MATH1035: Workbook Five

–M. Daws, 2010

The triangle inequality

We saw before that the polar form of a complex number works very well with multiplication. However, there is no simple way to write what $re^{i\theta} + se^{i\varphi}$ is. What can we say? It turns out that the modulus of this complex number is at most $r + s$. We aim to prove this.

First recall that if $z = a + bi$ for $a, b \in \mathbb{R}$, then we write $a = \mathrm{Re}(z)$. Then notice that

$$z + \overline{z} = a + bi + a - bi = 2a = 2\,\mathrm{Re}(z).$$

If z is written in polar form, say $z = re^{i\theta}$, then $z = r(\cos\theta + i\sin\theta)$ and so $\mathrm{Re}(z) = r\cos\theta$.

The Triangle Inequality: Let $z, w \in \mathbb{C}$. Then $|z + w| \leq |z| + |w|$.

Proof: We shall use the fact that for $t, s \geq 0$, we have that $t \leq s$ if and only if $t^2 \leq s^2$. So, we look at $|z + w|^2$,

$$|z + w|^2 = (z + w)\overline{(z + w)} = z\overline{z} + z\overline{w} + w\overline{z} + w\overline{w} = |z|^2 + 2\,\mathrm{Re}(z\overline{w}) + |w|^2,$$

because $\overline{z\overline{w}} = w\overline{z}$.

Let z and w be written in polar form $z = re^{i\theta}$ and $w = se^{i\varphi}$. Then $\overline{w} = se^{-i\varphi}$ and so

$$\mathrm{Re}(z\overline{w}) = \mathrm{Re}\left(rse^{i(\theta-\varphi)}\right) = rs\cos(\theta - \varphi).$$

As $-1 \leq \cos(\theta - \varphi) \leq 1$, it follows that

$$|\mathrm{Re}(z\overline{w})| \leq rs = |z||w|.$$

So finally

$$|z + w|^2 \leq |z|^2 + 2|\mathrm{Re}(z\overline{w})| + |w|^2 \leq |z|^2 + 2|z||w| + |w|^2 = (|z| + |w|)^2,$$

and taking the square-root gives the result. □

Why is this called the “Triangle Inequality”? We saw in lectures that, drawn in the Argand Diagram, this has a very natural interpretation as simply being the statement that the length of the hypothenuse of a triangle is at most the sum of the length of the other two sides.

Equivalence classes

We come now to probably the most abstract part of my section of the course. You’ll probably be a bit confused by this the first time you see it, but hopefully it will make some sense with time! Remember that an *equivalence relation* on X is a relation $\sim$ which satisfies: $x \sim x$ for all $x \in X$ (reflexive); $x \sim y \implies y \sim x$ (symmetric); $x \sim y$ and $y \sim z$ implies that $x \sim z$ (transitive).

Definition: Let X be a set, and let $\sim$ be an equivalence relation on X. For $x \in X$, the *equivalence class* of x is the set $\{y \in X : x \sim y\}$. In words, this is the set of all things related to x. We write $[x]$ for this set.

In Workbook 4, we showed that on $\mathbb{C}$, if we define $z \sim w \Leftrightarrow e^z = e^w$, then we have an equivalence relation. We also showed that $z \sim w$ if and only if $z = w + 2\pi ki$ for some $k \in \mathbb{Z}$. So the equivalence class of z is $[z] = \{z + 2\pi ki : k \in \mathbb{Z}\}$. On the Argand diagram, the equivalence class of z is all the points on the line directly above or below z which are a multiple of 2π distance from z.

A nicer example is given by, again on $\mathbb{C}$, defining $z \sim w \Leftrightarrow |z| = |w|$. We showed that $z \sim w$ if and only if z and w lie on the same circle, centred at the origin. So now

$$[z] = \{w \in \mathbb{C} : w \text{ lies on the same circle, centre 0, as } z\}.$$

In other words, the equivalence class $[z]$ is the circle with centre 0 and radius $|z|$,

$$[z] = \text{The circle, centre 0, with radius } |z|.$$

So the set of equivalence classes of $\sim$ is just the set of all the circles centred at the origin.

Claim: Let $\sim$ be an equivalence relation on a set X. For $x, y \in X$, we have that $[x] = [y]$ if and only if $x \sim y$.

Proof: If $[x] = [y]$ then as $y \sim y$, we have that $y \in [y] = [x]$, so $x \sim y$.

Now suppose that $x \sim y$; we aim to prove that $[x] = [y]$. First we show that $[x] \subseteq [y]$. If $z \in [x]$, then $x \sim z$ so $z \sim x$. As also $x \sim y$, we conclude that $z \sim y$, so also $y \sim z$, so $z \in [y]$.

Now we show that $[y] \subseteq [x]$. If $z \in [y]$ then $y \sim z$. As $x \sim y$, we conclude that $x \sim z$, so $z \in [x]$. Thus $[x] = [y]$ as required. □

Notice that the proof carefully uses all three properties of an equivalence relation: this is no accident! These properties are studied precisely because the above theorem holds.

So the equivalence classes split up the set X: we can this a *partition*.[1] In our example above, with $z \sim w$ if and only if $|z| = |w|$, the equivalence classes are circles centred at the origin, so this is just the statement that $\mathbb{C}$ can be split up into circles.

Well-defined functions

The example above of $z \sim w \Leftrightarrow e^z = e^w$ had some connection with the idea that in polar form, a complex number is not uniquely defined, as we can always add 2π to the angle θ.

A similar idea occurs for rational numbers: there is no unique way to write a rational number. For example, we have that

$$\frac{1}{2} = \frac{2}{4} = \frac{10}{20} = \frac{123}{246} = \cdots .$$

This can make life difficult when we try to define a function on the rationals.

For example, does the following function make sense?

$$f : \mathbb{Q} \to \mathbb{Z}; \quad f\left(\frac{a}{b}\right) = a.$$

A moment's thought shows that f does *not* make sense! As $1/2 = 2/4$, we must have that $f(1/2) = f(2/4)$. But $f(1/2) = 1$ and $f(2/4) = 2$, and $1 \neq 2$. In this case, we say that f is *not well-defined*.

Does this function make sense?

$$g : \mathbb{Q} \to \mathbb{R}; \quad g\left(\frac{a}{b}\right) = \frac{3a}{b}.$$

It seems like it does. But how do we prove this? Well, suppose we pick $q \in \mathbb{Q}$. There are lots of ways to write q as a fraction: we have to check that it doesn't matter how we do this, g will give the same answer. So, let

$$q = \frac{a}{b} = \frac{c}{d},$$

[1] Actually, any partition of X determines an equivalence relation on X, but to explain this would require me to formally define a partition, which is a bit tedious: see a book!

be two ways to write q. Then

$$\frac{3a}{b} = 3\frac{a}{b} = 3q = 3\frac{c}{d} = \frac{3c}{d}.$$

So we get the same answer, regardless of how we write q. We say that g is *well-defined.*

Similarly, define $C = \{z \in \mathbb{C} : |z| = 1\}$. Remember that any $z \in C$ can be written as $e^{i\theta}$, for some non-unique $\theta \in \mathbb{R}$. Does the following make sense?

$$h : C \to \mathbb{C}; \quad h\big(e^{i\theta}\big) = e^{i\theta/2}.$$

No, it doesn't. A counter-example is that $e^{i\pi} = e^{3i\pi}$, as this is just a strange way to write -1. So we should have that $h(e^{i\pi}) = e^{i\pi/2} = i$ and $h(e^{3i\pi}) = e^{3i\pi/2} = -i$ are the same, but clearly $i \neq -i$. So h is *not well-defined.*

So, what *are* the rational numbers?

We have been treating the rational numbers as being fractions. But fractions are tricky things. When I write

$$\frac{1}{2} = \frac{6}{12},$$

you know what I mean, but formally, this is actually very weird! Because the symbol $1/2$ is certainly not the same as $6/12$, as symbols.[2] Actually, the language of equivalence relations can help: so while the symbols $1/2$ and $6/12$ are different, they are "equivalent", in that they define the same number. In this section we'll show how to put this idea on a slightly more formal setting.

The rational numbers can formally be defined using equivalence relations. Consider the set

$$X = \big\{(a, b) \in \mathbb{Z}^2 : b \neq 0\big\}.$$

So X is the set of ordered pairs of integers, with the second co-ordinate being non-zero. We define $\sim$ on X by $(a, b) \sim (c, d)$ if and only if $ad = bc$. This is an equivalence relation:

- $(a, b) \sim (a, b)$ if and only if $ab = ba$, which is true.
- if $(a, b) \sim (c, d)$ then $ad = bc$ so $cb = da$ so $(c, d) \sim (a, b)$.
- if $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$ then $ad = bc$ and $cf = de$, and so $adf = bcf = bde$ so cancelling the d (which we can do, as $d \neq 0$) gives that $af = be$, so $(a, b) \sim (e, f)$.

Here's the tricky bit: we now want to look at the set of equivalence classes; this will be a "set of sets", as each equivalence class is a set. We write $X/\sim$ for this. So $X/\sim$ is a set; each element of $X/\sim$ is an equivalence class. In symbols,

$$X/\sim = \big\{[x] : x \in X\big\}.$$

We claim that $X/\sim$ and $\mathbb{Q}$ are really the same thing. To make this precise, we want to find a bijective map between them. Define

$$\theta : \mathbb{Q} \to X/\sim; \quad \theta\Big(\frac{a}{b}\Big) = \big[(a, b)\big].$$

So θ maps a fraction a/b to the equivalence class $[(a, b)]$.

[2] Maybe this explains why some people feel very uneasy when they first meet fractions.

Is this *well-defined*? If $a/b = c/d$, we must have that $\theta(a/b) = \theta(c/d)$. So we want $[(a,b)] = [(c,d)]$, which is if and only if $(a,b) \sim (c,d)$, which is if and only if $ad = bc$, equivalently, $a/b = c/d$, which is true. So θ is well-defined.

Claim: The function θ is a bijection.

Proof: If $\theta(a/b) = \theta(c/d)$ then $[(a,b)] = [(c,d)]$, so $(a,b) \sim (c,d)$, so $ad = bc$, so $a/b = c/d$. So θ is injective.

An equivalence class in $X/\sim$ is $[(a,b)]$ for some $(a,b) \in X$. As $b \neq 0$, we have that $a/b \in \mathbb{Q}$. Then $\theta(a/b) = [(a,b)]$. So θ is surjective. □

So we have found a bijection between $X/\sim$ and $\mathbb{Q}$. In other words, $X/\sim$ and $\mathbb{Q}$ *are the same*, once identified by θ. We can define addition and multiplication on $X/\sim$ by

$$[(a,b)] \times [(c,d)] = [(ac,bd)], \quad [(a,b)] + [(c,d)] = [(ad+bc,bd)].$$

These (using θ) correspond to the usual ideas of addition and multiplication for rationals.

It would be silly to use $X/\sim$ in place of thinking about $\mathbb{Q}$ as being fractions: however, it's nice to know that we can make fractions completely rigourous, if we wish.

Proof by contradiction

We shall say that a fraction is in *lowest form* if it's of the form a/b where no number (except 1 or -1) divides both a and b. Can we always put a fraction in lowest form? Yes: you just keep dividing by common factors![3] We now exploit this idea.

Claim: The number $\sqrt{2}$ is not rational.

Proof: Let's suppose that $\sqrt{2}$ is a rational number, say $\sqrt{2} = a/b$. We can let a/b be in lowest form. Squaring, we see that

$$2 = \frac{a^2}{b^2} \implies 2b^2 = a^2.$$

So a^2 is even.

Now, if a is odd, then $a = 2n-1$ for some $n \in \mathbb{Z}$. Then $a^2 = (2n-1)^2 = 4n^2 - 4n + 1 = 2(2n^2 - 2n) + 1$, which is an odd number. But a^2 is even; so a cannot be odd; so a must be even.

So $a = 2n$ for some $n \in \mathbb{Z}$. Then $a^2 = 4n^2$ and so

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

So b^2 is even, and thus b must also be even.

So both a and b are even, so 2 divides both a and b. So a/b isn't in lowest form. This is a contradiction! It's a contradiction to the fact that $\sqrt{2}$ could be written as a fraction. So $\sqrt{2}$ is not a rational number. □

This technique of proof is called "proof by contradiction". The idea is quite simple, but rather counter-intuitive:

- Suppose that what you want to prove is *not* true.
- Then form some argument which leads to a contradiction.
- So our original claim must have been true!

[3]Technically, this is a proof by induction! We will not explore this though.

If you get stuck in a proof, trying a proof by contradiction can be a good idea: it's often easier to try to find a contradiction than it is to prove something! Here's another example.

Claim: If $n \in \mathbb{N}$ is such that $n > 1$ and n is not prime, then there is a prime number which divides n.

Proof: Suppose this isn't true. Then let n be the *smallest* counter-example. Then n is not a prime number, so there is some $m \in \mathbb{N}$, with $1 < m < n$, which divides n. So $n = ma$ for some $a \in \mathbb{N}$. But m and a cannot be prime, or n wouldn't be a counter-example.

Now, $m < n$, so the claim does hold of m (as n is the smallest counter-example). So there is a prime number p which divides m, say $m = pb$ for some $b \in \mathbb{N}$. However, then $n = ma = pba$, so p divides n. This is a contradiction! So the result is true. □

Claim: There are an infinite number of prime numbers.

Proof: Suppose not, so there are only finitely many prime numbers. So we can list them all! Say $p_1, p_2, \cdots, p_n$ are the only prime numbers. Let's consider the number

$$q = 1 + p_1 p_2 \cdots p_n.$$

That is, multiply all the prime numbers together, and add 1.

Now, q cannot be a prime number: obviously q is bigger than each of $p_1, p_2, \cdots, p_n$, and these are the only primes. By the previous result, some prime number divides q. So there is some k such that p_k divides q. This cannot happen though, as

$$\frac{q}{p_k} = \frac{1}{p_k} + \frac{p_1 p_2 \cdots p_n}{p_k} = \frac{1}{p_k} + p_1 p_2 \cdots p_{k-1} p_{k+1} \cdots p_n,$$

which is not a whole number.

So we again have a contradiction. So there must be infinitely many primes. □

The exam

Next summer, you'll take an exam on all of Math1035. This first half of the course will have two questions, and the second half of the course will have four questions. You'll get 3 hours, and will need to answer a maximum of four questions.

Of course, as you are probably now realising, the material which I have covered turns up all over mathematics, and you'll meet ideas like equivalence relations, and functions, and mathematical induction in lots and lots of different modules.

But, what's on the exam for *this* module? You can look at the syllabus from the VLE: there's not much there!

Essentially, you need to know everything which I have covered in the workbooks:

- What are the number systems $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$?
- How do you add, subtract, multiply and divide in $\mathbb{C}$? How do you simple "equations" in $\mathbb{C}$? What is the Argand diagram? What are the modulus and argument of a complex number? What does De Moivre's Theorem say, and how do we use it to find roots of unity? What is the triangle-inequality?
- How do we formally define functions? What do injective, surjective, and bijective mean? How do we write simple proofs that a function is injective, or surjective? What's the inverse?
- What do $\forall$ and $\exists$ mean? How do we prove, or find counter-examples, for expressions using $\forall$ and $\exists$?

- What is an equivalence relation? Have some understanding of equivalence classes.
- How do we use proof by Induction? How do we use proof by Contradiction?

About the only example which you need to *learn* is De Moivre's theorem. However, the exam is not going to *just* ask for definitions: I'll get you to do little exercises with the ideas. So you need to *practise* doing exercises and examples, not (rote-)learn the examples.

Ideas for the tutorial

There will be some overlap between the time when you will be doing the problem set for this workbook, and when Prof Dales starts lecturing. So at least some of the tutorials should be devoted to covering the new lecture material; hence there are only a few suggestions here.

➥I will have (finally) lectured about the "geometric" interpretation of multiplying complex numbers: to multiply by $re^{i\theta}$ is to scale by r, and to rotate by an angle of θ (in an anti-clockwise direction). The printed notes can be found in Workbook 3. Maybe talk a little about this.

➥Use proof by contradiction to show:

- There are no positive (I mean, non-negative) integers x, y with $x^2 - y^2 = 1$.
- The sum of a rational number with an irrational number is irrational.
- There are not a finite number of rational numbers in $(0, 1)$.

➥Let P be the set of playing cards (the usual 52 cards, with suits Hearts, Diamonds, Clubs, Spades, with the ace, 2,3, $\ldots$, Jack, Queen, King. For more information, see `http://en.wikipedia.org/wiki/Playing_card`).

On P, define $a \sim b$ if and only if a and b have the same suit. This is an equivalence relation (show this if you want). What are the equivalence classes?

➥Let X be the set of non-zero real numbers, so $X = \mathbb{R} \setminus \{0\}$. On X, define $x \sim y$ if and only if $xy \geq 0$. Show that this is an equivalence relation. What are the equivalence classes?

➥On $\mathbb{R} \times \mathbb{R}$, define $(x, y) \sim (z, w)$ if and only if $x = z$. This is an equivalence relation (show this if you want). What are the equivalence classes?

Problem Set 5

Due in at the lecture on Wednesday 1 December.

1. The *triangle-inequality* is that $|z + w| \leq |z| + |w|$ for $z, w \in \mathbb{C}$. Use induction to prove that for $z_1, z_2, \cdots, z_n \in \mathbb{C}$, we have
$$\big|z_1 + z_2 + \cdots + z_n\big| \leq \sum_{j=1}^{n} |z_j|.$$
Hint: Maybe it would help to formally let $P(n)$ be this statement. How can you use the knowledge that $P(n)$ is true in helping to show $P(n+1)$. Perhaps it would help to focus on the right hand side?

2. Use the method of proof by contradiction to prove the following. In each case, you need to decide what it means for the statement to be false, and then try to find a contradiction.
   (a) If E is the set of even numbers, and D is the set of odd numbers, then $E \cap D = \emptyset$.
   (b) Show that if $n \in \mathbb{N}$ and n^2 is divisible by 3, then also n is divisible by 3.

3. Adapt the proof in lectures that $\sqrt{2}$ is not rational to shown that:
   (a) The cube root of 2 is not rational. *Hint:* The same idea, using even and odd numbers, should work.
   (b) $\sqrt{3}$ is not rational. *Hint:* Using even and odd numbers won't work here. Would looking at numbers of the form $3n$, $3n+1$ and $3n+2$ work?

4. Decide if the following functions are well-defined, or not. Either give a short proof or a counter-example, as appropriate.
   (a) Define $f : \mathbb{Q} \to \mathbb{R}$ by
$$f\Big(\frac{a}{b}\Big) = \log(|a| + |b|) - \log|b|.$$
   (b) Define $g : \mathbb{C} \to \mathbb{C}$ by
$$g\big(re^{i\theta}\big) = \begin{cases} -1 & \text{if } r = 0, \\ r^2 e^{2i\theta} & \text{if } r \neq 0. \end{cases}$$
   (c) Define $h : \mathbb{Q} \to \mathbb{R}$ by
$$h\Big(\frac{a}{b}\Big) = \exp(a - b).$$
   (d) Define $j : \mathbb{Q} \to \mathbb{C}$ by
$$j\Big(\frac{a}{b}\Big) = \frac{a^2}{b^2} + i\frac{a^2 + ab}{b^2}.$$

5. The following are equivalence relations (you do not need to prove this!) Try to find a really simple description of the equivalence classes. Give a short explanation of your answer. *Hint:* If you are stuck, then fix some element, and first try to work out the equivalence class of this element (as you did in Homework 4).
   (a) On the set of MATH1035 students, $p \sim q$ if and only if p and q are in the same tutor group.
   (b) On $\mathbb{C}$, $z \sim w$ if and only if $\text{Re}(z) = \text{Re}(w)$.

(c) On $\mathbb{N}$, $n \sim m$ if and only if 2 divides $n - m$. *Hint:* What are the numbers equivalent to 1, or to 3, or to 6?

(d) On $\mathbb{C}$, $z \sim w$ if and only if the principal value of the argument of z and w are the same. *Hint:* Think about the Argand diagram!

Hand in your work with **your name** and **your tutor's name** (one of Dr Daws, Prof Martin, Prof Read, Prof Bielawski, Mr Mihiesi (Naz) or Ms Montalvo-Ballesteros (Mayra)) and **your tutorial time** (either 9am or Noon) written clearly at the top.

Optional questions

1. Let X be a set and $f : X \to X$ be a function. Define a relation on X by xRy if and only if $f(x) = y$. Find simple conditions on the function for the relation to be:

   (a) Reflexive. *Hint:* So, when does xRx for all x?

   (b) Symmetric. *Hint:* First show that $xRf(x)$ for all x.

   (c) Transitive. (The same hint works well).

   Conversely, suppose that R is a relation on X. When is there a function $f : X \to X$ which defines R in the sense that xRy if and only if $y = f(x)$?

2. Prove that if p is a prime number, then $\sqrt{p} \notin \mathbb{Q}$. *Hint:* You might find it hard to give a completely rigourous proof. Can you at least pull out an "easily stated" property of numbers which you need?

3. The following are equivalence relations (you do not need to prove this!) Try to find a really simple description of the equivalence classes.

   (a) On $\mathbb{R}$, define $x \sim y$ if and only if $\lfloor x \rfloor = \lfloor y \rfloor$ *Hint:* This was considered in an optional question on Sheet 4.

   (b) On $\mathbb{R} \times \mathbb{R}$ define $(x, y) \sim (z, w)$ if and only if $x^2 + y^2 = z^2 + w^2$.

   (c) On $\mathbb{R} \times \mathbb{R}$ define $(x, y) \sim (z, w)$ if and only if $3x - y = 3z - w$.