THE FUNDAMENTAL THEOREM OF ALGEBRA

DAVID GLYNN

1. Introduction

Theorem 1.1. *Every non-constant polynomial with complex coefficients has at least one root in the field of complex numbers.*

The above theorem is known as the Fundamental Theorem of Algebra. It is a theorem which has garnered the contributions of some of the greatest names in mathematics such as Gauss, Cauchy, Liouville and Laplace. With all this interest, it is unsurprising that numerous proofs of the theorem have been discovered. The proof in this report is an elegant and comparably short argument which appears in [1, Chapter 19]. There is also a discussion of a topological approach to proving the theorem, as given by Peter Phelan during his talk.

2. Important Preliminary Facts

First we shall establish some important facts necessary to complete the proof. They are generally covered in a first-year analysis course and so the proofs are omitted.

(1) Polynomials are continuous functions.
(2) Let $z \in \mathbb{C}$ have absolute value 1. Then for any positive integer m there exists $\zeta \in \mathbb{C}$ with $\zeta^m = z$. ζ is called the m-th root of unity of z.
(3) A continuous function f on a compact set S attains a minimum in S.

Now we proceed to the first step of our argument, a proof of what is commonly known as d'Alembert's Lemma.

3. d'Alembert's Lemma

Let $p(z) = \sum_{k=0}^{n} c_k z^k$ be a complex polynomial of degree $n \geq 1$.

Lemma 3.1 (d'Alembert)**.** *If $p(a) \neq 0$ then every disk D around a contains an interior point b with $|p(b)| < |p(a)|$.*

Proof. Suppose the disk D has radius R. Therefore all points in the interior of D are of the form $a + w$ with $|w| < R$. First we shall demonstrate the following

$$p(a+w) = p(a) + cw^m(1 + r(w)), \tag{1}$$

where c is a nonzero complex number, $1 \leq m \leq n$, and $r(w)$ is a polynomial of degree $n - m$ without constant term.

Using the binomial theorem, we get

$$\begin{aligned}
p(a+w) &= \sum_{k=0}^{n} c_k(a+w)^k = \sum_{k=0}^{n} c_k \sum_{i=0}^{k} \binom{k}{i} a^{k-i} w^i \\
&= \sum_{i=0}^{n} (\sum_{k=i}^{n} \binom{k}{i} c_k a^{k-i}) w^i \quad \text{(Rewriting the double summation)} \\
&= \sum_{k=0}^{n} c_k a^k + \sum_{i=1}^{n} (\sum_{k=i}^{n} \binom{k}{i} c_k a^{k-i}) w^i \quad \text{(Taking out the } i=0 \text{ part)} \\
&= p(a) + \sum_{i=1}^{n} d_i w^i
\end{aligned}$$

Let $m = \min\{i \geq 1 : d_i \neq 0\}$, set $c = d_m$ and factor cw^m out to get

$$p(a+w) = p(a) + cw^m(1 + r(w))$$

The next step is to bound $|cw^m|$ and $|r(w)|$ from above.
Let $\rho_1 := \sqrt[m]{|p(a)/c}$, so if $|w| < \rho_1$ then $|cw^m| < |p(a)|$.
Also since $r(w)$ is continuous and $r(0) = 0$, we know that there exists ρ_2 such that $|r(w)| < 1$ whenever $|w| < \rho_2$.
Hence for $|w|$ less than $\rho = \min(\rho_1, \rho_2)$ we have

$$|cw^m| < |p(a)| \qquad \Big(\Rightarrow \frac{|cw^m|}{|p(a)|} < 1 \Big) \tag{2}$$

$$|r(w)| < 1 \tag{3}$$

Now consider the quantity $-\frac{p(a)/c}{|p(a)/c|}$. Clearly it has absolute value 1, so there exists $\zeta \in \mathbb{C}$ with $\zeta^m = -\frac{p(a)/c}{|p(a)/c|}$.
Let $\epsilon \in \mathbb{R}$ satisfy $0 < \epsilon < \min(\rho, R)$. Setting $w_0 = \epsilon\zeta$, consider the point $b = a + w_0$. The point b is in D since $|w_0| = \epsilon < R$, and we claim that it satisfies $|p(b)| < |p(a)|$. By (1) we have,

$$|p(b)| = |p(a+w_0)| = |p(a) + cw_0^m(1 + r(w_0))|, \tag{4}$$

Now define a factor δ by

$$cw_0^m = c\epsilon^m\zeta^m = -\frac{\epsilon^m}{|p(a)/c|}p(a) = -\delta p(a),$$

by (2) our δ satisfies

$$0 < \delta = \epsilon^m \frac{|c|}{|p(a)|} < 1 \text{ , since } \epsilon < \rho$$

Using the triangle inequality we get for the right-hand term of (4)

$$\begin{aligned}
|p(a) + cw_0^m(1 + r(w_0))| &= |p(a) - \delta p(a)(1 + r(w_0))| \\
&= |(1-\delta)p(a) - \delta p(a) r(w_0)| \\
&\leq (1-\delta)|p(a)| + \delta|p(a)||r(w_0)| \\
&< (1-\delta)|p(a)| + \delta|p(a)| = |p(a)|
\end{aligned}$$

where we have used (3) to get the strict inequality. Thus we have arrived at the desired result

$$|p(b)| < |p(a)|$$

□

4. Proof of the Fundamental Theorem

Now that we have established the validity of d'Alembert's Lemma, the proof of the theorem follows quite quickly. First we note that $|p(z)|$ goes to infinity as $|z| \to \infty$. Clearly, $p(z)z^{-n} = \sum_{k=0}^{n} c_k z^{k-n}$ approaches the leading coefficient c_n as $|z| \to \infty$. Therefore $|p(z)|$ must go to infinity as $|z| \to \infty$. Consequently, there exists $R > 0$ such that $|p(z)| > |p(0)|$ for all points z on the circle $\{z : |z| = R\}$. Since $p(z)$ is continuous and the disk $D = \{z : |z| \leq R\}$ is compact, $|p(z)|$ attains a minimum value at some $z_0 \in D$. Because $|p(z)| > |p(0)|$ for all z on the boundary of D, z_0 must lie in the interior. But by d'Alembert's Lemma we know that in any disk around $z_0 \in D^{\mathrm{o}}$ we can find a point z_1 with $|p(z_1)| < |p(z_0)|$, so long as $|p(z_0)| \neq 0$. This would be a contradiction to the minimality of $|p(z_0)|$, so we must have that $p(z_0) = 0$.

5. A topological argument

The following argument was outlined at the end of Peter Phelan's talk, and draws on elements from topology.

First, we need to introduce the concept of the winding number of a closed curve. The winding number of a closed curve around a given point is an integer representing the total number of times that curve travels anti-clockwise around the point. The sign of the number depends on the orientation of the curve, it is negative if the curve travels clockwise around the point. For example, the winding number of $z(t) = e^{it}, 0 \leq t \leq 2\pi$ is 1 while the winding number of $z(t) = e^{-it}, 0 \leq t \leq 4\pi$ is -2.

Now suppose that the polynomial $p(z)$ has no roots, $p(z) \neq 0$ for all $z \in \mathbb{C}$. We will think of $p(z)$ as a map from the complex plane to the complex plane. It maps any circle $C = \{z \in \mathbb{C} : |z| = R\}$ to a closed curve γ_R.

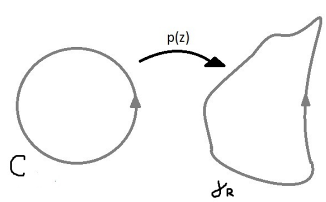

Figure 1. A circle mapped to a closed curve in $\mathbb{C}$

What happens to the winding number of γ_R when R is very large and when $R = 0$? When R is sufficiently large, the leading term z^n dominates all other terms in $p(z)$. The curve $z(\theta) = Re^{i\theta}$ $(0 \leq \theta \leq 2\pi)$ revolves once anti-clockwise around the origin, so it has a winding number of 1 around $(0, 0)$. Therefore $z(\theta)^n = Re^{in\theta}$ revolves n times anti-clockwise around the origin, so it has a winding number of n around $(0, 0)$. For sufficiently large R, γ_R also winds n times around the origin, as the leading term dominates all other terms. If $|z| = 0$, then γ_0 is simply the point $p(0)$, which we assumed is nonzero. Therefore the winding number of γ_0 around the origin is 0. If we change R continuously then γ_R will deform continuously. However we know that at some R the winding number must change, which only happens if the curve γ_R includes the origin $(0, 0)$. But then for some z_0 on the circle $|z| = R$ we have $p(z_0) = 0$. This contradicts our assumption that $p(z)$ has no roots, so it must have at least one.

References

[1] Martin Aigner and Gunter M. Ziegler. Proofs from The Book. Springer-Verlag, Berlin, fifth edition, 2014. Including illustrations by Karl H. Hofmann.