$.

Example 2.14. $\exp\colon \mathsf{R} \to \mathsf{R}_{>0}$, $\exp(x) = e^x$ is an isomorphism from $(\mathsf{R}, +)$ to $(\mathsf{R}_{>0}, \times)$, since we have $\exp(x_1 + x_2) = \exp(x_1)\exp(x_2)$.

3 Rational and Real Numbers

3.1 Rational Numbers

Having dealt with natural numbers and integers, we now move to fractions, or *rational numbers*.

Definition 3.1. The set of *rational numbers* Q is defined by $\mathsf{Q} = \{\frac{m}{n} : m, n \in \mathsf{Z}, n \neq 0\}$. We say that $\frac{m_1}{n_1} = \frac{m_2}{n_2}$ if and only if $m_1 n_2 = m_2 n_1$. We define

$$\frac{m_1}{n_1} + \frac{m_2}{n_2} = \frac{m_1 n_2 + m_2 n_1}{n_1 n_2}$$

and

$$\frac{m_1}{n_1} \times \frac{m_2}{n_2} = \frac{m_1 m_2}{n_1 n_2}.$$

By using the properties of highest common factors, we can show that there is a unique expression in lowest terms:

Proposition 3.2. Among all expressions for a given $q \in \mathsf{Q}$, there is a unique expression (up to sign) $\frac{m}{n}$ for which $\mathrm{hcf}\{m, n\} = 1$, i.e. the numerator and denominator are coprime; we call this form the *minimal expression* for q.

Unique up to sign simply means that if $\frac{m}{n}$ is minimal, then so is $\frac{-m}{-n}$, but that's it.

But the rationals can't do everything in mathematics, as the Greeks discovered:

Theorem 3.3. There is no rational number q such that $q^2 = 2$.

Proof. Suppose there is; then let its minimal expression be $\frac{m}{n}$. Then $m^2 = 2n^2$, hence $2 \mid m^2$, therefore $2 \mid m$. Write $m = 2p$ and substitute in to give $4p^2 = 2n^2$, which implies $n^2 = 2p^2$, and hence $2 \mid n^2$, so $2 \mid n$. But then $\mathrm{hcf}\{m, n\} = 2$, contradicting the fact that $\frac{m}{n}$ is the minimal expression. □

3.2 Real Numbers

A real number $x \in \mathsf{R}$ for which $x \notin \mathsf{Q}$ is called *irrational*: the above theorem tells us that $\sqrt{2}$ is irrational. Indeed, $\sqrt{n}$ is irrational for any $n \in \mathsf{N}$ unless n is a perfect square. We can represent real numbers by decimals, in which case:

Theorem 3.4. A real number is rational if and only if its decimal expansion $a_m \ldots a_1.b_1 b_2 \ldots b_k \ldots$ is eventually periodic.

A decimal is eventually periodic if, beyond some point N, there is a number T such that $b_{k+T} = b_k$ for all $k > N$; this is a *recurring decimal*. If all the decimal places beyond some point are 0, we sometimes call the decimal *terminating*.

So we have studied four number systems: N, Z, Q, R. In each case, the jump from one to the next was in order to solve more equations: Z is formed by appending negative numbers, Q by appending fractions, and R by appending all limits of Cauchy sequences of rational numbers. In N, there are no additive inverses; in Z there are additive inverses but no multiplicative inverses; in Q, however, there are additive inverses of every element and multiplicative inverses of every element except 0. For this reason we call Q a *field*; R is also a field, as is C, the complex numbers.

4 Complex Numbers

A complex number is represented by $a+bi$ where a and b are real numbers and i is a symbol that satisfies $i^2 = -1$. Where

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

Definition 4.1. Let α be a complex number and write $\alpha = a+bi$ where a and b are real numbers. We call a the real part of α and b the imaginary part of α. We write $\mathcal{R}(\alpha) = a$ and $\mathcal{I}(\alpha) = b$

4.1 Powers, Conjugates, Reciprocals and Division

Definition 4.2. If α is a complex number and n a positive integer the we define.

$$\alpha^n = \underbrace{\alpha \cdot \alpha \cdot \ldots \cdot \alpha}_{\text{n times}}$$

Definition 4.3. Let $\alpha = a+bi$ be a complex number, where a, b are real number. We define the conjugate of α denoted by $\bar{\alpha}$ to be $\bar{\alpha} = a-bi$.

Theorem 4.4. Suppose α, β are complex numbers. Then

1. The equality $\alpha = \bar{\alpha}$ holds if and only if α is a real number.
2. Conjugation distributes over addition and multiplication: in other words
$$\overline{\alpha+\beta} = \overline{\alpha}+\overline{\beta} \quad \text{and} \quad \overline{\alpha\cdot\beta} = \overline{\alpha}\cdot\overline{\beta}$$
3. If $\alpha = a+bi$ with a, b real numbers then
$$\alpha \cdot \overline{\alpha} = a^2+b^2$$
In particular $\alpha \cdot \overline{\alpha}$ is a non-negative real number, which is 0 if and only if $\alpha = 0$

With regards to the complex plane, conjugation can be seen as reflection in the the real line. It should be clear that the conjugate of any real number is just itself.

Definition 4.5. Let α be a non zero complex number and write $\alpha = a+bi$ where a, b are real and not both 0. Define the reciprocal of α to be

$$\frac{1}{\alpha} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i = \frac{1}{a^2+b^2}\overline{\alpha}$$

4.2 The Absolute Value and Argument of Complex Numbers

Let a be a real number, then we define the *absolute* value of a (or the *modulus* of a) as follows:

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

This definition of the absolute value can not be extended to the complex numbers as the inequalities make no sense. We can also define the absolute value of a complex number geometrically as the distance from 0 to α.

Definition 4.6. Let $\alpha = a+bi$ be a complex number with a, b real. We define the absolute value of α to be

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

Where we mean the positive square root. Notice that this definition of absolute value corresponds with the definition of absolute value of real numbers when α is just a real number.

Theorem 4.7. Let α, β be complex numbers.

1. $\alpha\overline{\alpha} = |\alpha|^2$
2. $|\alpha| = 0$ if and only if $\alpha = 0$
3. $|\alpha\beta| = |\alpha||\beta|$
4. $|\alpha + \beta| \leq |\alpha| + |\beta|$. This is know as the triangle inequality
5. $|\alpha - \beta| \geq |\alpha| - |\beta|$

Definition 4.8. Let $\alpha = a + bi$ be a non-zero complex number, and suppose that α is represented in the complex plane by the point P. Let θ be the angle of the ray $\overrightarrow{OP}$ makes with the real axis (or the positive x-axis). We call θ the argument of α. Note that we can take $0 \leq \theta \leq 2\pi$, or alternatively $-\pi \leq \theta \leq \pi$; each of these choices is sometimes called the Principal Argument of α.

We may represent complex numbers in the Cartesian coordinates (a, b) or by polar coordinates (r, θ)

Lemma 4.9. If $\alpha = a + bi$ is a non-zero complex number r is its absolute value and θ is its argument, then

$$a = r\cos\theta, \quad b = r\sin\theta$$

and

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

Moreover,

$$r = |\alpha| = \sqrt{a^2 + b^2}, \quad b = a\tan\theta$$

Theorem 4.10 (De Moivre's Theorem)**.** Suppose θ is real and n is an integer. Then

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

4.3 The Exponential Form of the Complex Numbers

Definition 4.11. Let θ be a real number. Define $e^{i\theta}$ by

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

Let $\alpha = t + i\theta$ where t and θ are real numbers. Define

$$e^{\alpha} = e^t \cdot e^{i\theta} = e^t(\cos\theta + i\sin\theta)$$

Where e^t has the usual meaning for real t.

Lemma 4.12. Let α be a non-zero complex number. Then

$$\alpha = re^{i\theta}$$

where $r = |\alpha| > 0$ and θ is the argument of α

Lemma 4.13. Suppose $r_1, r_2, r, \theta_1, \theta_2, \theta_3$ are real with $r_1, r_2 > 0$. Then

$$r_1e^{i\theta_1} \cdot r_2e^{i\theta_2} = r_1r_2e^{i(\theta_1+\theta_2)},$$

$$\frac{r_1e^{i\theta_1}}{r_2e^{i\theta_2}} = \frac{r_1}{r_2}e^{i(\theta_1-\theta_2)},$$

and

$$\overline{re^{i\theta}} = re^{-i\theta}$$

Moreover, for n an integer,

$$(re^{i\theta})^n = r^ne^{in\theta}$$

4.4 Roots of Complex Equations

Theorem 4.14 (Quadratic Formula)**.** Suppose a, b, c are complex numbers and $a \neq 0$. Then the (complex) solutions to the Quadratic Equation

$$ax^2 + bx + c = 0$$

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Lemma 4.15. Suppose α and β are non-zero complex numbers with exponential forms

$$\alpha = re^{i\theta}, \quad \beta = se^{i\phi}$$

Suppose that n is a positive integer. Then $\alpha^n = \beta$ is and only if

$$r = s^{\frac{1}{n}}, \quad \theta = \frac{\phi + 2\pi k}{n}$$

for some integer k.

The above gives us a way of expressing the n-th root of a number. If we write $\xi = exp(\frac{2\pi i}{n})$ the we see that the n-th roots of unity are $1, \xi, \xi^2, ..., \xi^{n-1}$

5 Sets

Sets are the one undefined concept in mathematics. When we define something, we have to define it in terms of something we already know, but any attempts to do so with sets becomes rather complicated. The heuristic definition is that a set is a collection of objects. But then, what's a collection? We will be rather naïve and hope that you can cope with the idea of a set as a collection of objects.

A set is determined entirely by its elements – thus two sets are equal if and only if they contain the same elements. If x is a member of a set X, we write $x \in X$; if x is not in X, we write $x \notin X$. If a set consists of elements a, b and c say, we can write the set as $\{a, b, c\}$. Note, however, that the order is immaterial, and that elements cannot appear twice – thus $\{a, b, c\} = \{a, a, c, b\} = \{c, b, a\}$. It must be possible to decide if an object x is an element of a set X; i.e. exactly one of $x \in X$ and $x \notin X$ can hold.

Definition 5.1. The *empty set*[1], is the set of no elements, denoted $?$ (or $\emptyset$). That is, for any x, $x \notin ?$.

Definition 5.2. A *subset* B of a set A is a set B such that every element of B is an element of A, i.e. $b \in B \implies b \in A$. We write $B \subseteq A$.

Note that A is a subset of itself: $A \subseteq A$. If we wish to emphasise that $B \subseteq A$ but that $B \neq A$, we sometimes write $B \subsetneq A$. Note also that, since there is no $b \in ?$ to check, the implication $b \in ? \implies b \in A$ holds vacuously; thus $? \subseteq A$ for any set A.

It follows from the definition that $A = B$ if and only if both $A \subseteq B$ and $B \subseteq A$; we often use this to check if $A = B$.

An *ordered pair* of a and b is defined by (a, b), where $(a, b) = (c, d)$ if and only if $a = c$ and $b = d$. The set of all ordered pairs of elements, one coming from each of A and B, gives us a way of constructing new sets out of A and B:

Definition 5.3. Given two sets A and B, the set of all ordered pairs (a, b) where $a \in A$ and $b \in B$ is called the *Cartesian product* of A and B, and is denoted $A \times B$.

If a set consists of all elements satisfying a property P, we write $\{x : x \text{ has property } P\}$, or $\{x \mid x \text{ has property } P\}$; in either case the separator is read as "such that". We must be careful though: this permits us to say $M = \{\text{sets } X : X \notin X\}$, the set of all sets which do not contain themselves. Does this set contain itself? If $M \in M$, then by definition $M \notin M$; if $M \notin M$, then by definition $M \in M$ – both lead to contradictions; this is known as Russell's Paradox.

[1] Why do we talk about *the* empty set rather than *an* empty set? Because a set is determined by its elements – so the empty set is unique.

We thus can only really talk about $\{x \in X : x \text{ has property } P\}$, that is, the subset of a set X which have property P. (We can call X the "universe of discourse".) The way we avoid Russell's Paradox is by not letting the set of all sets – of which M is a subset – be a set. That said, we will often leave implicit the fact that things must be subsets of a given set, for clarity of notation (and to avoid too much confusion).

Definition 5.4. Let A and B be sets.

1. The *union* of A and B is defined as $A \cup B := \{x : x \in A \text{ or } x \in B\}$.
2. The *intersection* of A and B is defined as $A \cap B := \{x : x \in A \text{ and } x \in B\}$.
3. The *complement* of B in A is defined as $A \setminus B := \{x \in A : x \notin B\}$; this is also written $A \setminus B$.

Note that when we say P or Q, we mean that either P happens, or Q happens, *or both*. That is, "or" is used in the inclusive sense, and not in the exclusive sense. (We won't mention this again.)

When we say the *complement* of A without saying "in B", we implicitly mean "in the universe of discourse X". As such we write $A^c := \{x \in X : x \notin A\} = X \setminus A$.

Proposition 5.5. The operations $\cup$ and $\cap$ are commutative and associative, that is, for any sets A, B, C,

$$A \cup B = B \cup A \quad \text{and} \quad A \cap B = B \cap A,$$
$$(A \cup B) \cup C = A \cup (B \cup C) \quad \text{and} \quad (A \cap B) \cap C = A \cap (B \cap C).$$

Furthermore, the following distributive laws hold:

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \quad \text{and} \quad A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

Finally, de Morgan's laws hold:

$$(A \cap B)^c = A^c \cup B^c \quad \text{and} \quad (A \cup B)^c = A^c \cap B^c.$$

How do we prove such set-theoretic identities? We take one and prove it in two different ways to illustrate the various methods.

Proof. We prove that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ in two different ways.

1. Firstly, we can prove the two inclusions $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$ and $A \cap (B \cup C) \supseteq (A \cap B) \cup (A \cap C)$. For the first, let $x \in A \cap (B \cup C)$; then $x \in A$ and $x \in B \cup C$, so $x \in A$ and either $x \in B$ or $x \in C$. This is the same as saying either $x \in A$ and $x \in B$, or $x \in A$ and $x \in C$; i.e. either $x \in A \cap B$ or $x \in A \cap C$, hence $x \in (A \cap B) \cup (A \cap C)$. The second is proved similarly.

2. Secondly, we can prove this using truth tables. Each column in this table indicates the truth or falsehood of the statement $x \in X$, where X is the set indicated in the top row of the table. We start by writing the three columns on the left, and then applying the definitions of union and intersection to derive the rest of the columns. For instance, we know that $x \in B \cup C$ if $x \in B$ or $x \in C$ (or both). Thus we conclude that the fourth column should be true except when $x \notin B$ and $x \notin C$, which eliminates the fourth and eighth rows; hence the fourth column has six Ts and two Fs.

A	B	C	$B \cup C$	$A \cap (B \cup C)$	$A \cap B$	$A \cap C$	$(A \cap B) \cup (A \cap C)$
T	T	T	T	**T**	T	T	**T**
T	T	F	T	**T**	T	F	**T**
T	F	T	T	**T**	F	T	**T**
T	F	F	F	**F**	F	F	**F**
F	T	T	T	**F**	F	F	**F**
F	T	F	T	**F**	F	F	**F**
F	F	T	T	**F**	F	F	**F**
F	F	F	F	**F**	F	F	**F**

Since the two columns in bold are equal, the sets at the top must be equal, proving the required identity. □

5.1 Truth Tables and Logic

We can generalise the above notions of truth tables to logical connectives. If P and Q are statements, then $P \vee Q$ is the statement "P or Q", and $P \wedge Q$ is the statement "P and Q"; furthermore, $\neg P$ is the statement "not P". Their significance is entirely determined by the following tables:

a	$\vee$	b
T	**T**	T
T	**T**	F
F	**T**	T
F	**F**	F

a	$\wedge$	b
T	**T**	T
T	**F**	F
F	**F**	T
F	**F**	F

a	$\implies$	b
T	**T**	T
T	**F**	F
F	**T**	T
F	**T**	F

a	$\iff$	b
T	**T**	T
T	**F**	F
F	**F**	T
F	**T**	F

a	$\neg$
T	**F**
T	**T**

The truth table for $\implies$ looks a bit odd at first glance, but if a is false, no matter whether or not b is true, the implication $a \implies b$ is vacuously true, since it never happens if a is false, and this is why the table for $\implies$ is such. (We can also see that $a \implies b$ is equivalent to $(\neg a) \vee b$, meaning that either a doesn't happen, or b does; sometimes this can be an easier way of thinking of it.)

5.2 Functions

While the foundations of mathematics are built upon sets, if we had no way to talk about the relationship between different sets, mathematics would be very boring. The "popular" view of mathematics is "hard sums", or at the root of it all, *counting* things. What does it mean to count? To answer this question we consider the general notion of a function, or mapping.

Definition 5.6. A *function* or *mapping* $f\colon A \to B$ is a rule which associates to each element $a \in A$ a unique element $b \in B$. We write $f(a) = b$ or $a \mapsto b$.

We call the set A the *domain* or *source* of f and the set B the *co-domain* or *target* of f.

You may have thought of a function as a "graph" at A-level: but it is important to realise the difference. A function must assign to each x–value a unique element y–value. There are two ways in which this can fail: non-existence and non-uniqueness; if there is no y–value corresponding to a particular x–value, or if there is more than one, then the "graph" is *not* the graph of a function.

Example 5.7.
1. $f\colon \mathsf{R} \to \mathsf{R}$, $f(x) = x^2$ is a function, since to each real number it associates a unique real number (its square).
2. $f\colon \mathsf{R} \to \mathsf{R}$, $f(x) = \sqrt{x}$ is *not* a function, since if x is negative we cannot take its square root, and if x is positive it has two square roots. By convention, we use $\sqrt{x}$ to denote the *positive* square root, hence $f\colon \mathsf{R}_{\geq 0} \to \mathsf{R}$ given by $f(x) = \sqrt{x}$ *is* a function.
3. A seemingly very boring, but very useful example: $\mathrm{id}_X\colon X \to X$, $\mathrm{id}_X(x) = x$ for any $x \in X$ and any set X is called the *identity* on X, the function that does nothing.
4. A silly example: $f\colon \{\text{Countries}\} \to \{\text{Cities}\}$ given by $f(X) =$ capital city of X is a function, assuming that each country has a unique capital city. (South Africa, anyone?)

We may turn this question round: while a function must have exactly one y–value corresponding to each x–value, how many x–values can correspond to a particular y–value? In many cases – and in particular, to count the elements – we need exactly one x–value to correspond to each y–value. This can fail in two ways: there can be no x–value, or there can be more than one. If there is never more than one, we call the function *injective*, and if there is always at least one, we call the function *surjective*.

Definition 5.8. A function $f\colon A \to B$ is called *injective*, or *one-one* if, for every $a_1, a_2 \in A$, $a_1 \neq a_2$ implies $f(a_1) \neq f(a_2)$, or equivalently if $f(a_1) = f(a_2)$ implies $a_1 = a_2$.

Definition 5.9. A function $f\colon A \to B$ is called *surjective*, or *onto* if, for every $b \in B$, there exists at least one $a \in A$ such that $f(a) = b$.

Definition 5.10. A function $f\colon A \to B$ is called *bijective*, or a *one-to-one correspondence*, if it is both surjective and injective; that is, if for every $b \in B$ there is a unique $a \in A$ such that $f(a) = b$.

Example 5.11.
1. $f\colon \mathsf{R} \to \mathsf{R}$, $f(x) = x^2$ is neither injective nor surjective: both x and $-x$ map to x^2, and nothing maps to -1 (or any negative number). However, restricting the domain and codomain to $f\colon \mathsf{R}_{\geq 0} \to \mathsf{R}_{\geq 0}$, $f(x) = x^2$, this is both injective and surjective, and hence bijective.

2. Back to our silly example above: $f\colon \{\text{Countries}\} \to \{\text{Cities}\}$ given by $f(X) =$ capital city of X is injective, assuming that no two countries have the same capital. (Does Israel and Palestine sharing Jerusalem count?) It is definitely *not* surjective, since not every city is the capital of some country.

If we apply one function to something, and then apply another function, we can "compose" the two functions and get another function:

Definition 5.12. Let $f\colon A \to B$ and $g\colon B \to C$ be functions. Then we define the *composition* of f and g, denoted $g \circ f$ (read "g following f") is the function $g \circ f\colon A \to C$ given by $g \circ f(a) = g(f(a))$ for any $a \in A$.

Example 5.13. For $f\colon \mathsf{R} \to \mathsf{R}^2$ given by $f(x) = (x, x^3 + 4)$ and $g\colon \mathsf{R}^2 \to \mathsf{R}$ given by $g(x, y) = x^2 y$, the composition $g \circ f$ is $g(x, x^3 + 4) = x^2(x^3 + 4) = x^5 + 4x^2$.

5.3 Inverses

If we want to count something, we wish to set up a bijection between the set we wish to count and some subset of N: we want not only f assigns a unique y–value to each x–value, but that we can turn this round and find a unique x–value corresponding to each y–value, since then we can "count" the y–values and be sure that we have "counted" all the x–values. We are thus led to the notion of *inverse* functions.

Definition 5.14. Let $f\colon A \to B$ is a function. Then a function $g\colon B \to A$ for which $g \circ f = \mathrm{id}_A$ is called a *left inverse* to f, and a function $g\colon B \to A$ for which $f \circ g = \mathrm{id}_B$ is called a *right inverse* to f. If g is both a left inverse and a right inverse, we call g an *inverse* of f.

$g \circ f = \mathrm{id}_A$ just means that $g \circ f(a) = a$ for every $a \in A$, and $f \circ g = \mathrm{id}_B$ means that $f \circ g(b) = b$ for every $b \in B$.

Beware: this is an example of a mathematical use of language in which adding an adjective makes the thing *less* restrictive: every inverse is both a left inverse and a right inverse, but not every left (or right) inverse is an inverse.

Let $g\colon B \to A$ be a left inverse of f and let $h\colon B \to A$ be a right inverse of f. Then for all $a \in A$, $g(f(a)) = a$; in particular this is true if $a = h(b)$ for some $b \in B$, so $g(f(h(b))) = h(b)$. But as h is a right inverse of f, $f(h(b)) = b$ for any $b \in B$, hence $g(b) = h(b)$ for any $b \in B$. Thus if g is a left inverse of f and h is a right inverse of f, then $g = h$; in particular, if g and h are both inverses of f, then $g = h$. Thus we talk about *the* inverse of f without fear that it might have two.

Proposition 5.15. If $p\colon X \to Y$ is a surjection then there is an injection $i\colon Y \to X$ which is a right inverse to p. If $i\colon Y \to X$ is an injection then there is a surjection $p\colon X \to Y$ which is a left inverse to i.

If $f\colon X \to Y$ is not a surjection, then it cannot have a right inverse. Similarly, if $f\colon X \to Y$ is not an injection, then it cannot have a left inverse.

Theorem 5.16. A map $f\colon A \to B$ is an inverse if and only if it is a bijection.

We denote the inverse of a bijection f by $f^{-1}\colon B \to A$.

Note: We use the symbol f^{-1} even when f does not have an inverse, to mean the *preimage*:

$$f^{-1}(b) = \{a \in A : f(a) = b\}.$$

If f is a bijection, then $f^{-1}(b) = \{a\}$, rather than a, so the only difference is the set brackets.

5.4 Relations

Definition 5.17. A given binary relation $\sim$ on a set X is said to be an equivalence relation if and only if it is reflexive, symmetric and transitive. Equivalently,

1. For all $x \in X$, $x \sim x$
2. For all $x, y \in X$, if $x \sim y$ then $y \sim x$
3. For all $x, y, z \in X$ if $x \sim y$ and $y \sim z$ then $x \sim z$

Definition 5.18. An order relation on a set X is a relation $\leq$ which, for all $x, y, z \in X$, it satisfies satisfy the following:

1. $x \leq x$
2. If $x \leq y$ and $y \leq x$ then $x = y$
3. If $x \leq y$ and $y \leq z$ then $x \leq z$

6 Polynomials

A *polynomial* is an expression like $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, in which the a_i are constants $(i = 0, \ldots, n)$ and x is the *variable*. For example, $P_1(x) = 9x^3+16x^2-45x^3+4$ and $P_2(x) = \frac{3}{2}x^5+\frac{9}{4}x-17$ are polynomials; P_1 has integer coefficients and P_2 has rational coefficients. The set of all polynomials with integer coefficients is denoted by $\mathsf{Z}[x]$; similarly $\mathsf{Q}[x]$, $\mathsf{R}[x]$ and $\mathsf{C}[x]$ have rational, real and complex coefficients respectively.

Definition 6.1. The *degree* of a polynomial is the highest power of x appearing in it with non-zero coefficient; we denote the degree of P by $\deg(P)$.

For example, P_1 above has degree 3 and P_2 has degree 5. A polynomial of degree 0 is constant. The zero polynomial does not have a degree: it is sometimes assigned degree -1 or degree $-\infty$.

We can add and multiply polynomials by the natural rules

$$(a_n x^n + \cdots + a_0) + (b_n x^n + \cdots + b_0) = (a_n + b_n)x^n + \cdots + (a_0 + b_0)$$

(we do not assume that both polynomials have the same degree, we merely append extra terms if necessary), and

$$(a_m x^m + \cdots + a_0) \times (b_n x^n + \cdots + b_0) = (a_m b_n)x^{m+n} + (a_m b_{n-1} + a_{m-1} b_n)x^{m+n-1} + \cdots + (a_1 b_0 + a_0 b_1)x + a_0 b_0$$

or, more succinctly,

$$\left(\sum_{i=0}^{m} a_i x^i\right)\left(\sum_{j=0}^{n} b_j x^j\right) = \sum_{k=0}^{m+n}\left(\sum_{i=0}^{k} a_i b_{k-i}\right)x^k$$

It is clear from this that:

Proposition 6.2. If P_1 and P_2 are polynomials, then $\deg(P_1 P_2) = \deg(P_1) + \deg(P_2)$ (provided $P_1, P_2 \neq 0$), and $\deg(P_1 + P_2) \leq \max\{\deg(P_1), \deg(P_2)\}$.

The Binomial Theorem is a very useful way of expanding out polynomials:

Theorem 6.3 (Binomial Theorem)**.** For $n \in \mathsf{N}$, $(a+b)^n = \sum_{k=0}^{n} \frac{n!}{k!(n-k)!} a^k b^{n-k}$.

For convenience, we often denote $\frac{n!}{k!(n-k)!}$ by $\binom{n}{k}$, read "n choose k". It gives the k^{th} entry in the n^{th} row of Pascal's triangle (counting from 0).

6.1 The Euclidean Algorithm

Just as with integers, we can divide with remainder, something you should be familiar with from A–level:

Proposition 6.4. If $P_1, P_2 \in \mathsf{R}[x]$, and $P_2 \neq 0$, then there exist $Q, R \in \mathsf{R}[x]$ such that $P_1 = QP_2 + R$, with either $R = 0$ or $\deg(R) < \deg(P_2)$.

Essentially, given two polynomials, we can subtract a multiple of P_2 from P_1 such that the leading terms cancel, and hence get a remainder of lower degree. Indeed, Q and R are uniquely determined by P_1 and P_2. This proposition holds with $\mathsf{R}[x]$ replaced with $\mathsf{Q}[x]$ or $\mathsf{C}[x]$, since we can divide in any field; it does *not* hold for $\mathsf{Z}[x]$.

As with integers, when $P_1 = QP_2$ (i.e. $R = 0$), we say that P_2 divides P_1, and write $P_2 \mid P_1$. It would be nice if we could define a similar notion of "prime" for polynomials; but every polynomial is not only divisible by itself and the constant polynomial 1, but also by the constant polynomials -1 or $\frac{1}{2}$. So instead, we define:

Definition 6.5. The polynomial $P \in \mathsf{R}[x]$ is *irreducible in* $\mathsf{R}[x]$ if, whenever it factorises as a product of polynomials $P = P_1P_2$, with $P_1, P_2 \in \mathsf{R}[x]$, either P_1 or P_2 is constant. If P is not irreducible in $\mathsf{R}[x]$, we say it is *reducible in* $\mathsf{R}[x]$.

Note that irreducibility depends on the field we are working over: $(x^2 + 1)$ is irreducible in $\mathsf{R}[x]$, but factorises as $(x^2 + 1) = (x - i)(x + i)$ in $\mathsf{C}[x]$, so it is reducible in $\mathsf{C}[x]$. Over any field, however, any polynomial of degree 1 (i.e. of the form $a_1x + a_0$) is irreducible. We focus on $\mathsf{R}[x]$. Just as in the integers, we have that (almost) every polynomial is divisible by an irreducible polynomial:

Proposition 6.6. Every polynomial of degree greater than 0 (i.e. non-constant) is divisible by an irreducible polynomial.

The analogy between Z and $\mathsf{R}[x]$ is in fact quite deep – we can also define hcf and lcm of polynomials:

Definition 6.7. If P_1 and P_2 are polynomials in $\mathsf{R}[x]$, we say that $P \in \mathsf{R}[x]$ is a *highest common factor* of P_1 and P_2 if it is a common factor of P_1 and P_2, and they have no common factor of higher degree. (By common factor, we simply mean that P divides both P_1 and P_2.)

We speak of *a* highest common factor rather than *the* highest common factor, since if P is a highest common factor, then so is λP for any non-zero real number λ. However, this is the only way in which uniqueness is violated: so the highest common factor is unique up to multiplication by a non-zero constant.

We denote by $\mathsf{F}(P_1, P_2)$ the set of all common factors of P_1 and P_2. Just as with integers, we can use the following lemma to obtain an algorithm for finding the hcf and lcm:

Lemma 6.8. Suppose $P_1, P_2, Q, R \in \mathsf{R}[x]$, with $P_1 = QP_2 + R$. Then $\mathsf{F}(P_1, P_2) = \mathsf{F}(P_2, R)$; that is, the set of common factors of P_1 and P_2 is equal to the set of common factors of P_2 and R.

So by repeatedly dividing by remainder, we can use this lemma to find the highest common factor. As usual, an example is worth a thousand theorems:

Example 6.9. Let us find the highest common factor of $x^4+5x^3-2x^2+10x-8$ and $x^3+8x^2+11x-12$. By long division:

$$\begin{aligned} x^4 + 5x^3 - 2x^2 + 10x - 8 &= (x - 3)(x^3 + 8x^2 + 11x - 12) + 11(x^2 + 5x + 4) \\ x^3 + 8x^2 + 11x - 12 &= (x + 3)(x^2 + 5x + 4) \end{aligned}$$

From the first, we conclude that

$$\begin{aligned} \mathsf{F}(x^4 + 5x^3 - 2x^2 + 10x - 8, x^3 + 8x^2 + 11x - 12) &= \mathsf{F}(x^3 + 8x^2 + 11x - 12, x^2 + 5x + 4) \\ &= \mathsf{F}(x^2 + 5x + 4, 0) \end{aligned}$$

Thus we conclude that the highest common factor of these two polynomials is $x^2 + 5x + 4$.

In general, we can always find the hcf of two polynomials using the Euclidean algorithm:

$$\begin{aligned} P_1 &= Q_1P_2 + R_1 & \mathsf{F}(P_1,P_2) &= \mathsf{F}(P_2,R_1)\\ P_2 &= Q_2R_1 + R_2 & \mathsf{F}(P_2,R_1) &= \mathsf{F}(R_1,R_2)\\ R_1 &= Q_3R_2 + R_3 & \mathsf{F}(R_1,R_2) &= \mathsf{F}(R_2,R_3)\\ &\vdots & &\vdots\\ R_{N-3} &= Q_{N-1}R_{N-2} + R_{N-1} & \mathsf{F}(R_{N-3},R_{N-2}) &= \mathsf{F}(R_{N-2},R_{N-1})\\ R_{N-2} &= Q_NR_{N-1} & \mathsf{F}(R_{N-2},R_{N-1}) &= \mathsf{F}(R_{N-1},0) \end{aligned}$$

From this, we conclude that the highest common factor is the last remainder, i.e. R_{N-1}.

Non-examinable philosophical remark: The fundamental reason behind Z and $\mathsf{R}[x]$ being so similar in how hcf and lcm work is that both Z and $\mathsf{R}[x]$ are examples of *rings*. A ring is much like a field – a set with notions of addition and multiplication – but we are not guaranteed that there are always multiplicative inverses. More in MA249 Algebra II: Groups and Rings.

6.2 Roots of Polynomials

The number α is a *root* of the polynomial P if $P(\alpha) = 0$. Finding roots is closely linked with factorising polynomials:

Proposition 6.10 (The Remainder Theorem)**.** If $P \in \mathsf{R}[x]$, and $\alpha \in \mathsf{R}$, then the remainder on division of P by $x - \alpha$ is $P(\alpha)$. Hence if $P(\alpha) = 0$, then $(x - \alpha)$ divides P.

Proof. If $P(x) = (x - \alpha)Q(x) + R(x)$ with $R = 0$ or $\deg(R) < 1 = \deg(x - \alpha)$, then substituting $x = \alpha$ gives $P(\alpha) = R(\alpha)$. Since R is either zero or constant, the remainder is the constant $P(\alpha)$. □

Corollary 6.11. A polynomial $P \in \mathsf{R}[x]$ of degree n can have at most n roots in R.

These are both true in $\mathsf{Q}[x]$ and $\mathsf{C}[x]$ as well as $\mathsf{R}[x]$. However, a polynomial $P \in \mathsf{R}[x]$ is not guaranteed to have a root: for example, $P(x) = x^2 + 1$ has no roots over R. However, it has the two roots $\pm i$ over C. In fact:

Theorem 6.12 (Fundamental Theorem of Algebra)**.** If $P \in \mathsf{C}[x]$, then P has at least one root in C, and hence has exactly $\deg(P)$ roots in C.

To see the "hence" part, it suffices to take a root α of P and divide by $(x-\alpha)$; this gives a polynomial of one lower degree, to which we can then find a root, which is thus also a root of P, and so on until we are left with a constant. The proof of the Fundamental Theorem of Algebra is well beyond the scope of the course.

Definition 6.13. A complex number α is *algebraic* if it is the root of some polynomial $P \in \mathsf{Q}[x]$. A complex number which is not algebraic is called *transcendental*.

It is not clear that transcendental numbers exist; but we will prove this easily in the next section. Actually proving a particular number is transcendental is rather hard: the proofs that e and π are transcendental are rather long. But the fact that π is transcendental is the fundamental reason why you can't square the circle, i.e. you can't construct a square of the same area as a given circle with ruler and compasses. More in MA3D5 Galois Theory.

7 Different Infinities

We return to what it means to count:

Definition 7.1. A set A is *finite* if there exists a bijection $\{1, \dots, n\} \to A$; if so we write $|A| = n$ to represent the number of elements of A. If there is no such bijection, we call A an *infinite* set.

Is this it? Do all infinite sets have the "same" number of elements? No – given two infinite sets, there is not necessarily a bijection between them: R is *not* in bijection with N.

Definition 7.2. The set A is *countable* if there is a bijection between A and some subset of N. It is *countably infinite* if it is countable but not finite.

Proposition 7.3. If $B \subset \mathsf{N}$ is infinite, then there is a bijection $B \to \mathsf{N}$. Hence every countably infinite set is in bijection with N.

So if we can find a bijection from a set A to the natural numbers, we can say that A is countably infinite.

Example 7.4. Z is countably infinite. To see this, define $f\colon \mathsf{Z} \to \mathsf{N}$ by

$$f(x) = \begin{cases} 2x & \text{if } x \geq 0 \\ -2x - 1 & \text{if } x < 0 \end{cases}$$

Thus each positive integer is mapped to its double: $0 \mapsto 0$, $1 \mapsto 2$, $2 \mapsto 4$, $3 \mapsto 6$ and so on, creating space at the odd integers to map the negative integers: $-1 \mapsto 1$, $-2 \mapsto 3$, $-3 \mapsto 5$ etc. This is a bijection: thus Z is countably infinite, and in bijection with N.

Theorem 7.5. R is *not* countable.

Proof. If R were countable, then any subset would also be countable; in particular, the open interval $(0, 1)$ would be countable. So suppose $(0, 1)$ is countable, and enumerate them in a list $a_1, a_2, \dots, a_k, \dots$ (i.e. put them in bijection with N), and write them as decimal expansions:

$$\begin{aligned} a_1 &= 0.a_{11}a_{12}a_{13}\dots \\ a_2 &= 0.a_{21}a_{22}a_{23}\dots \\ &\vdots \\ a_k &= 0.a_{k1}a_{k2}a_{k3}\dots \\ &\vdots \end{aligned}$$

(To avoid repetition, we avoid decimal expansions ending in an infinite sequence of 9s.) We construct a number b, by choosing the k^{th} decimal place b_k to be different to a_{kk} and not equal to 0 or 9. Then $b = 0.b_1b_2\dots$ differs from a_k at the k^{th} place, and hence $b \neq a_k$ for every $k \in \mathsf{N}$. Thus we have produced a number in $(0, 1)$ which was not in our enumeration, which is a contradiction. Hence $(0, 1)$ is not countable. □

Example 7.6. The set of algebraic numbers in C is countably infinite. Essentially this is because the coefficients of the polynomial must be rational and Q is countable, hence there are only countably many different numbers reachable as roots of polynomials. This implies that transcendental numbers exist; if they didn't, then every real number would be algebraic, and hence R would be countable, which we've shown is false.

The fact that R is not countable means we can begin a theory of *transfinite numbers*. We say that two sets have the same *cardinality* if there is a bijection between them. We denote the cardinality of N by $\aleph_0$; thus the statement that Z (resp. Q) is countable is that $|\mathsf{Z}|(= |\mathsf{Q}|) = \aleph_0$. As $|R| \neq \aleph_0$, can we say $|R| > \aleph_0$? Does it make sense to compare cardinals?

Definition 7.7. Given cardinals $\aleph$ and $\aleph'$, we say that $\aleph \leq \aleph'$ (and $\aleph' \geq \aleph$) if there are sets X and Y with $|X| = \aleph$ and $|Y| = \aleph'$, and an injection $X \to Y$.

Theorem 7.8 (Schröder–Bernstein)**.** If X and Y are sets, and there are injections $i\colon X \to Y$ and $j\colon Y \to X$, then there is a bijection $X \to Y$.

The Schröder–Bernstein Theorem essentially says that if $|X| \leq |Y|$ and $|Y| \leq |X|$, then $|X| = |Y|$; thus comparing cardinals makes sense. But how many cardinals are there to compare?

Definition 7.9. Let X be a set. Its *power set*, denoted $\mathsf{P}(X)$, is the set of all subsets of X.

Proposition 7.10. If $|X| = n$ then $|\mathsf{P}(X)| = 2^n$.

Proposition 7.11. If X is a set, there is no surjection $X \to \mathsf{P}(X)$.

From this, we see that for every set X, we have $|X| < |\mathsf{P}(X)|$. Hence we see that

$$\aleph_0 \leq |\mathsf{N}| < |\mathsf{P}(\mathsf{N})| < |\mathsf{P}(\mathsf{P}(\mathsf{N}))| < |\mathsf{P}(\mathsf{P}(\mathsf{P}(\mathsf{N})))| < \cdots .$$

Hence there are infinitely many different infinite cardinals.

Closing Remarks

That's all there is to it – it's really not as bad as it looks at first sight. We hope this revision guide has been useful. But it's no use just reading it – practise, practise, PRACTISE! The best source is past exam papers, which can be bought from the Maths General Office, or are available to download from:

`http://go.warwick.ac.uk/exampapers/?q=MA131X`

With that, good luck on the exam!

This guide would not be possible without our wonderful sponsors: