Chapter 3: Complex Numbers

Daniel Chan

UNSW

Semester 1 2018

Philosophical discussion about numbers

Q In what sense is -1 a number? DISCUSS

Q Is $\sqrt{-1}$ a number?

A from your Kindergarten teacher Not a REAL number.

Why not then a non-real number? After all, $\sqrt{-1}$ exists as an expression, and as such it pops up all the time when you solve enough equations EVEN IF you are only interested in REAL numbers (see later).

OK. Let's extend our number system by pretending $\sqrt{-1}$ is a number which we'll denote as usual by i, and see what happens.

Thought experiment concerning i

- Well if i is a number, then surely so is $3i$ and $2+3i$.
- In fact, for any $a, b, c, d \in \mathbb{R}$, $a+bi, c+di$ are numbers too, surely.
- But then $(a+bi)+(c+di)$ is a number!That's OK, it must be one we've seen before $(a+c)+(b+d)i$.
- But also $(a+bi)(c+di)$ is a number(??).

I guess it ought to be

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

since $i^2 = -1$. We've seen this number before.

Q When does $a+bi = c+di$?

A Then $(a-c)^2 = (d-b)^2 i^2 = -(d-b)^2$ which occurs precisely when $a=c$ and $b=d$. (WHY?)

Major Question

If we keep playing this game blindly, using our usual rules of arithmetic, will we ever end up proving absurd statements like $1=0$?

Fields

Our new number system should satisfy the “usual rules of arithmetic”, and we need to formalise what this means. This uses the following

Definition

A *field* is the data consisting of a non-empty set $\mathbb{F}$ together with

- an *addition rule* $+$, which assigns to any $x, y \in \mathbb{F}$ an element $x + y \in \mathbb{F}$.
- a *multiplication rule*, which assigns to any $x, y \in \mathbb{F}$ an element $xy \in \mathbb{F}$.

such that the axioms on the following page hold.

Field axioms

1. **Associative Law of Addition**. $(x+y)+z = x+(y+z)$ for all $x, y, z \in \mathbb{F}$.
2. **Commutative Law of Addition**. $x+y = y+x$ for all $x, y \in \mathbb{F}$.
3. **Existence of a Zero**. There exists an element of $\mathbb{F}$ (usually written as 0 & called *zero*) such that $0+x = x+0 = x$ for all $x \in \mathbb{F}$.
4. **Existence of a Negative**. For each $x \in \mathbb{F}$, there exists an element $w \in \mathbb{F}$ (usually written as $-x$ & called the *negative* of x) such that $x+w = w+x = 0$.
5. **Associative Law of Multiplication**. $x(yz) = (xy)z$ for all $x, y, z \in \mathbb{F}$.
6. **Commutative Law of Multiplication**. $xy = yx$ for all $x, y \in \mathbb{F}$.
7. **Existence of a One**. There exists a non-zero element of $\mathbb{F}$ (usually written as 1 & called the *multiplicative identity*) such that $x1 = 1x = x$ for all $x \in \mathbb{F}$.
8. **Existence of an Inverse for Multiplication**. For each non-zero $x \in \mathbb{F}$, there exists an element w of $\mathbb{F}$ (usually written as $1/x$ or x^{-1} & called the *multiplicative inverse* of x) such that $xw = wx = 1$.
9. **Distributive Law**. $x(y+z) = xy+xz$ for all $x, y, z \in \mathbb{F}$.
10. **Distributive Law**. $(x+y)z = xz+yz$, for all $x, y, z \in \mathbb{F}$.

Examples

E.g. $\mathbb{F} = \mathbb{R}, \mathbb{Q}$ are fields when endowed with the usual addition and multiplication of numbers for the addition and multiplication rule.

E.g. the field with 2 elements Let $\mathbb{F} = \{\text{even}, \text{odd}\}$. Define the addition rule by

$$\text{even} + \text{even} = \text{even}, \quad \text{even} + \text{odd} = \text{odd}, \ldots.$$

and the multiplication rule by

$$\text{even} \times \text{even} = \text{even}, \quad \text{even} \times \text{odd} = \text{even}, \ldots.$$

You can check all field axioms are satisfied.

Remark This field is very important in coding theory.

What's subtraction and division?

The point of the axioms, is that this is the minimal set of assumptions to ensure you can do all the usual arithmetic in the usual way.

In particular, you can subtract and divide (by non-zero field elements). To do this you need

Fact

In a field $\mathbb{F}$, the zero, negative, one and multiplicative inverse are unique. (What's this mean?)

The proof (omitted) is not hard, but many of you might find it strange.
Hence for $x, y \in \mathbb{F}$ we can define: $x - y = x + (-y)$ and if $y \neq 0$, $\frac{x}{y} = xy^{-1}$.

E.g. Simplify the following expression in a field

$$x(y+z) - yx$$

Complex numbers

Our thought experiment suggests the following

Definition

A *complex number* is a formal expression of the form $a + bi$ for some $a, b \in \mathbb{R}$. In particular, two such numbers $a + bi, a' + b'i$ are equal iff $a = a', b = b'$ as real numbers.
The *real part* of $a + bi$ is $\mathrm{Re}(a + bi) = a$ and the *imaginary part* is $\mathrm{Im}(a + bi) = b$.

Remarks 1. Formal means in particular, that the $+$ is just a symbol, it doesn't mean addition (yet).
2. We often write a for $a + 0i$ and bi for $0 + bi$.

Arithmetic of complex numbers

Definition

Given complex numbers $a+bi, a'+b'i$ as above, we define addition and multiplication by

$$(a+bi)+(a'+b'i) = (a+a')+(b+b')i$$
$$(a+bi)(a'+b'i) = (aa'-bb')+(ab'+a'b)i$$

Warning There are two clashes of notation. What's $a+bi$ mean? We're OK.

Theorem

The set $\mathbb{C}$ of complex numbers with the above addition and multiplication rule is a field.

Proof. Is long and tedious but elementary. Note zero is $0+0i$.
This means we can perform complex number arithmetic as usual.
N.B. $\mathbb{C}$ extends the real number system since complex numbers of form $a+0i$ add and multiply just like real numbers.

Examples of complex arithmetic

Eg What's the negative of $a + bi$?

Eg $(5 - 7i) - (6 + i)$?

Eg Simplify $(2 + i)(1 - 3i) - 1 + 3i$

Division

To get the inverse we need

Cool Formula

Let $z = a + bi \in \mathbb{C}$ (with $a, b \in \mathbb{R}$ of course). We define the *conjugate of z* to be $\bar{z} = a - bi$.

$$z\bar{z} = a^2 + b^2 \in \mathbb{R}_{\geq 0}\,.$$

This gives the multiplicative inverse of z as

$$z^{-1} = \frac{\bar{z}}{a^2 + b^2}.$$

This is all we need since we know inverses of real numbers.

Usually though, we divide as follows
E.g.

Cartesian form

A complex number z written in the form $a + bi$ with $a, b \in \mathbb{R}$ is called the *cartesian form* (Later we'll meet the polar form).
Q Express $\frac{1+i}{1-i} - \frac{1-i}{1+i}$ in cartesian form.

Properties of conjugation

Proposition

1. z is real iff (= if and only if) $\overline{z} = z$.
2. $\overline{\overline{z}} = z$.
3. $\overline{z + w} = \overline{z} + \overline{w}$ and $\overline{z - w} = \overline{z} - \overline{w}$.
4. $\overline{zw} = \overline{z}\,\overline{w}$ and $\overline{\left(\dfrac{z}{w}\right)} = \dfrac{\overline{z}}{\overline{w}}$.
5. $\mathrm{Re}(z) = \frac{1}{2}(z + \overline{z})$ and $\mathrm{Im}(z) = \frac{1}{2i}(z - \overline{z})$.

Proof. Easy. Write both sides out e.g.

E.g. Show that for any $z \in \mathbb{C}$, $(i + 5)z - (i - 5)\overline{z}$ is real.

The Argand diagram

Just as real numbers can be represented by points on the real number line, complex numbers can be represented on the complex plane (or Argand diagram) as follows.

$z = a + bi$ is represented by the point with coords $(a, b) = (\mathrm{Re}z, \mathrm{Im}z)$.

The axes though are called the *real* and *imaginary* axes.

Adding complex numbers is by adding real and imaginary parts, i.e. coordinatewise so is represented geometrically by the addition of vectors. Similarly for subtraction.

Polar form

Writing a complex number as $z = x + yi, x, y \in \mathbb{R}$ is called the *cartesian form* of z. It corresponds to rectilinear coordinates.

Suppose the polar coordinates for z are given by (r, θ) as above.

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

Definition

Let $z = x + iy, x, y \in \mathbb{R}$.

1. The *modulus of* z is defined to be $|z| = r = \sqrt{x^2 + y^2}$ so $z\bar{z} = |z|^2$.
2. If $z \neq 0$, an *argument for* z is any $\theta = \arg z$ as above i.e. so that $\tan\theta = \frac{y}{x}$ and $\cos\theta, \mathrm{Re}z$ have the same sign. $\theta =: \mathrm{Arg}z$ is the *principal* argument if further $-\pi < \theta \leq \pi$.

Examples: modulus and argument

E.g. Find the modulus and principal argument of $1 - \sqrt{3}i$.

E.g. Find the modulus and principal argument of $-5 - 12i$.

E.g. Find the complex number with modulus 3 and argument $\pi/4$.

Euler's formula

Definition (Euler's formula)

For $\theta \in \mathbb{R}$, we define $e^{i\theta} = \cos\theta + i\sin\theta$.

This is reasonable by

Formulas

1. $e^{i\theta_1} e^{i\theta_2} = e^{i(\theta_1+\theta_2)}$.
2. (De Moivre's thm) For $n \in \mathbb{Z}$, $(e^{i\theta})^n = e^{in\theta}$.
3. $\frac{d}{d\theta}(e^{i\theta}) = ie^{i\theta}$.

Proof. 2) & 3) easy omitted. We only check 1).

$$
\begin{aligned}
&(\cos\theta_1 + i\sin\theta_1) \times (\cos\theta_2 + i\sin\theta_2) \\
&\quad = \cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2 + i(\cos\theta_1\sin\theta_2 + \sin\theta_1\cos\theta_2) \\
&\quad = \cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2).
\end{aligned}
$$

Challenge Q What's i^i?

Arithmetic of polar forms

The *polar form* of z is $z = re^{i\theta}$ where $r = |z|$ and θ is an argument of z.
Our formulas above give

$$r_1 e^{i\theta_1}\, r_2 e^{i\theta_2} = (r_1 r_2) e^{i(\theta_1+\theta_2)} \qquad , \qquad (re^{i\theta})^{-1} = r^{-1} e^{-i\theta}.$$

Geometrically, this says that when you multiply complex numbers, you **multiply the moduli** and **add the arguments**. Inverting inverts the modulus and negates the argument.

$$|z_1 z_2| = |z_1|\,|z_2| \qquad\qquad |z^{-1}| = |z|^{-1}$$

$$\mathrm{Arg}(z_1 z_2) = \mathrm{Arg}(z_1) + \mathrm{Arg}(z_2) + 2k\pi, \qquad\qquad \mathrm{Arg} z^{-1} = -\mathrm{Arg} z \text{ unless}$$

where $k \in \mathbb{Z}$ is chosen so that

E.g. Find the exact value of $\mathrm{Arg}\frac{1+i}{1+\sqrt{3}i}$.

Q Let $z \in \mathbb{C}$ have $|z| = 1$. Show that $w = \frac{i-z}{i+z}$ is *purely imaginary* in the sense that $\mathrm{Re} w = 0$. Interpret the result geometrically.

Square roots of complex numbers

E.g. Find the complex square roots $\pm z$ of $16 - 30i$

Quadratic formula

E.g. Solve $z^2 + (1+i)z + (-4+8i) = 0$.

Cubic formula

In the 16th century Ferro, Tartaglia, Cardano,. . . , discovered how to solve cubics.

Formula

$z^3 + pz = q$ has solutions

$$z = \sqrt[3]{\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

Q Let's use this to solve $z^3 - z = 0$ (which we know has solns ???)

Bizarre fact If there are 3 real roots, then the formula above ALWAYS involves non-real numbers.

Moral to this story Even if you only ever cared about real numbers, complex numbers naturally arise.

Proof of the cubic formula

Recall the **Binomial Thm** $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$ where $\binom{n}{k} = \frac{n!}{k!(n-k)!}$

We use Vieta's substitution $x = w - \frac{p}{3w}$

$$\begin{aligned} q &= \left(w^3 - 3w^2 \frac{p}{3w} + 3w \frac{p^2}{9w^2} - \frac{p^3}{27w^3} \right) + p(w - \frac{p}{3w}) \\ &= w^3 - \frac{p^3}{27w^3} \end{aligned}$$

This is equivalent to the quadratic in w^3

$$0 = w^6 - qw^3 - \frac{p^3}{27}$$

which has roots

$$w^3 = \frac{1}{2} \left(q \pm \sqrt{q^2 + \frac{4p^3}{27}} \right).$$

Substituting back into $x = w - \frac{p}{3w}$ gives the formula.

Powers of complex numbers

Polar form allows us to find n-th powers and n-th roots of a complex number.

E.g. Find $w = (1+i)^{18}$.
[Dumb way: multiply out $(1+i)(1+i)\dots(1+i)$]

Roots of complex numbers

More interestingly, polar forms allow easy computation of roots.

E.g. Solve $z^4 = i$.

The geometry of complex n-th roots

This example shows something that is true more generally.

Suppose that $0 \neq z_0 \in \mathbb{C}$ is given and $n \in \mathbb{Z}^+$. Then the equation

$$z^n = z_0$$

has exactly n solutions. These all lie equally spaced on the circle centred at the origin with radius $|z_0|^{1/n}$.

One solution has argument $\dfrac{\mathrm{Arg}(z_0)}{n}$, and from this you can see where the remaining solutions lie.

A number theoretic result

A *sum of squares* is an integer of the form $a^2 + b^2$ where $a, b \in \mathbb{Z}$. E.g. 6??

Theorem

The product of two sums of squares is itself a sum of squares.

Proof. We have to show given integers a, b, c, d, that $(a^2 + b^2)(c^2 + d^2)$ is a sum of two squares. Just note that

$$(a^2 + b^2)(c^2 + d^2) =$$

Note Using an extension of complex numbers called *hypercomplex numbers* or *quaternions*, one can show that every non-negative integer is the sum of 4 squares!

Expressing trigonometric polynomials as polynomials in $\cos\theta, \sin\theta$

A *trigonometric polynomial* is a linear combination of functions of the form $\cos n\theta, \sin n\theta$.

Example: Use De Moivre's thm to show $\cos(3\theta) = 4\cos^3\theta - 3\cos\theta$.

$$\begin{aligned}
\cos 3\theta &= \mathrm{Re}\left(e^{i3\theta}\right) \\
&= \mathrm{Re}\left(\cos\theta + i\sin\theta\right)^3 \\
&= \mathrm{Re}\left(\cos^3\theta + 3i\cos^2\theta\sin\theta - 3\cos\theta\sin^2\theta - i\sin^3\theta\right) \\
&= \cos^3\theta - 3\cos\theta\sin^2\theta \\
&= \cos^3\theta - 3\cos\theta(1-\cos^2\theta) \\
&= 4\cos^3\theta - 3\cos\theta.
\end{aligned}$$

Application to solving cubics

Q Solve $x^3 - 3x = 1$

A We use the substitution $x = r\cos\theta$ so

$$r^3\cos^3\theta - 3r\cos\theta = 1.$$

Pick $r = 2$ so ratio of co-efficients matches with $4\,\cos^3\theta - 3\,\cos\theta$.

Divide the eqn by $r = 2$ to obtain

$$\frac{1}{2} = 4\,\cos^3\theta - 3\,\cos\theta = \cos 3\theta.$$

Hence $3\theta = \frac{\pi}{3} + 2k\pi$ for $k \in \mathbb{Z}$. The roots are thus

$$x = 2\cos\frac{\pi}{9}, 2\cos\frac{7\pi}{9}, 2\cos\frac{-5\pi}{9}.$$

Challenge Q Show that if a cubic $x^3 - px - q$ has 3 real roots, then this method always works.

Remark on solving higher order equations

- Cardano's formula for the cubic can be used to solve the general cubic.
- There's a similar formula for the quartic (i.e. degree 4).
- There is no similar formula for degree 5 and higher. Abel and Galois proved this in the 18th century. This is taught in our 3rd/4th year course Galois theory.
- Our solution to the cubic via trigonometric functions can be extended to quintics if you use fancier functions called *elliptic functions*.

$\cos\theta, \sin\theta$ in terms of exponentials

Since

$$\begin{aligned} e^{i\theta} &= \cos\theta + i\sin\theta \\ e^{-i\theta} &= \cos(-\theta) + i\sin(-\theta) \\ &= \cos\theta - i\sin\theta \\ &= \overline{e^{i\theta}} \end{aligned}$$

we have

$$\cos\theta = \frac{e^{i\theta} + e^{-i\theta}}{2}, \qquad \text{and} \qquad i\sin\theta = \frac{e^{i\theta} - e^{-i\theta}}{2}.$$

Expressing $\cos^n \theta, \sin^n \theta$ as trig polynomials

E.g. Prove that $\sin^4 \theta = \frac{1}{8}\cos 4\theta - \frac{1}{2}\cos 2\theta + \frac{3}{8}$.

$$\sin^4 \theta = \left(\frac{e^{i\theta} - e^{-i\theta}}{2i}\right)^4$$

$$= \frac{e^{i4\theta} - 4e^{i2\theta} + 6 - 4e^{-i2\theta} + e^{-i4\theta}}{16}$$

$$= \frac{e^{i4\theta} + e^{-i4\theta}}{16} - 4\ \frac{e^{i2\theta} + e^{-i2\theta}}{16} + \frac{6}{16}$$

$$= \frac{1}{8}\cos 4\theta - \frac{1}{2}\cos 2\theta + \frac{3}{8}.$$

Thus $\int \sin^4 \theta \, d\theta =$

Trigonometric sums

Q Find $\Sigma = \cos\theta + \cos 2\theta + \ldots + \cos n\theta$.
A Consider the sum of a geometric progression

$$S := e^{i\theta} + e^{i2\theta} + \ldots + e^{in\theta} = \frac{e^{i(n+1)\theta} - e^{i\theta}}{e^{i\theta} - 1}.$$

Then

$$\Sigma = \mathrm{Re} S = \frac{S + \overline{S}}{2} = \frac{1}{2}\left(\frac{e^{i(n+1)\theta} - e^{i\theta}}{e^{i\theta} - 1} + \frac{e^{-i(n+1)\theta} - e^{-i\theta}}{e^{-i\theta} - 1}\right) = \cdots$$

OR note

$$S = e^{i\theta}\frac{e^{in\theta} - 1}{e^{i\theta} - 1} = e^{i\theta}\frac{e^{in\theta/2}(e^{in\theta/2} - e^{-in\theta/2})}{e^{i\theta/2}(e^{i\theta/2} - e^{-i\theta/2})} = e^{i(n+1)\theta/2}\frac{\sin n\theta/2}{\sin\theta/2}$$

which has real part $\Sigma = \cos\left((n+1)\theta/2\right)\frac{\sin n\theta/2}{\sin\theta/2}$.

Desribing domains in the complex plane

If z and w are complex numbers then $|z-w|$ is the distance from w to z, and $\mathrm{Arg}(z-w)$ is the "direction" from w to z. Thus

$$S = \{z \in \mathbb{C} : |z-i| \leq 3\}$$

is the disk centred at $i = (0,1)$ with radius 3.

The set

$$T = \{z \in \mathbb{C} : 0 \leq \mathrm{Arg}(z-1+i) \leq \pi/2\}$$

is the set of all the points z for which the direction from $1-i$ lies between 0 and $\pi/2$.
[For the pedants: $1-i \notin T$]

Example: domain in the complex plane

Q Sketch the set $\{z \in \mathbb{C} \,|\mathrm{Re} z < 1, \mathrm{Arg}(z+1) \leq \pi/3\}$.

Q Sketch the set $\{z \in \mathbb{C} \,|0 \leq \mathrm{Arg} z^3 \leq \pi/3\}$.

Q Sketch the set $\{z \in \mathbb{C} \,|\, \mathrm{Im} z = |z - i|\}$.

Triangle inequality

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

Triangle Inequality

$$|z+w| \leq |z| + |w|$$

The name comes from the following geometric interpretation.

Complex polynomials

Definition

A function $p : \mathbb{C} \to \mathbb{C}$ of the form

$$p(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0$$

(with *coefficients* $a_n, \ldots, a_0 \in \mathbb{C}$) is called a *(complex) polynomial*.
The *degree* of p, written $\deg(p)$, is the highest power with a non-zero coefficient.
If n above is the degree, then a_n is called the *leading coefficient*.

The fundamental theorem of algebra

A *(complex) root* of a polynomial p is any $\alpha \in \mathbb{C}$ such that $p(\alpha) = 0$.

Theorem (Gauss)

Every complex polynomial of degree at least one has a root $\alpha \in \mathbb{C}$.

Note It does not give any formula for the roots (unlike the quadratic and cubic formula).

About the proofs

- You will see a proof in your 2nd year complex analysis course.
- There is another proof via Galois theory.
- Gauss himself gave several proofs, including the following below which requires algebraic topology to make rigorous.

Factorising polynomials

Let p, q be complex polynomials of degree at least 1. Then q is a *factor* of p if there is a polynomial r such that $p = qr$. We also say q divides p.

eg. $z - 1$ is a factor of $z^3 - 1$ as $z^3 - 1 = (z-1)(z^2 + z + 1)$.

Theorem (Remainder and Factor)

Let p be a complex polynomial of degree at least one. The remainder on dividing p by $z - \alpha$ is $p(\alpha)$. In particular, $z - \alpha$ is a factor of $p(z)$ if and only if α is a root of p.

Proof. Use the long division algorithm for polynomial division to see that $p(z) = (z - \alpha)q(z) + r$ for some polynomial $q(z)$ and remainder r which is constant since its degree must be less that $\deg(z - \alpha)$.
Then $p(\alpha) = r$ which is zero precisely when α is a root or equivalently, $z - \alpha$ is a factor.

Fundamental theorem of algebra (factor form)

Putting the Factor Theorem and the Fundamental Theorem of Algebra together says that if p is a polynomial of degree n, then there exists $\alpha_1 \in \mathbb{C}$ such that $p(z) = (z - \alpha_1)g_1(z)$, where $g_1(z)$ has degree $n - 1$.

If $n - 1 \geq 1$ then there exists $\alpha_2 \in \mathbb{C}$ such that $p(z) = (z - \alpha_1)(z - \alpha_2)g_2(z)$. Continuing, you get

Theorem

Any degree n complex polynomial has a factorisation of the form

$$p(z) = (z - \alpha_1)(z - \alpha_2)\ldots(z - \alpha_n)c$$

with $\alpha_i, c \in \mathbb{C}$. The terms $(z - \alpha_j)$ are called *linear factors* of p.
This factorisation is unique up to swapping factors around.

E.g. Factorise $p(z) = z^3 + z^2 - 2$ into linear factors.

Multiplicity of roots

In an example like

$$p(z) = (z-3)^4(z-i)^2(z+1)$$

where the linear factors are not distinct, we say that $(z-3)$ is a factor of *multiplicity* 4, and that 3 is a *root of multiplicity* 4.
Similarly, i is a root of multiplicity 2 and -1 is a root of multiplicity 1.

Q Find all cubic polynomials which have 2 as a root of multiplicity 3.

Proof of uniqueness of factorisation

Consider two factorisations

$$p(z) = (z - \alpha_1)(z - \alpha_2)\ldots(z - \alpha_n)c = (z - \beta_1)(z - \beta_2)\ldots(z - \beta_n)d. \qquad (1)$$

We need to show that we can re-order the β_i's so that $\alpha_1 = \beta_1, \ldots, \alpha_n = \beta_n, c = d$. First note $c = d$ since they are both the leading co-efficient of p.

We argue by induction on n. The case $n = 0$ already has been verified so assume $n > 0$. Substitute in $z = \alpha_1$ to obtain

$$0 = (\alpha_1 - \beta_1)(\alpha_1 - \beta_2)\ldots(\alpha_1 - \beta_n)d.$$

One of the RHS factors, say $\alpha_1 - \beta_i = 0$. Swap β_i, β_1 so $\alpha_1 = \beta_1$.

Dividing (1) by $z - \alpha_1$ gives 2 factorisations of

$$\frac{p(z)}{z - \alpha_1} = (z - \alpha_2)\ldots(z - \alpha_n)c = (z - \beta_2)\ldots(z - \beta_n)d.$$

By induction, we may assume also $\alpha_2 = \beta_2, \ldots, \alpha_n = \beta_n, c = d$, so we've won.

Example: factorisation

E.g Write $p(z) = z^4 + 1$ as a product of linear factors.

N.B. Here, the complex roots occur in complex conjugate pairs. This is general phenomena for *real* polynomials.

Roots of real polynomials

A polynomial is *real* if the co-efficients are real.

Theorem

Suppose that α is a root of a real polynomial p. Then $\overline{\alpha}$ is also a root of p.

Proof.

Note that in such a case $(z - \alpha)$ and $(z - \overline{\alpha})$ are both factors. If $\alpha \notin \mathbb{R}$, then unique factorisation $\implies$ $p(z)$ has a quadratic factor

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

which is a real quadratic.

Factorising real polynomials

We say a real polynomial p is *irreducible over the reals* if it can't be factored into a product of two real polynomials of positive degree.

E.g. $z^2 - 3z + 2$ is not irreducible but $z^2 + 1$ is.
Why?

Upshot A real quadratic polynomial is irreducible over $\mathbb{R}$ iff it has non-real roots. Using the the fundamental thm of algebra and the previous slide (and our old inductive argument) we see

Theorem

Any real polynomial can be factored into a product of real linear and real irreducible quadratic polynomials.

Example: factorisation of a real polynomial

Q Factorise $p(z) = z^6 - 1$ into real irreducible factors.
Method 1 Just try your luck with factorisation facts you know

$$\begin{aligned} z^6 - 1 &= (z^2-1)(z^4+z^2+1) = (z-1)(z+1)((z^2+1)^2 - z^2) \\ &= (z-1)(z+1)(z^2+z+1)(z^2-z+1) \end{aligned}$$

OR **Method 2** Factorise into complex linear factors first.

Remark This is the first instance of common technique in mathematics, to answer a question involving real numbers, first answer it over the complex numbers and deduce your result accordingly.

Sums and products of roots

Formula

Consider a degree n polynomial $p(z) = a_0 + a_1 z + \ldots + a_n z_n$. Let $\alpha_1, \ldots, \alpha_n$ be its roots (listed with multiplicity). Then

$$\sum_{i=1}^{n} \alpha_i = -\frac{a_{n-1}}{a_n}, \quad \prod_{i=1}^{n} \alpha_i = (-1)^n \frac{a_0}{a_n}.$$

Why? For example when $n = 3$, just expand
$a_n(z - \alpha_1)(z - \alpha_2)(z - \alpha_3) =$

Eg Any real cubic of form $x^3 + a_2 x^2 + a_1 x - 1$ has a positive real root

Challenge Q Express $\sum_i \alpha_i^2$ in terms of the co-efficients.