MATH 2022 Linear and Abstract Algebra

LECTURE 39 Thursday 30/05/2019

Complex numbers revisited

- mixing up real and "imaginary" numbers, involving square roots of negative numbers
- field of complex numbers $\mathbb{C}$ represented by 2×2 matrices over $\mathbb{R}$ (Second Assignment)
- can also represent $\mathbb{C}$ using an analogue of familiar modular arithmetic using polynomials
- the field $\mathbb{C}$ has central place in history of mathematics because of the

Fundamental Theorem of Algebra,

which implies that all nontrivial polynomial equations over $\mathbb{C}$ have solutions.

The field of complex numbers :

Recall

$$\mathbb{C} = \{ a + bi \mid a, b \in \mathbb{R} \}$$

where $i = \sqrt{-1}$, becomes a field under usual addition and multiplication of complex numbers :

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

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

In the Second Assignment, we saw

$$\mathbb{C} \cong \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \mid a, b \in \mathbb{R} \right\}$$

isomorphic as field arithmetics

usual matrix addition and multiplication

The field of complex numbers :

Recall

$$\mathbb{C} = \{ a + bi \mid a, b \in \mathbb{R} \}$$

where $i = \sqrt{-1}$, becomes a field under usual addition and multiplication of complex numbers :

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

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

In the Second Assignment, we saw

$$\mathbb{C} \cong \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \mid a, b \in \mathbb{R} \right\}$$

isomorphic as field arithmetics

usual matrix addition and multiplication

$$a+bi \mapsto \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \quad \forall a, b \in \mathbb{R}$$ is an isomorphism

Using modular arithmetic :

- can also construct $\mathbb{C}$ (up to isomorphism) using "remainder arithmetic" with respect to a polynomial

Put

$$F = \{ a + bx \mid a, b \in \mathbb{R} \}$$

with usual polynomial addition

$$(a+bx) + (c+dx) = (a+c) + (b+d)x,$$

and usual polynomial multiplication, but followed by taking the remainder after dividing by x^2+1.

Using modular arithmetic :

- can also construct $\mathbb{C}$ (up to isomorphism) using "remainder arithmetic" with respect to a polynomial

Put

$$F = \{ a + bx \mid a, b \in \mathbb{R} \}$$

with usual polynomial addition

$$(a+bx) + (c+dx) = (a+c) + (b+d)x,$$

and usual polynomial multiplication, but followed by taking the remainder after dividing by x^2+1.

x^2+1 is the simplest real polynomial without any real root

e.g.

$$x^2+1 \;\overline{)\; x^2 \;}\; 1$$

$$x^2+1$$

$$-1$$

← remainder

Thus in any polynomial expression we may replace x^2 by -1.

Hence

$$(a+bx)(c+dx) = ac + (ad+bc)x + bdx^2$$

$$= ac + (ad+bc)x + bd(-1) \quad \text{in } F$$

$$= ac - bd + (bc+ad)x$$

But, in $\mathbb{C}$,

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

e.g.

$$x^2+1 \;\overline{)\; x^2 \;}\;\; 1$$

$$x^2+1$$

$$-1$$

← remainder

Thus in any polynomial expression we may replace x^2 by -1.

Hence

$$(a+bx)(c+dx) = ac + (ad+bc)x + bdx^2$$

$$= ac + (ad+bc)x + bd(-1)$$

in F

$$= ac - bd + (bc+ad)x$$

But, in $\mathbb{C}$,

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

$a+bi \mapsto a+bx \quad \forall a,b \in \mathbb{R}$ is a field isomorphism between $\mathbb{C}$ and F.

Amazing fact about $\mathbb{C}$:

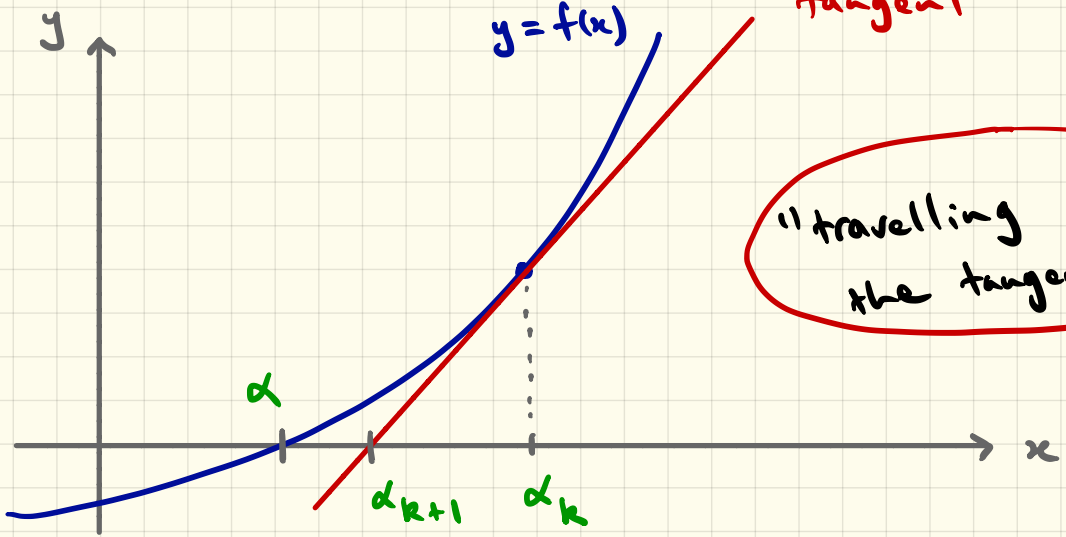
The Fundamental Theorem of Algebra:

Every nonconstant polynomial over $\mathbb{C}$ has a root in $\mathbb{C}$.

thus, in principle, all polynomial equations over $\mathbb{C}$ can be completely solved

how those solutions may or may not be described is a different story, and leads into Galois theory.

We sketch a proof of the FTA using an adaptation of Newton's Method :



"travelling down the tangent line"

$$\alpha_{k+1} = \alpha_k - \frac{f(\alpha_k)}{f'(\alpha_k)}$$

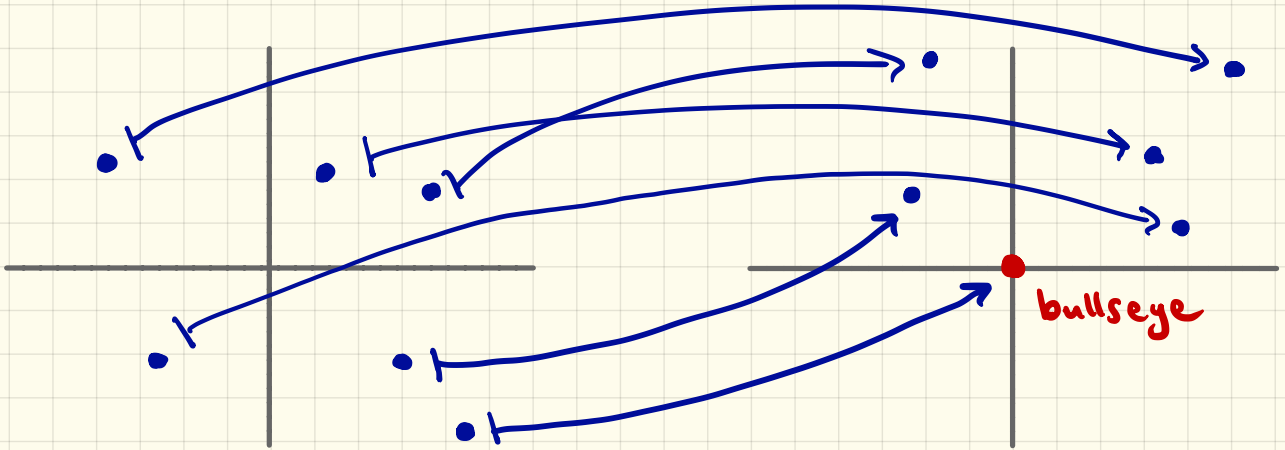
Sketch of proof of the FTA:

Suppose $p : \mathbb{C} \to \mathbb{C}$

where

$$p(z) = a_0 + a_1 z + \cdots + a_n z^n$$

where $n > 0$ and $a_n \neq 0$ (so $p(z)$ is not constant).



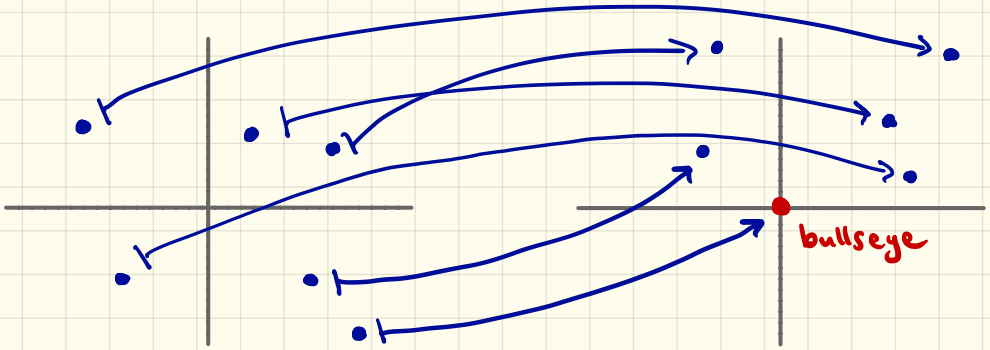
Sketch of proof of the FTA:

Suppose $p : \mathbb{C} \to \mathbb{C}$

where

$$p(z) = a_0 + a_1 z + \cdots + a_n z^n$$

where $n > 0$ and $a_n \neq 0$ (so $p(z)$ is not constant).



source $\mathbb{C}$ (inputs) target $\mathbb{C}$ (outputs)

If $p(z) = 0$, the "bullseye" in the target copy of $\mathbb{C}$ then we have found a root of the polynomial $p(z)$

Suppose, by way of contradiction, that $p(z) \neq 0$ for all $z \in \mathbb{C}$, so we always "miss the bullseye".

We obtain a contradiction in several steps.

Step (i): Form the derivative $p'(z)$ of degree $n-1$, and list all critical points (if any, but only finitely many)

$$c_1, c_2, \ldots, c_k \qquad (k \geq 0)$$

where

$$p'(c_1) = p'(c_2) = \cdots = p'(c_k) = 0,$$

and the critical values

$$p(c_1), p(c_2), \ldots, p(c_k)$$

located in the target copy of $\mathbb{C}$.

Suppose, by way of contradiction, that $p(z) \neq 0$ for all $z \in \mathbb{C}$, so we always "miss the bullseye".

We obtain a contradiction in several steps.

Step (i): Form the derivative $p'(z)$ of degree $n-1$, and list all critical points (if any, but only finitely many)

$$c_1, c_2, \dots, c_k \quad (k \geq 0)$$

where

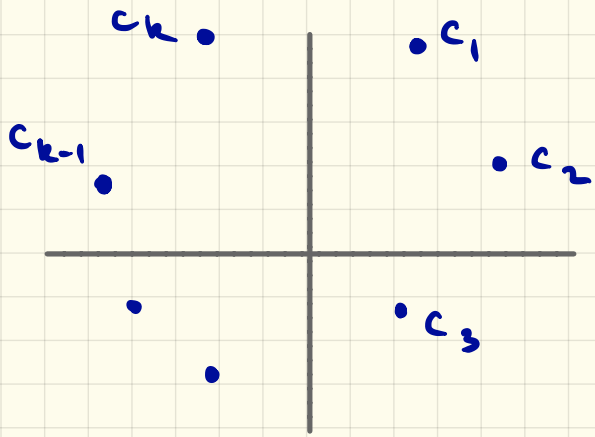
$$p'(c_1) = p'(c_2) = \dots = p'(c_k) = 0,$$

and the critical values

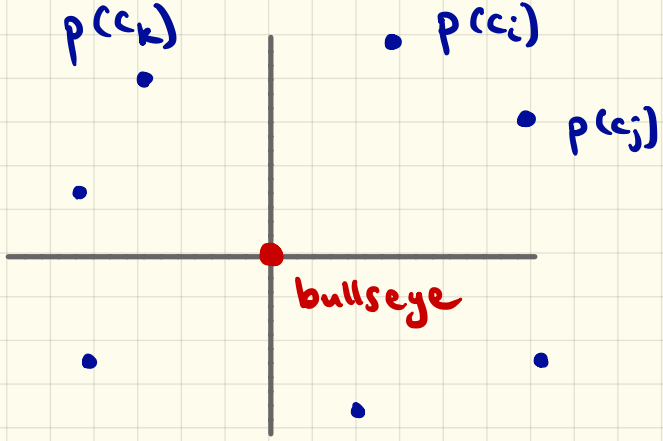
$$p(c_1), p(c_2), \dots, p(c_k)$$

located in the target copy of $\mathbb{C}$.

all non-zero since we always miss the bullseye



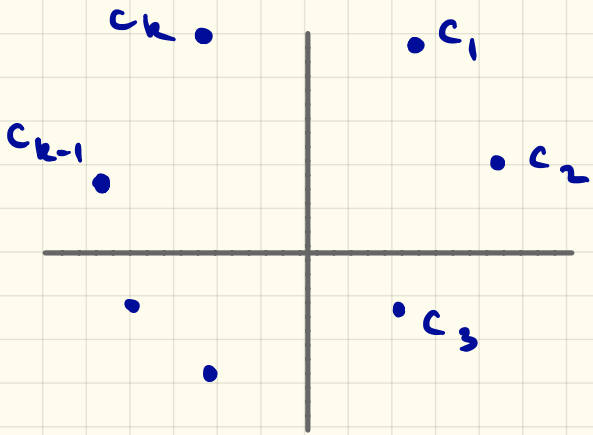
source $\mathbb{C}$ (inputs)



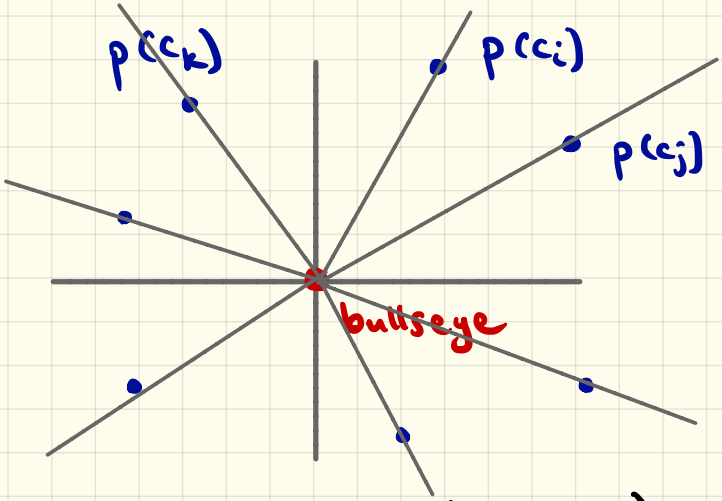
target $\mathbb{C}$ (outputs)

In the target copy of $\mathbb{C}$, form spokes from the origin passing through the critical values.

The spokes divide the target copy of $\mathbb{C}$ into "wedges".



source $\mathbb{C}$ (inputs)

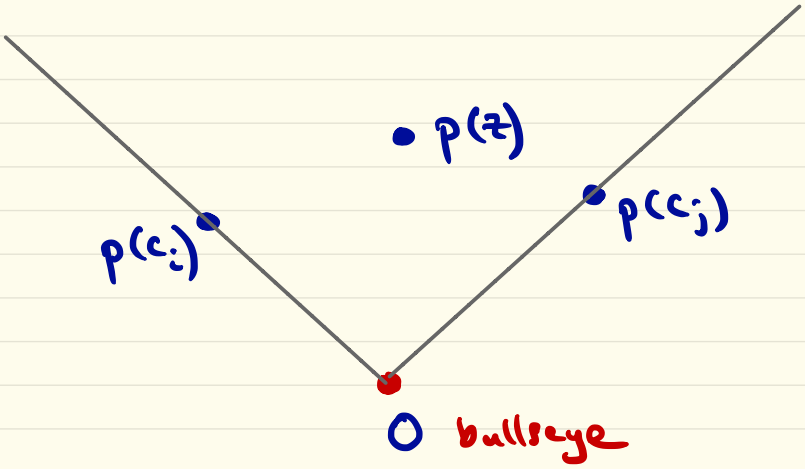


target $\mathbb{C}$ (outputs)

In the target copy of $\mathbb{C}$, form spokes from the origin passing through the critical values.

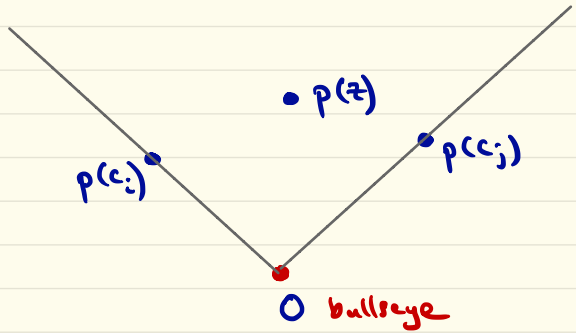
The spokes divide the target copy of $\mathbb{C}$ into "wedges".

Step (ii): Choose z in the source copy of $\mathbb{C}$ such that $p(z)$ falls inside the wedge between adjacent spokes in the target copy of $\mathbb{C}$.



This is always possible (by continuity)

Step (ii): Choose z in the source copy of $\mathbb{C}$ such that $p(z)$ falls inside the wedge between adjacent spokes in the target copy of $\mathbb{C}$.

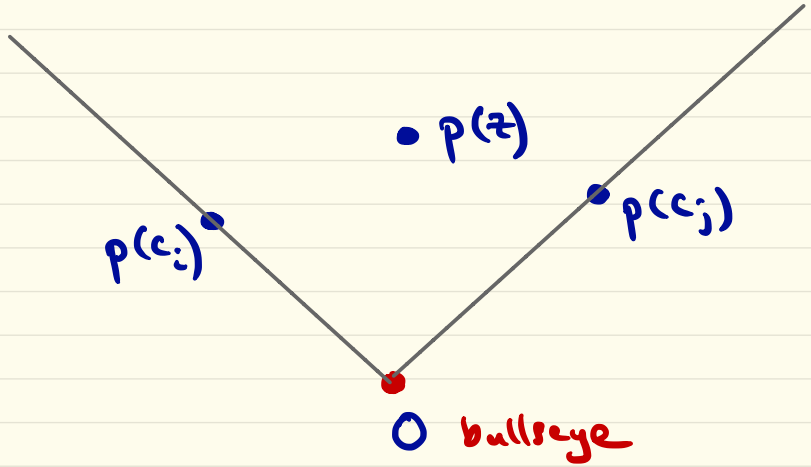


This is always possible (by continuity), since a path from c_i to c_j in the source copy of $\mathbb{C}$ always produces a path from $p(c_i)$ to $p(c_j)$ in the target copy of $\mathbb{C}$.

This is always possible (by continuity), since a path from c_i to c_j in the source copy of $\mathbb{C}$ always produces a path from $p(c_i)$ to $p(c_j)$ in the target copy of $\mathbb{C}$.

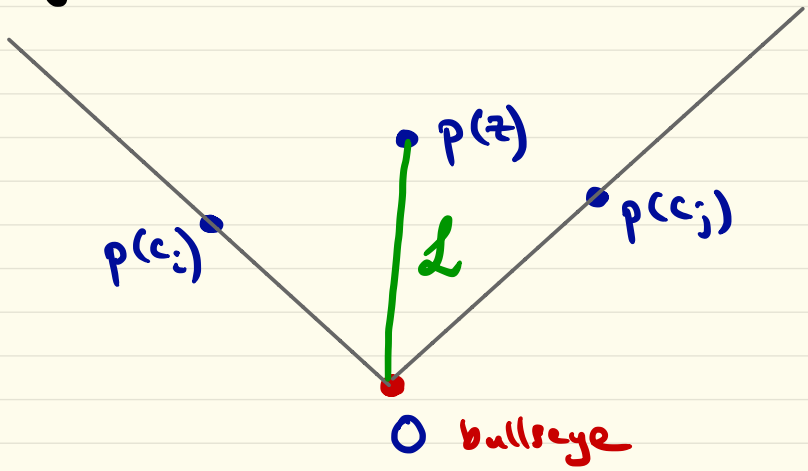
We always avoid the bullseye, so must move into the interior of some wedge.

We always avoid the bullseye, so must move into the interior of some wedge.



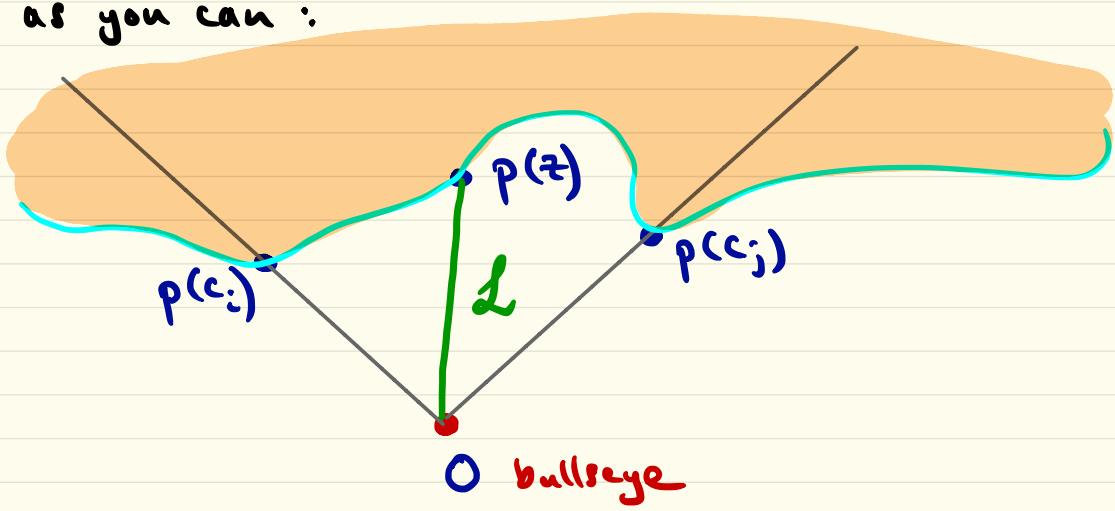
Step (iii): Add a line segment ℓ from $p(z)$ to the origin 0 (bullseye), and move towards the bullseye as far as you can:

Step (iii) : Add a line segment ℓ from $p(z)$ to the origin 0 (bullseye), and move towards the bullseye as far as you can :



Without loss of generality, we may suppose $p(z)$ is in the range of p, but any point on ℓ closer to 0 falls outside the range of p.

Step (iii) : Add a line segment ℓ from $p(z)$ to the origin 0 (bullseye), and move towards the bullseye as far as you can :



Without loss of generality, we may suppose $p(z)$ is in the range of p, but any point on ℓ closer to 0 **falls outside the range** of p.

Step (iv) : Recall the definition of the derivative :

$$p'(z) = \lim_{h \to 0} \frac{p(z+h) - p(z)}{h}$$

So

$$p(z+h) \approx p(z) + h\,p'(z)$$

can make the approximation as good as we like by choosing h sufficiently small

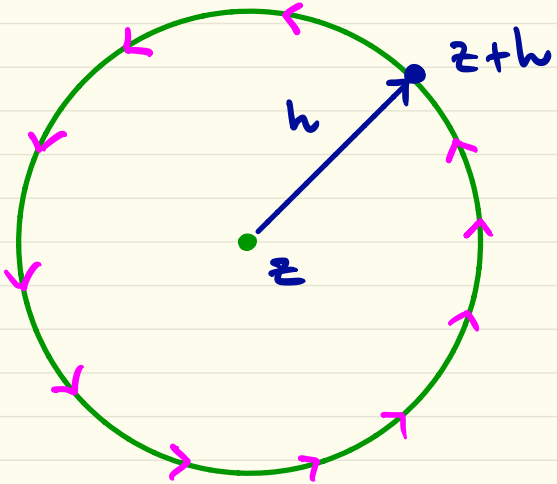
Write h in polar form : $h = \delta e^{i\theta}$

where $\delta = |h|$ is small and $0 \leq \theta \leq 2\pi$.

As θ moves from 0 to 2π,

$$z+h = z+\delta e^{i\theta}$$

makes a full revolution around z in the source copy of $\mathbb{C}$:

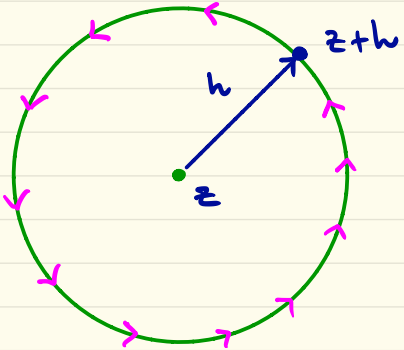


source $\mathbb{C}$

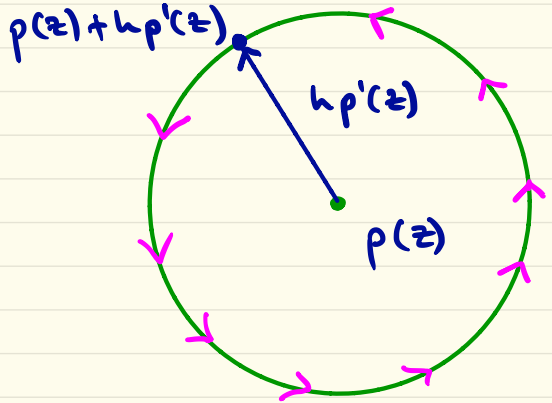
As θ moves from 0 to 2π,

$$z+h = z+\delta e^{i\theta}$$

makes a full revolution around z in the source copy of $\mathbb{C}$:



source $\mathbb{C}$

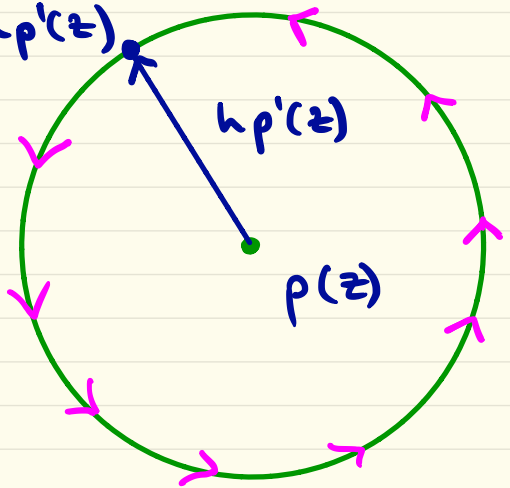


target $\mathbb{C}$

At the same time, noting $p'(z) \neq 0$, $p(z) + hp'(z)$ makes a full revolution around $p(z)$ in the target copy of $\mathbb{C}$.

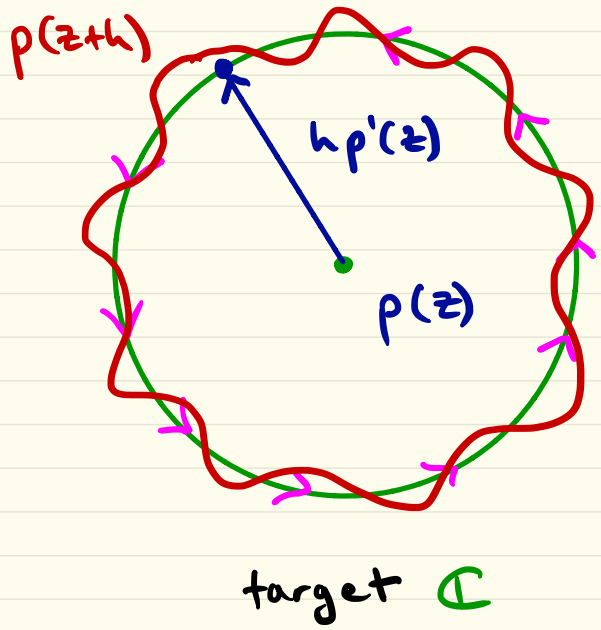
But

$p(z+h) \approx p(z) + hp'(z)$

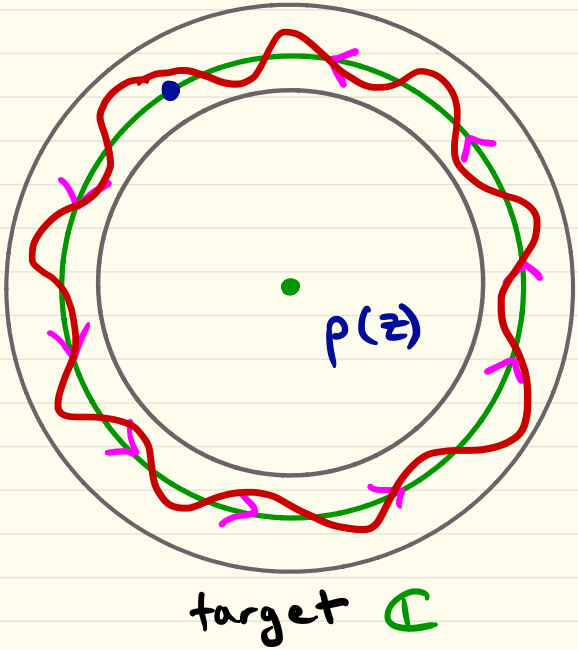


target $\mathbb{C}$

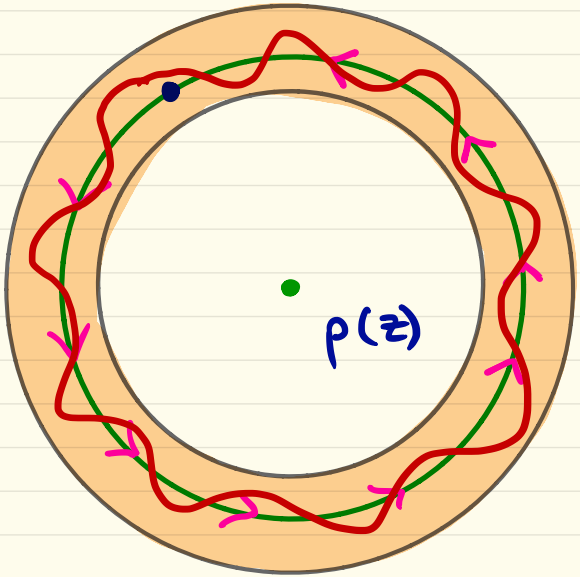
and we can choose h small enough that $p(z+h)$ is trapped inside an annulus centred at $p(z)$.



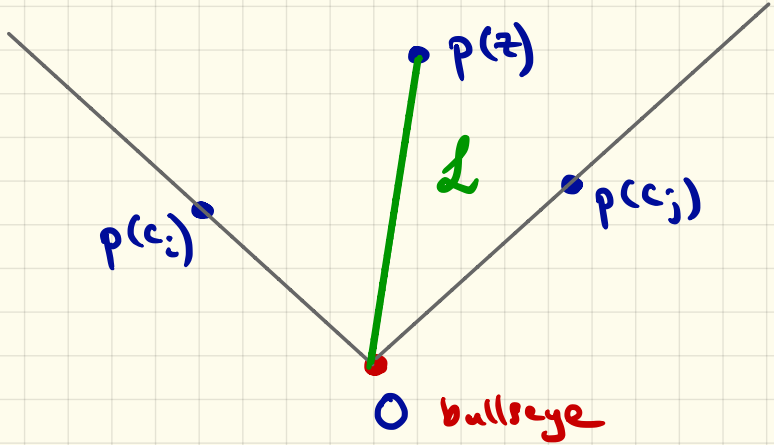
and we can choose h small enough that $p(z+h)$ is trapped inside an annulus centred at $p(z)$.

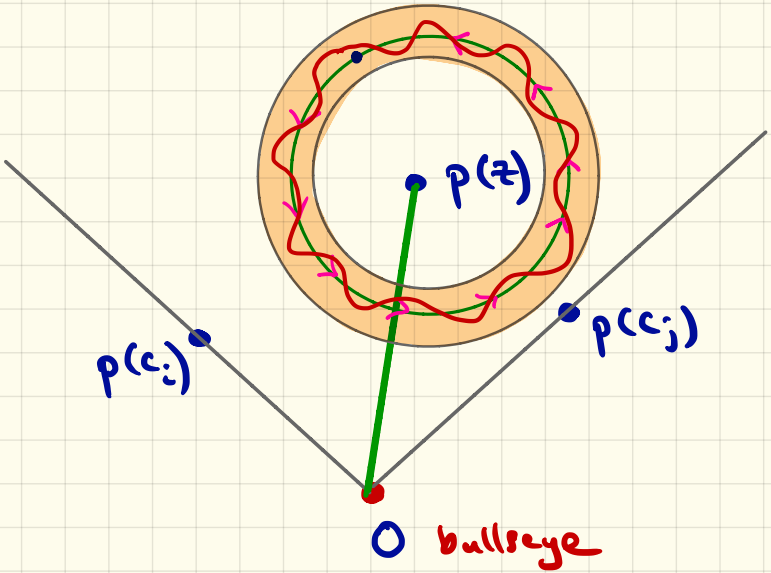


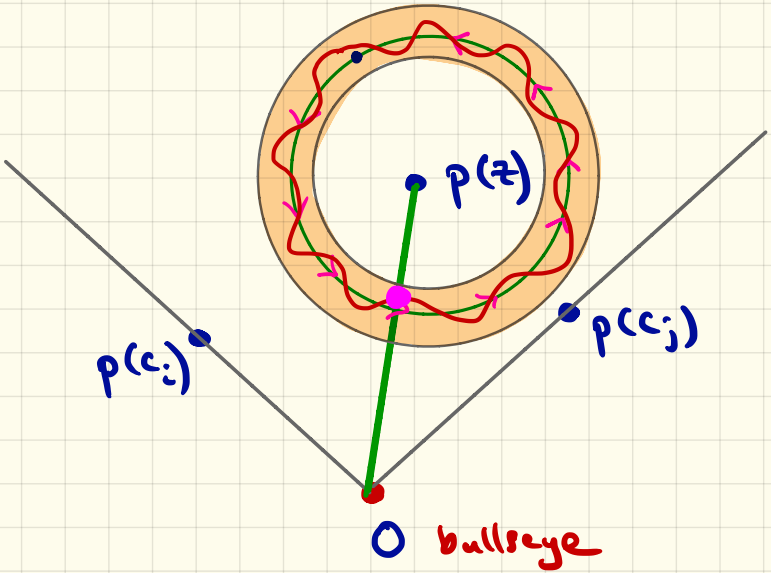
and we can choose h small enough that $p(z+h)$ is trapped inside an annulus centred at $p(z)$.

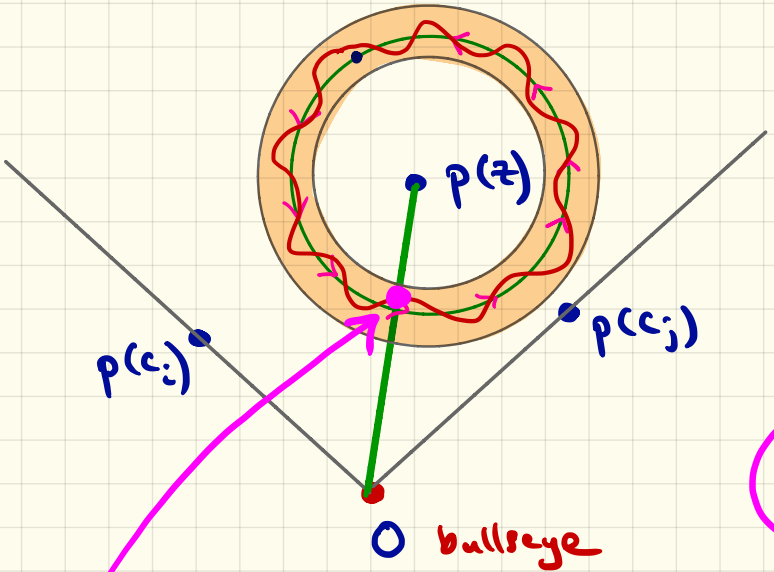


and we can choose h small enough that $p(z+th)$ is trapped inside an annulus centred at $p(z)$.


p(z)
l
p(c_i)
p(c_j)
bullseye

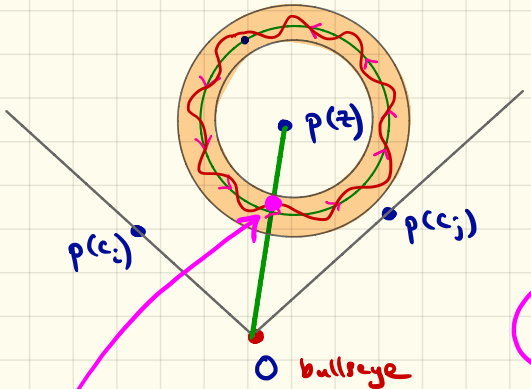

p(z)
p(c_i)
p(c_j)
bullseye


p(z)
p(c_i)
p(c_j)
bullseye



using continuity of p

But $p(z+h)$ touches the line $\mathcal{L}$ closer to 0, which is impossible!!



using continuity of p

But $p(z+h)$ touches the line $\mathcal{L}$ closer to 0, which is impossible!!

This contradiction shows our supposition is false, so $p(z) = 0$ for some z, completing the proof of the Fundamental Theorem of Algebra. $\square$

Connection with Newton's Method :

If we choose h so that

$$p(z) + h\,p'(z) = 0$$

then

$$h = -\frac{p(z)}{p'(z)}$$

so, back in the source copy of $\mathbb{C}$,

$$z + h = z - \frac{p(z)}{p'(z)}$$

which is the formula for Newton's Method.

THE END ☺