Complex Numbers

Vicky Neale

Michaelmas Term 2019

Contents

1 Introduction **2**

2 What is a complex number? **2**

3 Arithmetic of complex numbers **4**

4 The Argand diagram **4**

5 Complex conjugation **6**

6 Modulus **7**

7 Argument **10**

8 Historical interlude **13**

9 De Moivre's Theorem **13**

10 Roots of unity **15**

11 Euler's formula and polar form **16**

12 Polynomials **17**

13 Historical interlude **19**

1 Introduction

This course on complex numbers will introduce new ideas to some of you, refresh ideas for others, and make sure that we all agree on notation and terminology as you begin your course in Oxford.

There are several resources that will help you as you study the course:

- the lectures
- these notes
- the problems sheet
- unusually, solutions to the problems sheet
- each other.

You will not generally receive solutions to problems sheets. But, just for this course, the department understands that tutors and students might not have time to schedule a tutorial, and so I'll provide solutions online. I strongly encourage you to talk with your fellow students about your solutions, their solutions and my solutions, and more generally to help each other out if there are parts of the course that are unfamiliar to you.

Acknowledgements

These notes, and the lectures they accompany, are extremely closely based on those produced by Dr Peter Neumann, which in turn built on notes by previous lecturers. The same applies to the problems sheet.

I would like these notes to be as useful as possible. If you (whether student or tutor) think that you've noticed a typo, or mistake, or part that is unclear, please check the current, up-to-date, notes on the website, to see whether I've already fixed it. If not, please email me (vicky.neale@maths) and I'll do something about it, and (with your permission) thank you here.

Thanks to Ken Cao, Yukai Chou and Afaq Mikaiil Tahir for helping to fix glitches in these notes and in the solutions for the problems sheet.

2 What is a complex number?

Definition. A *complex number* is an object of the form $a + bi$, where a and b are real numbers and $i = \sqrt{-1}$. The set of complex numbers is denoted $\mathbb{C}$.

This is not the place for a formal definition of $\mathbb{R}$, the set of real numbers. You will explore fundamental properties of $\mathbb{R}$ in detail in the Analysis I course this term. Here, we can think of them informally as the familiar numbers on the number line, including both the rationals (of the form $\frac{p}{q}$ where p, q are integers and $q \neq 0$) and the irrationals (the many, many numbers that fill in the gaps between the rationals, such as $\sqrt{2}$, π and e).

Our current vagueness about our notion of real numbers may be worrying, but perhaps more concerning is the appearance of $\sqrt{-1}$ in the definition of a complex number, since famously the square of any real number is non-negative: that is, $x^2 \geq 0$ for all real x. So what does it mean to write $\sqrt{-1}$? Certainly $\sqrt{-1}$ is not a 'real number', in the sense that it is not in the set $\mathbb{R}$, but as mathematicians we may still study and work with it. We *define* $i = \sqrt{-1}$ to be an object with the property that $i^2 = -1$. As we shall see, allowing ourselves to work with i gives rise to lots of useful and fascinating mathematics, and does not introduce any difficulties beyond our instinctive anxiety about writing $\sqrt{-1}$.

One happy consequence of extending our horizons to include complex numbers is that we can suddenly solve many more equations than we could previously. Negative numbers allow us to solve equations such as $x + 1 = 0$. Complex numbers allow us to solve equations such as $x^2 + 1 = 0$. In fact, more is true: by introducing i, a solution of $x^2 + 1 = 0$, we can solve not just this one quadratic equation, but also *every* quadratic equation with real coefficients.

For real numbers a, b and c, with $a \neq 0$, we know that the equation

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

can be rearranged as

$$4a^2 \left(x + \frac{b}{2a} \right)^2 = b^2 - 4ac$$

(*completing the square*). Rearranging this expression to find x in terms of a, b and c gives the familiar *quadratic formula*

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

The quantity under the square root in this formula, $b^2 - 4ac$, is called the *discriminant* of the quadratic. If $b^2 - 4ac \geq 0$, then the equation has real roots—either two distinct real roots or one repeated real root. If $b^2 - 4ac < 0$, then there is no real solution, but we see that there are still two complex solutions, since we can have

$$2a\left(x+\frac{b}{2a}\right)=\pm\sqrt{4ac-b^2}\ i$$

(note that $4ac-b^2>0$ inside the square root here). We'll consider more general polynomial equations later in the course.

3 Arithmetic of complex numbers

We add and multiply complex numbers just as you would guess, remembering where appropriate that $i^2=-1$, so we expect

$$(a+bi)(c+di)=ac+bci+adi+bdi^2=(ac-bd)+(ad+bc)i.$$

Here's the formal definition.

Definition. For real a, b, c, d we define

$$(a+bi)+(c+di)=(a+c)+(b+d)i$$

and

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

We can use this to see how to subtract too.

Addition and multiplication in $\mathbb{C}$ are *binary operations*, and have many nice properties that you will explore in other courses.

We can also divide a complex number by a non-zero complex number. If $a+bi\neq 0$, then we see that

$$\frac{1}{a+bi}=\frac{a-bi}{(a+bi)(a-bi)}=\frac{a-bi}{a^2+b^2}=\frac{a}{a^2+b^2}-\frac{b}{a^2+b^2}i.$$

This is perhaps a little mysterious at the moment, but will be more natural when we have studied complex numbers further.

4 The Argand diagram

Real numbers naturally sit along the number line. Complex numbers naturally sit in a 2-dimensional complex plane, called the *Argand diagram*. We interpret the complex number $a+bi$ as corresponding to the point with Cartesian coordinates (a,b). Figure 1 shows some complex numbers on an Argand diagram.

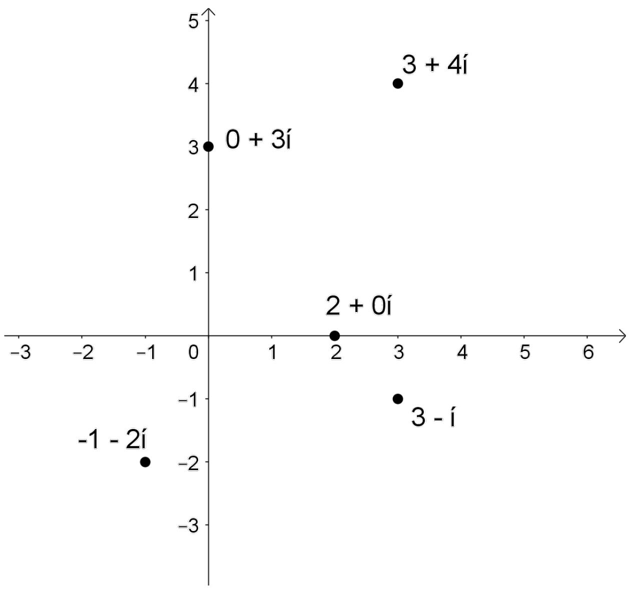

Figure 1: Argand diagram marked with the complex numbers $3i$, $3 + 4i$, 2, $3 - i$ and $-1 - 2i$.

Definition. The *real part* of $z = a + bi$ is a and is denoted $\mathrm{Re}(z)$, and the *imaginary* part of $z = a + bi$ is b and is denoted $\mathrm{Im}(z)$.

When we visualise $\mathbb{C}$ using the Argand diagram, we find that the real numbers (those complex numbers with imaginary part 0) form the horizontal axis, called the *real axis*, and the *purely imaginary numbers* (those complex numbers with real part 0) form the vertical axis, called the *imaginary axis*.

The Argand diagram gives a bridge between algebraic and geometric thinking. For example, we can interpret addition of complex numbers geometrically, as shown in Figure 2.

Note how this resembles addition of vectors. We can interpret multiplication geometrically too—we'll return to this later.

One really crucial difference between $\mathbb{R}$ and $\mathbb{C}$ relates to ordering. We have a notion of $<$ for real numbers: we can say that $-17.2 < 3$ and that $0 < 0.001$, for example. This ordering behaves rather nicely: for real numbers a and b, we see that

- if $0 < a$ and $0 < b$, then $0 < a + b$;
- if $0 < a$ and $0 < b$, then $0 < ab$;
- exactly one of $0 < a$, $a = 0$ and $0 < -a$ holds.

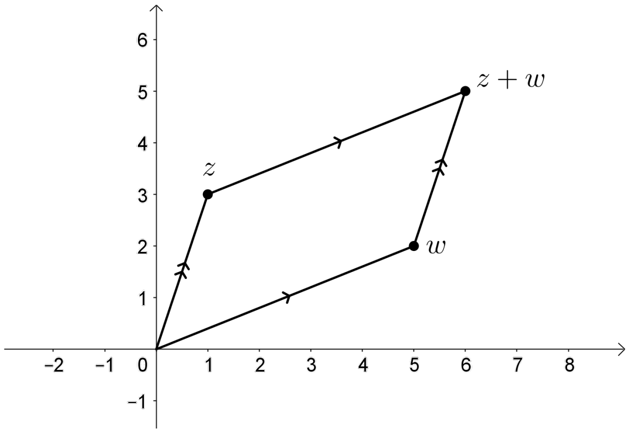

Figure 2: Argand diagram with the complex numbers 0, z, w and $z + w$ forming the vertices of a parallelogram.

You will explore these properties of the binary relation $<$ on $\mathbb{R}$ in detail in the Analysis I course. What we note here is that there is *no* such ordering on $\mathbb{C}$. I don't mean "the ordering you might first think of doesn't work". I mean that it is not possible to define a binary relation on $\mathbb{C}$ that has all three of the properties above.

Exercise. Prove this!

Health warning. *Please do not write inequalities between complex numbers (except in the very special case that those complex numbers are in fact real).*

5 Complex conjugation

Definition. The *complex conjugate* of the complex number $z = a + bi$ is $\overline{z} = a - bi$. (Some people write the complex conjugate of z as z^* instead of $\overline{z}$.)

Geometrically (in the Argand diagram), complex conjugation corresponds to reflection in the real (horizontal) axis, as illustrated in Figure 3.

Notice that if $z \in \mathbb{R}$ then $\overline{z} = z$. That is, real numbers are unchanged by complex conjugation.

Complex conjugation is very important, and happily it interacts well with the operations on $\mathbb{C}$.

Proposition 1. *For $z, w \in \mathbb{C}$ we have $\overline{z + w} = \overline{z} + \overline{w}$ and $\overline{zw} = \overline{z}\,\overline{w}$.*

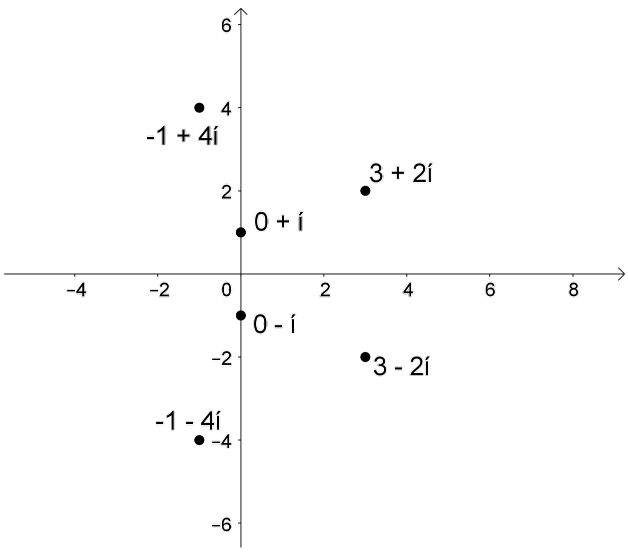

Figure 3: Argand diagram showing the complex numbers $-1 + 4i$, i and $3 + 2i$, and the complex conjugates of these, namely $-1 - 4i$, $-i$ and $3 - 2i$ respectively.

Proof. Exercise (see the problems sheet). □

Remark. Note that $z + \overline{z} = 2\,\mathrm{Re}(z)$ and $z - \overline{z} = 2\,\mathrm{Im}(z)i$. (Check this!) These are useful observations.

Interesting observation If we multiply $z = a + bi$ by $\overline{z} = a - bi$, then we get

$$z\overline{z} = (a + bi)(a - bi) = a^2 + b^2$$

—a real number. (Did you notice the difference of two squares identity there?) In fact this is an important real number...

6 Modulus

Definition. The *modulus* of the complex number $z = a + bi$ is defined to be $|z| = \sqrt{a^2 + b^2}$. (This is also sometimes called the *absolute value* of z.)

Remark. Notice that a and b are real, so $a^2 + b^2 \geq 0$, so $|z|$ is a real number. By convention, for real x when we write $\sqrt{x}$ we mean the non-negative square root. So $|z| \geq 0$ for all $z \in \mathbb{C}$, and $|z| = 0$ if and only if $z = 0$.

Geometrically, $|z|$ is the length of z, that is, the distance of z from the origin 0.

Lemma 2. *For $z = a + bi \in \mathbb{C}$, we have*

(i) $|\overline{z}| = |z|$*;*

(ii)

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

—so the modulus of a real number is just the usual absolute value;

(iii) $|z| \geq |a|$*, that is,* $|z| \geq |\operatorname{Re}(z)|$*, and similarly* $|z| \geq |\operatorname{Im}(z)|$*.*

Proof. These are immediate from the definition. (Can you write out the details?). □

Proposition 3. *Take z, $w \in \mathbb{C}$. Then*

(i) $z\overline{z} = |z|^2$*;*

(ii) $|zw| = |z||w|$*.*

Proof. (i) Write $z = a + bi$. Then

$$z\overline{z} = (a + bi)(a - bi) = a^2 + b^2 = |z|^2$$

by definition of $|z|$.

(ii) Using (i), and Proposition 1, we have

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

Now we can take square roots, since we know that $|zw|$ and $|z||w|$ are both non-negative.

□

Tip We could have proved Proposition 3(ii) by writing out real and imaginary parts. Try it yourself! I predict that it will take longer, and more importantly give less insight, than the proof here. It is often a good idea to work with complex numbers as single entities rather than real and imaginary parts, using properties such as those we have proved so far. This can take some practice to feel natural, but it is worth investing the effort until it becomes habit.

Theorem 4 (Triangle Inequality)**.** *For z, $w \in \mathbb{C}$ we have $|z+w| \leq |z|+|w|$.*

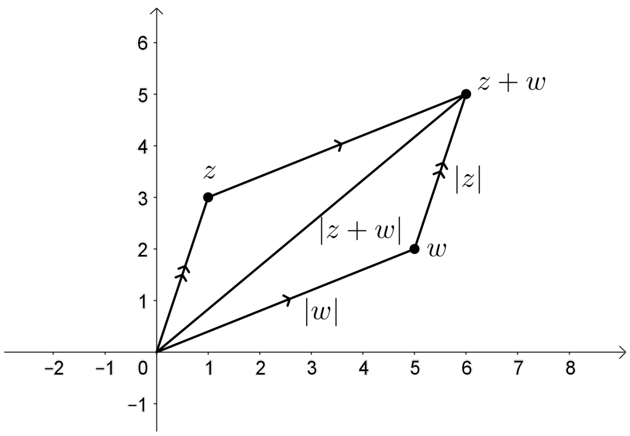

Figure 4: Argand diagram showing a parallelogram with vertices 0, z, w and $z+w$, and with line segments of lengths $|w|$, $|z|$ and $|z+w|$ forming a triangle.

Remark. Looking at the Argand diagram, as shown in Figure 4, we see that this is recording the fact that the length of any side of a triangle is less than or equal to the sum of the lengths of the other two sides. This can be proved geometrically. Here is an alternative, algebraic argument using properties of complex numbers.

Proof. Using Proposition 3, we have

$$\begin{aligned} |z+w|^2 = (z+w)(\overline{z+w}) &= (z+w)(\overline{z}+\overline{w}) \\ &= z\overline{z} + z\overline{w} + \overline{z}w + w\overline{w}. \end{aligned}$$

But

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

and, by Lemma 2 and Proposition 3,

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

so

$$\begin{aligned} |z+w|^2 &= |z|^2 + 2\,\mathrm{Re}(z\overline{w}) + |w|^2 \\ &\leq |z|^2 + 2|\,\mathrm{Re}(z\overline{w})| + |w|^2 \\ &\leq |z|^2 + 2|z||w| + |w|^2 = (|z|+|w|)^2. \end{aligned}$$

Now taking non-negative square roots gives the desired inequality. □

Remark. Equality holds in the Triangle Inequality (that is, $|z+w| = |z| + |w|$) if and only if $z = 0$ or $w = \lambda z$ for some real $\lambda \geq 0$.

Exercise. Prove this!

Now is a good time to revisit division of complex numbers.

If $z \in \mathbb{C}$, then $z\overline{z} = |z|^2$, and if $z \neq 0$ then $|z|^2 \neq 0$, so

$$\frac{1}{z} = \frac{\overline{z}}{|z|^2}.$$

Writing $z = a + bi$, this gives

$$\frac{1}{z} = \frac{1}{a+bi} = \frac{a-bi}{a^2+b^2},$$

exactly as we saw previously.

Now that we can compute $\frac{1}{z}$ for any $z \in \mathbb{C} \setminus \{0\}$, we can more generally compute $\frac{w}{z}$ for any w, $z \in \mathbb{C}$ with $z \neq 0$ (by multiplying w by $\frac{1}{z}$).

So we can add, subtract and multiply complex numbers, and we can divide by nonzero complex numbers, and these operations behave in the usual 'nice' ways. Formally, $\mathbb{C}$ is a *field* (as are $\mathbb{R}$ and $\mathbb{Q}$, and other examples too). You'll study fields in other courses.

7 Argument

So far, we have written complex numbers as $z = a + bi$. We have given the real and imaginary parts. Geometrically, we interpret this number using Cartesian coordinates (a, b). Often it is more convenient to work with complex numbers when they are written in *modulus-argument form*, which corresponds geometrically to *polar coordinates*. Rather than recording a point using distances relative to the horizontal and vertical axes, we measure the distance from the origin 0 and the angle anticlockwise from the positive horizontal axis. We illustrate this in Figure 5.

We have already defined the modulus $|z|$ of a complex number z to be the distance of z from the origin.

Definition. For a nonzero complex number z, the *argument* of z is the angle anticlockwise from the positive real axis to the line segment joining 0 and z. We write $\arg z$ for the argument of z. We do not define the argument of 0.

Remark. This definition is not entirely satisfactory, because the angle is not uniquely defined. If the angle θ satisfies the definition, then so does the angle $\theta + 2k\pi$ for any integer k. We say that $\arg z$ is only determined *modulo* 2π. To address this, we can define the *principal value* of the argument, by requiring it to lie in a particular interval. Traditionally we require either

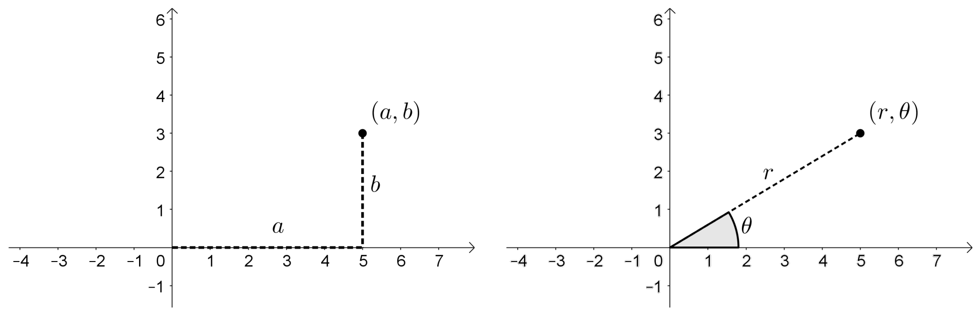

Figure 5: Two sets of axes, with the same point marked on both. In one, it is described using Cartesian coordinates, in the other with polar coordinates.

$0 \le \arg z < 2\pi$ or $-\pi < \arg z \le \pi$, depending on the context. Generally in this course we'll work with arguments modulo 2π, rather than using a principal argument, as this streamlines various results. For example, the statement that $\arg(\overline{z}) = -\arg z$ works modulo 2π, but not for every choice of principal value.

You will explore the *multifunction* argument, and related issues, in the second-year course on Complex Analysis.

Useful thought We can pass between Cartesian and polar coordinates.

If $z = a + bi$ is a nonzero complex number with modulus $|z| = r$ and argument $\arg z = \theta$, then $a = r\cos\theta$ and $b = r\sin\theta$, so $z = r(\cos\theta + i\sin\theta)$. Figure 6 illustrates this.

Notice that the ambiguity about $\arg z$ does not matter here, thanks to the 2π-periodicity of cos and sin. So we can find a and b from r and θ.

What happens in the other direction, where we know a and b and would like to find r and θ? Now $r = \sqrt{a^2 + b^2}$ just as previously—this was the definition. Also, $\tan\theta = \frac{b}{a}$ (at least when $a \neq 0$). Now determining θ requires care, because the inverse of tangent, like the argument, is a delicate 'function'. But we can recover a value if we want to.

We saw in Proposition 3 that we can find the modulus of a product zw in terms of the modulus of z and the modulus of w. What happens for the argument of a product?

Proposition 5. *Take z, $w \in \mathbb{C}$ with z, $w \neq 0$. Then*

$$\arg(zw) = \arg(z) + \arg(w).$$

Proof. Let $\theta = \arg z$, $\phi = \arg w$. Then, as above,

$$z = |z|(\cos\theta + i\sin\theta) \text{ and } w = |w|(\cos\phi + i\sin\phi).$$

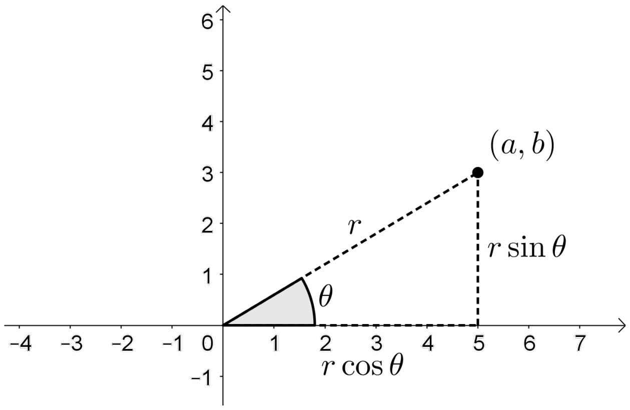

Figure 6: Axes are shown, with a triangle with vertices at the origin, at the point (a, b), and at the point on the horizontal axis vertically below (a, b). The hypotenuse has length r, and the angle at the origin is θ. The other two sides have lengths $r\cos\theta$ (horizontal) and $r\sin\theta$ (vertical).

Now

$$zw = |z||w|(\cos\theta + i\sin\theta)(\cos\phi + i\sin\phi).$$

But

$$\begin{aligned}(\cos\theta + i\sin\theta)(\cos\phi + i\sin\phi) &= (\cos\theta\cos\phi - \sin\theta\sin\phi) \\ &\quad +i(\cos\theta\sin\phi + \sin\theta\cos\phi) \\ &= \cos(\theta+\phi) + i\sin(\theta+\phi).\end{aligned}$$

So, using Proposition 3,

$$zw = |zw|(\cos(\theta+\phi) + i\sin(\theta+\phi)),$$

and so $\arg(zw) = \theta + \phi$. □

Remark. Notice that it was important here that we worked with arguments modulo 2π. If we had insisted for example that $-\pi < \arg z,\ \arg w \leq \pi$, then we might have had $\arg z + \arg w$ outside this interval, and then we'd have had to worry about 'wrapping round'.

Remark. Notice that the modulus function is multiplicative ($|zw| = |z||w|$), but argument looks more like the logarithm. This is not a coincidence (there are no coincidences in mathematics!). The complex logarithm is subtle and intriguing, and you'll study it lots in the Complex Analysis course.

Remark. We can now interpret multiplication of complex numbers geometrically. Multiplying by the nonzero complex number z rotates the complex plane anticlockwise by $\arg z$, and enlarges by a factor of $|z|$ centred on the origin.

8 Historical interlude

It's good to know at least a bit about the history of our subject. Mathematical ideas don't just turn up: mathematicians think of them! But who are the mathematicians, and what else do we know about their lives and work beyond their most famous theorems?

One useful resource is the MacTutor History of Mathematics Archive: `http://www-history.mcs.st-and.ac.uk/`. There's a list of biographies of mathematicians there. Why not look up the mathematicians we've met so far in this course?
Jean Argand
`http://www-history.mcs.st-and.ac.uk/Biographies/Argand.html`
René Descartes
`http://www-history.mcs.st-and.ac.uk/Biographies/Descartes.html`

Of course, we don't meet every significant mathematician in an undergraduate course. Plenty of mathematicians did really important work, but we don't hear their names very often. So here are a couple of additional suggestions of early mathematicians you might like to read about.
Brahmagupta
`http://www-history.mcs.st-and.ac.uk/Biographies/Brahmagupta.html`
Sun Zi
`http://www-history.mcs.st-and.ac.uk/Biographies/Sun_Zi.html`

9 De Moivre's Theorem

If $z \in \mathbb{C}$ has $|z| = 1$ and $\arg z = \theta$, then we have seen that $z = \cos\theta + i\sin\theta$. Conversely, if $z = \cos\theta + i\sin\theta$, then $|z| = \sqrt{\cos^2\theta + \sin^2\theta} = 1$. So we can nicely understand the unit circle in $\mathbb{C}$.

Definition. The *unit circle* in $\mathbb{C}$ is $S^1 := \{z \in \mathbb{C} : |z| = 1\}$.

We have just noted that also $S^1 = \{\cos\theta + i\sin\theta : \theta \in \mathbb{R}\}$.
Fun fact If $z \in S^1$ then $z^{-1} = \overline{z}$, and $z^{-1} \in S^1$.

Remark. If z, $w \in S^1$ then $|zw| = |z||w| = 1$ so $zw \in S^1$. We say that S^1 is *closed under multiplication.* It turns out that the set S^1 forms a *group* under multiplication (the fun fact above is relevant here too). You'll study groups in the course Groups and Group Actions. This group, the unit circle in $\mathbb{C}$ under multiplication, is a very important group. Watch out for it appearing in other courses!

Theorem 6 (De Moivre's Theorem)**.** *If $z \in S^1$ and $n \in \mathbb{Z}$, then*

$$\arg(z^n) = n \arg z.$$

Equivalently, for $\theta \in \mathbb{R}$ and $n \in \mathbb{Z}$, we have

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

Proof. Fix $z \in S^1$ and let $\theta = \arg z$.

For $n \geq 0$, we use induction on n.

$n = 0$: We have $z^0 = 1$ so $\arg(z^0) = 0$, and $n \arg z = 0$.

inductive step: Suppose the result holds for some $n \geq 0$, so $\arg(z^n) = n \arg z$.

Then, by Proposition 5 and the inductive hypothesis, we have

$$\begin{aligned} \arg(z^{n+1}) &= \arg(z^n) + \arg z \\ &= n\arg z + \arg z \\ &= (n+1)\arg z \end{aligned}$$

so the result holds for $n+1$.

For $n < 0$, we use the result for positive values. Fix $n < 0$, and let $m = -n$, so $m > 0$. Then, as above, $\arg(w^m) = m \arg w$ for all $w \in S^1$.

But $z^n = (z^{-1})^m = \overline{z}^m$ and $\arg(\overline{z}) = -\arg z$, so

$$\begin{aligned} \arg(z^n) &= \arg(\overline{z}^m) \\ &= m \arg \overline{z} \\ &= m(-\arg z) \\ &= (-m)\arg z \\ &= n \arg z. \end{aligned}$$

□

Example. Here is a classic application of de Moivre's theorem, for compound angle trig formulas. For any real θ, by de Moivre we have

$$\begin{aligned} \cos(3\theta) + i\sin(3\theta) &= (\cos\theta + i\sin\theta)^3 \\ &= \cos^3\theta + 3i\cos^2\theta\sin\theta - 3\cos\theta\sin^2\theta - i\sin^3\theta \\ &= (\cos^3\theta - 3\cos\theta\sin^2\theta) + i(3\cos^2\theta\sin\theta - \sin^3\theta). \end{aligned}$$

Taking real parts gives

$$\begin{aligned}\cos(3\theta) &= \cos^3\theta - 3\cos\theta\sin^2\theta \\ &= \cos\theta(\cos^2\theta - 3\sin^2\theta) \\ &= \cos\theta(\cos^2\theta - 3(1-\cos^2\theta)) \\ &= 4\cos^3\theta - 3\cos\theta\end{aligned}$$

and similarly taking imaginary parts gives

$$\begin{aligned}\sin(3\theta) &= 3\cos^2\theta\sin\theta - \sin^3\theta \\ &= \sin\theta(3\cos^2\theta - \sin^2\theta) \\ &= \sin\theta(3(1-\sin^2\theta) - \sin^2\theta) \\ &= 3\sin\theta - 4\sin^3\theta.\end{aligned}$$

10 Roots of unity

Definition. If $z \in \mathbb{C}$, $n \in \mathbb{Z}^{>0}$ and $z^n = 1$, then we say that z is a *root of unity* (an n^{th} *root of unity*).

Example. The square roots of 1 are 1, -1. The fourth roots of 1 are 1, i, -1, $-i$.

Proposition 7. *Take $z \in \mathbb{C}$. Then z is an n^{th} root of unity if and only if $|z| = 1$ and $\arg z = \frac{2k\pi}{n}$ for some $k \in \mathbb{Z}$.*

Proof. ($\Rightarrow$) Suppose that z is an n^{th} root of unity, so $z^n = 1$.

Then $|z|^n = |z^n| = 1$, and $|z|$ is a positive real, so $|z| = 1$.

By de Moivre's theorem, we have $\arg(z^n) = n \arg z$. Now

$$\arg z = \frac{\arg 1}{n} = \frac{2k\pi}{n}$$

for some $k \in \mathbb{Z}$.

($\Leftarrow$) Suppose that $|z| = 1$ and that $\arg z = \frac{2k\pi}{n}$ for some $k \in \mathbb{Z}$.

Then $|z^n| = |z|^n = 1$ and, by de Moivre, $\arg(z^n) = n \arg z = 2k\pi$, so z^n has the same modulus and argument as 1, so $z^n = 1$. □

Remark. Note that Proposition 5 shows that roots of unity lie on the unit circle S^1.

Corollary 8. *Take $n \in \mathbb{Z}^{>0}$. Then there are exactly n n^{th} roots of unity.*

Proof. From Proposition 7, we see that the n^{th} roots of unity are

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

There are n distinct such values (for example we can choose k from the set $\{0, 1, \dots, n-1\}$). □

Definition. If $z \in \mathbb{C}$ is an n^{th} root of unity and $z^m \neq 1$ for $1 \leq m \leq n-1$, then we say that z is a *primitive n^{th} root of unity.*

Proposition 9. *Let $z \in \mathbb{C}$, let n be an integer with $n \geq 2$. If z is an n^{th} root of unity and $z \neq 1$, then $z^{n-1} + z^{n-2} + \cdots + z + 1 = 0$.*

Proof. We have $0 = z^n - 1 = (z-1)(z^{n-1} + z^{n-2} + \cdots + z + 1)$ and $z \neq 1$. □

Example. Let ω be a primitive cube root of 1. Then, by Proposition 9, $\omega^2 + \omega + 1 = 0$. We can solve the quadratic equation to find that

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

We could also use Corollary 8 to see that

$$\omega = \cos\left(\frac{2\pi}{3}\right) + i\sin\left(\frac{2\pi}{3}\right) \text{ or } \omega = \cos\left(\frac{4\pi}{3}\right) + i\sin\left(\frac{4\pi}{3}\right).$$

Happily, a quick check using the values of these trig expressions shows that we get the same answer either way.

11 Euler's formula and polar form

Fact (Euler's formula) For any real number θ, we have $e^{i\theta} = \cos\theta + i\sin\theta$.

Remark. This looks like a statement requiring proof. In order to do this, we'd first need to have carefully defined the exponential, cosine and sine functions—and we haven't. You'll do this in Prelims Analysis. For now, we'll just accept the above fact. But here is a sketch of what's going on.

We can, if we are very careful, define the exponential function for complex z via a power series:

$$e^z := 1 + z + \frac{z^2}{2!} + \frac{z^3}{3!} + \frac{z^4}{4!} + \cdots .$$

(We need to be very careful because adding together infinitely many things is a delicate business....)

With that definition, we would see that

$$e^{i\theta} = 1 + i\theta - \frac{\theta^2}{2!} - \frac{i\theta^3}{3!} + \frac{\theta^4}{4!} + \cdots .$$

Separating the real and imaginary parts gives power series that you might recognise as those for cosine and sine—that in fact we can, with care, use to define cosine and sine. Watch out for more on this in Analysis!

Remark. Using Euler's formula gives a convenient way to represent a complex number in polar form. If $z \in \mathbb{C}$ has modulus r and argument θ, then we have $z = re^{i\theta}$.

We can use this to generalise Corollary 8, which counts roots of unity.

Proposition 10. *Take $z \in \mathbb{C}$ with $z \neq 0$, and let n be a positive integer. Then z has exactly n n^{th} roots.*

Proof. (Existence of at least one n^{th} root) Write $z = re^{i\theta}$, where $r = |z|$ and $\theta = \arg z$. Then $r > 0$ so (by an argument from Prelims Analysis I) there is a positive real number s such that $s^n = r$ (in fact, s is unique). Let $\phi = \frac{\theta}{n}$. Let $w = se^{i\phi}$. Then $w^n = s^n e^{in\phi} = re^{i\theta} = z$.
(Existence of at least n n^{th} roots) Let w be an n^{th} root of z as above. Let α be an n^{th} root of 1. Then $(\alpha w)^n = \alpha^n w^n = 1 \cdot z = z$. But from Corollary 8 we know that there are n possibilities for α, which give n distinct n^{th} roots of z.
(There are at most n n^{th} roots) Take w as above, and let u be any n^{th} root of z. Then $w^n = z = u^n$. Since $z \neq 0$ we have $w \neq 0$, so $\left(\frac{u}{w}\right)^n = 1$. So $\frac{u}{w}$ is an n^{th} root of unity, so $u = \beta w$ where β is one of the n n^{th} roots of unity (n by Corollary 8), so there are at most n possibilities for u. □

12 Polynomials

We saw earlier that every quadratic with real coefficients has exactly two (possibly repeated) complex roots. The same argument, of completing the square, generalises to quadratics with complex coefficients. We obtain the same quadratic formula. By Proposition 10, we know that the (complex) discriminant has exactly two square roots if it is nonzero (and exactly one square root if it is zero). So a quadratic with complex coefficients also has two roots in $\mathbb{C}$—either two distinct roots, or one root with multiplicity 2.

What happens when we generalise to polynomials of higher degree?

Proposition 11. *A complex polynomial of degree n has at most n roots in $\mathbb{C}$.*

Proof. We use induction on the degree of the polynomial.

The result is clear for polynomials of degree 1 (this is a quick check), so we focus on the induction step.

Suppose that the result holds for all polynomials of degree at most $n-1$.

Let $\tilde{p}(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ where $a_0, a_1, \ldots, a_n \in \mathbb{C}$ and $a_n \neq 0$—so the polynomial $\tilde{p}$ has degree n.

We can divide through by a_n (which is nonzero), to obtain

$$p(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$$

with $c_0, c_1, \ldots, c_{n-1} \in \mathbb{C}$. (We say that p is a *monic polynomial*, because its leading coefficient is 1.) Note that p and $\tilde{p}$ have the same roots.

If p has no roots in $\mathbb{C}$, then we are done.

If p has a root $\alpha \in \mathbb{C}$, then $p(\alpha) = 0$, so

$$\begin{aligned} p(x) = p(x) - p(\alpha) &= (x^n - \alpha^n) + c_{n-1}(x^{n-1} - \alpha^{n-1}) + \cdots + c_1(x - \alpha) \\ &= (x - \alpha) f(x) \end{aligned}$$

for some polynomial f with complex coefficients, where f is monic and has degree $n-1$.

By the induction hypothesis, f has at most $n-1$ roots in $\mathbb{C}$. Now a root β of p must satisfy $p(\beta) = 0$, which is equivalent to $(\beta - \alpha) f(\beta) = 0$. So a root of p must either be α, or must be a root of f. So p has at most n roots in $\mathbb{C}$. $\square$

Questions Does every polynomial with complex coefficients have a root? Does every such polynomial of degree n have n roots (counted with multiplicity)?

Theorem 12 (Fundamental Theorem of Algebra)**.** *Every complex polynomial with degree n has exactly n roots (counted with multiplicity). That is, if p is a monic polynomial with complex coefficients and degree n, then $p(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ for some $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ (not necessarily distinct).*

Proof. Not in this course! There are proofs using ideas of complex analysis and topology. For now, you may assume it—but only if you *really* have to. $\square$

13 Historical interlude

I'm not sure whether it's still called an interlude when it comes at the end, but I like the name 'Historical interlude', so let's stick with it. Here's another couple of MacTutor biographies for mathematicians we've met in the second part of the course.

Abraham De Moivre

`http://www-history.mcs.st-and.ac.uk/Biographies/De_Moivre.html`

Leonhard Euler

`http://www-history.mcs.st-and.ac.uk/Biographies/Euler.html`

And here are a couple of mathematicians we haven't met in this course, this time with Oxford connections.

Mary Cartwright

`http://www-history.mcs.st-and.ac.uk/Biographies/Cartwright.html`

G.H. Hardy

`http://www-history.mcs.st-and.ac.uk/Biographies/Hardy.html`

Finally, here's some history of the Fundamental Theorem of Algebra:

`http://www-groups.dcs.st-and.ac.uk/history/HistTopics/Fund_theorem_of_algebra.html`