

Article

Not peer-reviewed version

A Recurrent Proof of the Fundamental Theorem of Algebra

[Vincenzo Manca](#)*

Posted Date: 15 August 2024

doi: 10.20944/preprints202408.1127.v1

Keywords: Fundamental Theorem of Algebra; Recurrent Equation; Polynomial Coefficient Function; Complex Hyperspace



Preprints.org is a free multidiscipline platform providing preprint service that is dedicated to making early versions of research outputs permanently available and citable. Preprints posted at Preprints.org appear in Web of Science, Crossref, Google Scholar, Scilit, Europe PMC.

Copyright: This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Disclaimer/Publisher's Note: The statements, opinions, and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.

Article

A Recurrent Proof of the Fundamental Theorem of Algebra

Vincenzo Manca

University of Verona (Italy); vincenzo.manca@univr.it

Abstract: The *Polynomial coefficient function* F^n , from \mathbb{C}^n in itself, is given by the function F^n that provides the coefficients of the polynomial $(x - a_1)(x - a_2) \dots (x - a_n)$: $F^n = \lambda_{a_1, a_2, \dots, a_n} \cdot (b_1, b_2, \dots, b_n) : \prod_{i=1, n} (x - a_i) = x^n + b_1 x^{n-1} + b_2 x^{n-2} + \dots + b_n$. A proof of the fundamental theorem of algebra is given where the surjectivity of this function is obtained from a *Recurrent Coefficient Equation*.

Keywords: fundamental theorem of algebra; recurrent equation; polynomial coefficient function; complex hyperspace

1. Introduction

The fundamental theorem of algebra (FTA) asserts that any polynomial with complex coefficients has a root in the field of complex numbers. In a different form, it was stated by Albert Girard in 1629 and René Descartes in 1637. Colin MacLaurin and Leonard Euler gave a formulation, that is proven equivalent to the previous one. According to FTA, any polynomial with real coefficients can be decomposed into a product of linear and quadratic factors with real coefficients. In modern terms, the theorem says that the field \mathbb{C} of complex numbers is algebraically closed (a polynomial with coefficient in \mathbb{C} has solutions in \mathbb{C}). Tentatives of proof were given by d'Alembert (1746), Euler, Laplace, Lagrange, and others in the second half of the 18th century. Carl Friedrich Gauss was the first to prove the theorem in an almost complete way. He gave four different proofs, the first in 1799 and the last in 1849 (almost at the end of his life). He was never satisfied with his proofs. Namely, the theorem involves some form of topological properties, not rigorously defined in Gauss' time, related to the completeness of complex numbers (having the limits of all their Cauchy sequences). Many proofs are available now, deduced by algebraic, topological, and complex analysis arguments. (see [1–6] for detailed accounts of the history and proofs of the theorem). We recall that: i) \mathbb{C}^n is the product of n copies of the complex plane; ii) according to the Heine-Borel theorem [7,8], any bounded and closed set of \mathbb{C}^n is a compact set; iii) for any continuous function f from \mathbb{C}^n into \mathbb{C}^n , the image of a compact set is a compact set too; iv) the image of the frontier ∂X of a compact subset X of \mathbb{C}^n coincides with the frontier of the image $f(X)$ (the images of internal points of X are internal points of the image).

2. A Proof Based on the Polynomial Coefficient Function

A formulation of the fundamental theorem of algebra is the following.

Theorem 1. For any polynomial $P(x)$ of degree $n > 0$, with complex coefficients, there are $a_1, a_2, \dots, a_n \in \mathbb{C}$, such that $P(x) = (x - a_1)(x - a_2) \dots (x - a_n)$.

This formulation is equivalent to claim the surjectivity of the *Polynomial coefficient function* F^n :

$$F^n : \mathbb{C}^n \rightarrow \mathbb{C}^n.$$

Namely, if F^n is surjective, then we can conclude that the complex coefficients of any n -th-degree polynomial are the image of the *Polynomial coefficient function* applied to n complex numbers (the polynomial roots).

In symbols, if F^n is surjective and $P(x) = b_0x^n + b_1x^{n-1} + b_2x^{n-2} + \dots + b_n$ there exists a vector (a_1, a_2, \dots, a_n) such that $(b_1/b_0, b_2/b_0, \dots, b_n/b_0) = F^n(a_1, a_2, \dots, a_n)$, that is:

$$P(x) = (x - a_1)(x - a_2) \dots (x - a_n).$$

In a sense, the function F^n inverts the equation-solving process in that of equation-making. Of course, F^n is easy to compute from the roots, while equation-solving is, in general, very difficult to obtain (F^n is a *one-way encoding*). Here we develop a proof of F^n surjectivity by combining basic notions of general topology in hyperspaces of any finite dimension over complex numbers and a recurrent equation holding for F^n .

Theorem 2. $F^n : \mathbb{C}^n \rightarrow \mathbb{C}^n$ is surjective.

Proof.

Let us fix a value for n , the arguments we develop apply to any value of n . For the sake of brevity, in the following, we drop the exponent n of the function F^n that provides the coefficients of the polynomial $(x - a_1)(x - a_2) \dots (x - a_n)$.

It is easy to verify that coefficients b_1, b_2, \dots, b_n are respectively given by the functions:

$$\begin{aligned} F_1(a_1, a_2, \dots, a_n) &= -(a_1 + a_2 + \dots + a_n) = b_1 \\ F_2(a_1, a_2, \dots, a_n) &= + \sum (a_i a_j)_{i < j = 1, \dots, n} = b_2 \\ F_3(a_1, a_2, \dots, a_n) &= - \sum (a_i a_j a_k)_{i < j < k = 1, \dots, n} = b_3 \\ &\dots \dots \dots \\ F_n(a_1, a_2, \dots, a_n) &= (-1)^n (a_1 a_2 \dots a_n) = b_n. \end{aligned} \tag{1}$$

Of course, functions F_k , for $k = 1, 2, \dots, n$, are continuous, therefore also $F = (F_1, F_2, \dots, F_n)$ is continuous. However, F is not injective because permutations of the same vector will provide the same F image.

Let $u = (1, i)$ and $(0, 0) = \mathbf{0}$. For $k = 1, 2, \dots, n$ with m a natural number greater than 1, we call z_k m -pair the hyperplane pairs of \mathbb{C}^n :

$$z_k = -mu, z_k = mu.$$

The z_k m -pairs, for $k = 1, 2, \dots, n$, determine the portions of the space between them. The set of points between all the z_k pairs mutually orthogonal defines, for every m , the H_m n -cubic m -block centered on the origin $\mathbf{0}^n$ of \mathbb{C}^n :

$$H_m = \{(z_1, z_2, \dots, z_n) \mid -mu \leq z_k \leq mu, k = 1, 2, \dots, n\}.$$

where \leq is the partial order over complex numbers $x + iy \leq x' + iy'$ if $x \leq x'$ e $y \leq y'$ (which extends to \mathbb{C}^n applying the condition on all the components). The family $\mathcal{H} = (H_m \mid m \in \mathbb{N}, m > 0)$ provides a covering of the hyperspace \mathbb{C}^n .

The block H_m has 2^n vertices, and the vertex (mu, mu, \dots, mu) is called the superior vertex, while $(-mu, -mu, \dots, -mu)$ is called the inferior vertex. The remaining vertices are $(\pm mu, \pm mu, \dots, \pm mu)$ for all possible choices of signs $+$ or $-$ in any component.

The image $F(H_m) = \{(F_k(Z) \mid k = 1, 2, \dots, n) \mid Z \in H_m\}$ is a compact set of \mathbb{C}^n because H_m is compact and F is continuous (which sends compacts into compacts). Moreover, in \mathbb{C}^n any closed and bounded set is compact (Heine-Borel's theorem). The image $F(H_m)$ of H_m has $(n + 1)$ vertices:

$$\begin{aligned} Z_0 &= F(mu, mu, \dots, mu) \\ Z_1 &= F(-mu, mu, \dots, mu) \\ Z_2 &= F(-mu, -mu, \dots, mu) \\ &\dots\dots\dots \\ Z_n &= F(-mu, -mu, \dots, -mu) \end{aligned}$$

We know that a metric complete space such as \mathbb{C}^n contains all the limits of Cauchy sequences in the space, and any closed subset of the space, is complete [7,8]. Therefore, for any closed and bounded set X of \mathbb{C}^n , $F(\partial X) = \partial F(X)$.

Let $\rho(F(H_m))$ be the radius of $F(H_m)$, as the minimum norm (distance from the origin) reached by the points of the frontier $\partial F(H_m)$ of $F(H_m)$.

We will prove that, for $E \in \partial H_m$, $\|F(E)\| \geq \|mu\| - 1$. This means that for increasing values of m the radius of $F(H_m)$ grows illimitably so that any vector in \mathbb{C}^n is an image of F , whence the surjectivity of F follows.

In the following, we use $n + 1$ rather than n (with no loss of generality because n is a generic value, and the theorem we are proving holds trivially for $n = 1$).

Let $a \in \mathbb{C}$, we denote by $[a, E]$ the vector of \mathbb{C}^{n+1} extending $E \in \mathbb{C}^n$, such that:

$$[a, E]_1 = a$$

and, for $k = 1, \dots, n$:

$$[a, E]_{k+1} = E_k.$$

Symmetrically, for $k = 1, \dots, n$:

$$[E, a]_k = E_k$$

and:

$$[E, a]_{n+1} = a.$$

The following equations easily derive from the definition (1) of F , for $k = 0, \dots, n$, with $F_0(E) = 1$ and $F_{n+1}(E) = 0$:

$$F_{k+1}([a, E]) = -aF_k(E) + F_{k+1}(E). \quad (2)$$

which explicitly gives all the following equations:

$$\begin{aligned} F_1([a, E]) &= -a + F_1(E) \\ F_2([a, E]) &= -aF_1(E) + F_2(E) \\ &\dots\dots\dots \\ F_n([a, E]) &= -aF_{n-1}(E) + F_n(E) \\ F_{n+1}([a, E]) &= -aF_n(E). \end{aligned} \quad (3)$$

Then, from the definitions of $[a, E]$, $[E, a]$, the equations above are synthesized, for any $a \in \mathbb{C}$, and $a \neq 0$, by the **Recurrent Coefficient Equation**:

$$F([a, E]) = -a[1, F(E)] + [F(E), 0]. \quad (4)$$

Now, let $E \in \partial H_m \subset \mathbb{C}^{n+1}$, then we can suppose with no loss of generality (the order of components is not relevant in the determination of the F -image) that $E = [a_1, A_n]$, with $A_n = (a, a_2, \dots, a_n)$ where $-mu \leq a \leq mu$ and $a_i = \pm mu$, for $i = 1, 2, \dots, n$, that is, E is a point of the edge between vertices $(a_1, mu, a_2, \dots, a_n)$ and $(a_1, -mu, a_2, \dots, a_n)$ of H_m . According to the Recurrent Coefficient Equation (4) the following inequalities hold, which give a lower bound of the radius $\rho(F(H_m))$:

$$\|F(E)\| = \|F([\pm mu, A_n])\| = \|\mp mu[1, F(A_n)] + [F(A_n), 0]\| \geq \quad (5)$$

$$\geq \|mu[1, F(A_n)]\| - \|[1, F(A_n)]\| \quad (6)$$

$$= (\|mu\| - 1)\|[1, F(A_n)]\| > \|mu\| - 1. \quad (7)$$

In conclusion, the radius of $F(H_m)$ grows with m , therefore any of the blocks of \mathcal{H} (which is a covering of \mathbb{C}^{n+1}) is included in the image of some block of \mathcal{H} . Then, F is surjective.

References

1. Arnold, B.H.: A topological proof of the fundamental theorem of algebra. *Amer. Math. Monthly*, 56, 465-466 (1949)
2. Courant, R., Robbins, H.: *What is Mathematics*. Oxford University Press, 2nd Edition (1941)
3. Dunham, W.: Euler and the Fundamental Theorem of Algebra, *The College Mathematics Journal*, 22, 4, 282-293 (1991)
4. https://en.wikipedia.org/wiki/Fundamental_theorem_of_algebra
5. Kline, M.: *Mathematical Thought from Ancient to Modern Times*, Oxford University Press (1972)
6. Lang, S.: *Algebra*, Addison-Wesley (1974)
7. Dugundji, J. *Topology*, Allyn & Bacon (1966)
8. Kelley, J. L.: *General Topology*. D. van Nostrand Company (1975)

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.