An Alternative Proof of the Fundamental Theorem of Algebra

Darshan P.
Independent Researcher and Computer Programming Specialist
drshnp@bayesiancorp.com

1734236220

Abstract

This note presents an alternative proof of the Fundamental Theorem of Algebra. Specifically, we show that the degree of an *irreducible* polynomial in $\mathbb{R}[X]$ is either 1 or 2. The argument then extends naturally to $\mathbb{C}[X]$, where every irreducible polynomial must have degree 1. For background on classical approaches to the theorem, see [1, 2].

1 Proof setup

Let $n > 1$ be an integer and let $P \in \mathbb{R}[X]$ be an irreducible polynomial of degree n. We claim that $n = 2$. Denote by $\langle P \rangle$ the ideal generated by P in $\mathbb{R}[X]$. Because P is irreducible, the quotient ring $\mathbb{R}[X]/\langle P \rangle$ is a field. Define

$$\psi : \mathbb{R}^n \longrightarrow \mathbb{R}[X]/\langle P \rangle, \quad (a_0, \ldots, a_{n-1}) \longmapsto a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + \langle P \rangle.$$

Then ψ is a group isomorphism from $(\mathbb{R}^n, +)$ onto $(\mathbb{R}[X]/\langle P \rangle, +)$. Via ψ we transport the field structure of the quotient to $\mathbb{R}^n$: addition coincides with the usual vector addition, and we denote the product of $x, y \in \mathbb{R}^n$ by $x \cdot y$. The multiplicative identity is written 1. Because the transported product is bilinear, the map $\mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$, $(x, y) \mapsto x \cdot y$ is continuous.

2 Proof

Fix any norm $\|\cdot\|$ on the underlying real vector space $\mathbb{R}^n$ such that $\|1\| = 1$, and set

$$\|x\| \;=\; \sup_{\|y\|=1} |x \cdot y|, \qquad x \in \mathbb{R}^n.$$

That is, $\|x\|$ is the operator norm of the endomorphism $y \mapsto x \cdot y$. It satisfies $\|1\| = 1$ and $\|x \cdot y\| \leq \|x\| \, \|y\|$ for all $x, y \in \mathbb{R}^n$.

The exponential and logarithm series

$$\sum_{k=0}^{\infty} \frac{x^k}{k!}, \qquad \sum_{k=1}^{\infty} \frac{(-1)^{k+1}(x-1)^k}{k},$$

are absolutely and locally uniformly convergent with respect to this norm; the first on all of $\mathbb{R}^n$ and the second on the open ball $\{x \in \mathbb{R}^n : \|x - 1\| < 1\}$. We write $e(x)$ and $\ln(x)$ for their respective sums. Because the product on $\mathbb{R}^n$ is commutative, one checks

$$e(x+y) = e(x) \cdot e(y) \qquad (x, y \in \mathbb{R}^n). \tag{1}$$

Moreover $e(x) \neq 0$ since $e(x) \cdot e(-x) = e(0) = 1$. Thus

$$e : (\mathbb{R}^n, +) \longrightarrow (\mathbb{R}^n \setminus \{0\}, \cdot)$$

is a continuous group homomorphism.

Exactly as in the matrix case (see [3, Sec. 2.1] or [4, Sec. 4B]), one shows that

$$e\bigl(\ln x\bigr) = x \quad \text{and} \quad \ln\bigl(e(x)\bigr) = x \tag{2}$$

whenever $\|x - 1\| \leq 1$.

From (1) we deduce that if V is any neighbourhood of 0, then $e(V)$ is a neighbourhood of 1; hence e is an *open* mapping. Consequently e is surjective: if $G = e(\mathbb{R}^n)$, then G is an open subgroup of $\mathbb{R}^n \setminus \{0\}$, and the complement of G is also open; because $\mathbb{R}^n \setminus \{0\}$ is connected, that complement must be empty.

It follows from (2) that $\ker(e)$ is discrete, and it is well known (see [4, Chap. 7, Sec. 1.1] or [2, Sec. 1.12]) that, unless $\ker(e) = \{0\}$, there exist linearly independent vectors $v_1, \ldots, v_m \in \mathbb{R}^n$ ($m \geq 1$) such that $\ker(e) = \bigoplus_{k=1}^m \mathbb{Z}v_k$. Because e is open, it induces a homeomorphism from $\mathbb{R}^n / \ker(e)$which is homeomorphic to $(S^1)^m \times \mathbb{R}^{n-m}$onto $\mathbb{R}^n \setminus \{0\}$. But for $n \geq 2$ the punctured space $\mathbb{R}^n \setminus \{0\}$ is simply connected, whereas $(S^1)^m \times \mathbb{R}^{n-m}$ is *not* simply connected when $1 \leq m \leq n$. To avoid a contradiction we must have $\ker(e) = \{0\}$.

Hence $\mathbb{R}^n \setminus \{0\}$ would be homeomorphic to $\mathbb{R}^n$, which is impossible: in $\mathbb{R}^n$ every compact set K is contained in another compact set whose complement is connected, whereas this fails in $\mathbb{R}^n \setminus \{0\}$ (take $K = S^{n-1}$, the unit sphere). Therefore $n = 2$, completing the proof.

References

[1] J. L. Lehman, *Quadratic Number Theory: An Invitation to Algebraic Methods in the Higher Arithmetic*, North Star Publishing, 2004.

[2] M. H. Weissman, *An Illustrated Theory of Numbers*, American Mathematical Society, 2017.

[3] R. A. Horn and C. R. Johnson, *Matrix Analysis*, 2nd ed., Cambridge University Press, 2012.

[4] A. Hatcher, *Algebraic Topology*, Cambridge University Press, 2002.