The Fundamental Theorem of Algebra

Problems from the History of Mathematics

Lecture 10 — February 23, 2018

Brown University

Statement of the FTOA

The Fundamental Theorem of Algebra is the following statement:

Theorem:

Every polynomial in $\mathbb{C}[z]$ of degree n has exactly n roots in $\mathbb{C}$.

This phrasing is certainly anachronistic. There are earlier versions of this theorem would make the claim just for polynomials in $\mathbb{R}[z]$, or that:

Theorem:

Every polynomial in $\mathbb{R}[z]$ factors uniquely into a product of linear and quadratic polynomials in $\mathbb{R}[z]$.

Counting Solutions to Polynomial Equations: A Recap

Progress towards the FTOA can be thought of as occurring in two steps:

1. Estimating the number of roots for a polynomial of degree n
2. Realizing that $\mathbb{C}$ was 'large enough' to solve all equations.[1]

For (1), it was known to the Greeks that quadratics could have up to two solutions. Omar Khayyam observed that cubics could have multiple roots, and Vieté (1540-1603) constructed polynomials of degree n with n roots.

Polynomial division can be used to derive the following theorem:

Theorem (Harriot, popularized by Descartes in 1632):

If x is a root of $f(z)$, then $f(z) = (z - x)q(z)$ for some polynomial $q(z)$ of degree $\deg(f) - 1$.

It follows that a polynomial of degree n has at most n roots.

[1] In other words, that $\mathbb{C}$ is algebraically closed.

Are Complex Numbers Enough?

Realizing that $\mathbb{C}$ was algebraically closed would take a lot more work.

Here, bear in mind that complex numbers were not used in calculations until Cadano's *Ars Magna* in 1545 and the rules for their manipulation were not laid out until Bombelli's *l'Algebra* in 1572.

Most assumed that roots should exist in a general enough sense[2] but did not believe that complex numbers could account for all of them.

Example: Liebniz claimed in 1702 that $z^4 + 1$ could not be written as a product of quadratic factors. (This is equivalent to the claim $\sqrt{i} \notin \mathbb{C}$.) Euler countered this claim in correspondence with Daniel Bernoulli and Goldbach in 1742:

$$z^4 + 1 = (z^2 + \sqrt{2}z + 1)(z^2 - \sqrt{2}z + 1).$$

[2]Albert Girard (1595-1632) conjectured that $f(z)$ of degree n should have n roots in 1629.

Failed Proofs

d'Alembert's Proof

d'Alembert published two versions of a proof of the FTOA. His basic idea was to consider the equation

$$F(x, y) := a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + y = 0$$

and prove that $F(x, y)$ had a root for every choice of y. It certainly does for $y = 0$, and he claimed you could invert $F(x, y)$ to solve for $y = y(x)$ in a neighborhood of $x = 0$.

d'Alembert uses this to prove the following Lemma:

d'Alembert's Lemma (Argand, 1806):

If $f(z_0) \neq 0$, there exists a point z_1 near z_0 with $|f(z_1)| < |f(z_0)|$.

This work ultimately assumed the FTOA and would not be justified until the introduction of Puiseux series in 1850.

Euler's Proof

Euler believed in the validity of d'Alembert's proof but wanted a purely algebraic one. In his work, the FTOA follows from the following claim:

"Theorem" (Euler, 1748):

Fix $k > 0$. Any real polynomial of degree 2^{k+1} factors as a product of real polynomials of degrees 2^k.

Euler's idea is to 'depress' the polynomial $f(z) = z^{2n} + a_{2n-2}z^{2n-2} + \dots$ and factor $f(z)$ as

$$(z^n + tz^{n-1} + b_{n-2}z^{n-2} \dots + b_0)(z^n - tz^{n-1} + c_{n-2}z^{n-2} \dots + c_0).$$

The new coefficients are rational functions of t, a_j and are understable.

Lagrange (1772) pointed out some flaws in the general case of Euler's proof involving rational functions in indeterminate forms. Lagrange made a new version using his knowledge of root permutations. (But his work assumed the existence of roots to permute.)

Euler's Proof in the Quartic Case

The only case that Euler wrote down in any detail was that of quartics. Here, we have

$$z^4 + a_2 z^2 + a_1 z + a_0 = (z^2 + tz + b_0)(z^2 - tz + c_0).$$

Equating coefficients gives three relations:

$$a_2 = c_0 - b_0 - t^2, \quad a_1 = t(c_0 - b_0), \quad a_0 = b_0 c_0.$$

Substitution gives a cubic equation in t^2. Applying the cubic formula, we solve for t and use it to obtain b_0 and c_0.

Two Notes on Euler's Solution

1. It's not surprising that the only case Euler could write down in detail is the only case in which a solution is obtainable by radicals. Only by the time of Lagrange (1772) were higher order polynomials thought insoluble by radicals.

2. Euler wants a factorization over the reals, which means we need t to be the real root of the cubic. This is fine in degree three (because of the cubic formula) but the general existence of real roots for odd degree polynomials requires some form of the Intermediate Value Theorem.[3]

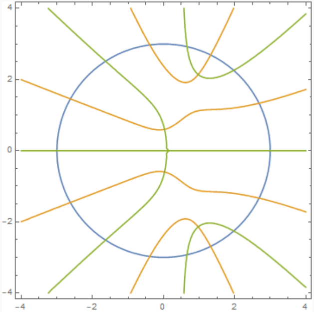
[3] Proven as a consequence of Bolzano's Theorem in 1817. The proof, while good for its time, is no longer considered rigorous.

Gauss' Proof

Gauss is usually credited with the earliest proof of the FTOA. His proof appears in his 1799 doctoral thesis and is topological in nature.

The rough outline follows:

1. The equations $\mathrm{Re} f(z) = 0$ and $\mathrm{Im} f(z) = 0$ describe contours in $\mathbb{C}$.
2. For large R, each intersects the circle of radius R in $2 \deg f$ points.
3. These intersections alternate.
4. The contours must cross between intersections with the circle.



$z^4 - 2z^3 + 6z^2 - z + 2$

$\mathrm{Im} f(z) = 0$; $\mathrm{Re} f(z) = 0$

But Gauss fails to prove that *an algebraic curve which enters a disk must leave it.* This would not be proven until 1920.

Argand's Proof

The oldest proof of the FTOA *without gaps* is due to Argand in 1814. Argand builds on the work of d'Alembert and considers the global minimum of $|f(z)|$ as z varies in $\mathbb{C}$.

If z_0 produces a non-zero minimum, consider

$$f(z_0 + \zeta) = \sum_{k=0}^{n} a_k (z_0 + \zeta)^k = f(z_0) + \sum_{k=1}^{n} b_k \zeta^k.$$

It then suffices to choose ζ such that $|f(z_0 + \zeta)| < |f(z)|$. But the correction term is $b_1\zeta + O(\zeta^2)$, which (as a vector) can point in any direction as ζ varies.[4]

Choosing ζ to oppose the direction of $f(z_0)$ gives a contradiction.

[4] I've simplified. The actual proof would have been more explicit.

Post-Mortem

In 1816, Gauss published a second proof of the FTOA using a variant of Euler's (factorization-based) proof. However, instead of working with roots which may or may not exist, Gauss works with indeterminates.[5]

The advantage with working with indeterminates is that you may avoid assuming the existence of roots. At the time, people believed in a large hierarchy

$$\mathbb{R} \subset \mathbb{C} \subset \dots$$

and it was not clear how deep you'd have to go to get roots.

Gauss called these quanitities shadows of shadows, etc.

[5] Gauss' second proof is correct.

Quaternions

Hamilton discovered the quaternions in 1843 while searching for these generalized roots. Defined as

$$\{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}, i^2 = j^2 = k^2 = ijk = -1\},$$

the quaternions form the unique four-dimensional associative normed division algebra over the reals.

Hamilton's original motivation was in modeling points in $\mathbb{R}^3$. Hamilton experimented with three-dimensional algebras for a long time but could not model multiplication and division in them. (There do not exist three-dimensional $\mathbb{R}$-algebras.)

Questions?