Another Proof of the Fundamental Theorem of Algebra

José Carlos de Sousa Oliveira Santos

American Mathematical Monthly, January 2005

The goal of this note is to prove the fundamental theorem of algebra. To be more precise, we show that the degree of an irreducible polynomial in $\mathbb{R}[X]$ is either 1 or 2. The same method can be used to prove that the degree of an irreducible polynomial in $\mathbb{C}[X]$ is always 1.

Let n be an integer larger than 1, and let P be an irreducible polynomial in $\mathbb{R}[X]$ of degree n. We assert that $n = 2$. Denote by $\langle P \rangle$ the ideal generated by P in the ring $\mathbb{R}[X]$. Since P is irreducible, the quotient of the ring $\mathbb{R}[X]$ by $\langle P \rangle$ is a field. If we define $\psi : \mathbb{R}^n \longrightarrow \mathbb{R}[X]/\langle P \rangle$ by

$$(a_0, a_1, \ldots, a_{n-1}) \mapsto a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + \langle P \rangle,$$

then ψ is a group isomorphism from $(\mathbb{R}^n, +)$ onto $(\mathbb{R}[X]/\langle P \rangle, +)$. This isomorphism induces in the obvious way a field structure in $\mathbb{R}^n$, the addition being the usual one. The product of two elements x and y of $\mathbb{R}^n$ is denoted by $x \cdot y$, and the identity element for the product is denoted by 1. The product, which is a bilinear function from $\mathbb{R}^n \times \mathbb{R}^n$ into $\mathbb{R}^n$, is continuous.

Let $|\cdot|$ be a norm in $\mathbb{R}^n$ (with respect to its usual real vector space structure) such that $|1| = 1$ and define

$$\|x\| = \sup_{|y|=1} |x \cdot y|$$

for each x in $\mathbb{R}^n$. This is just the norm of the endomorphism $y \mapsto x \cdot y$ of $\mathbb{R}^n$. Then $\|1\| = 1$ and $\|x \cdot y\| \leq \|x\|\|y\|$ holds for all x and y in $\mathbb{R}^n$. The series

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

are both absolutely and locally uniformly convergent with respect to this norm, the first one in $\mathbb{R}^n$ and the second one in $\{x \in \mathbb{R}^n \mid \|x-1\| < 1\}$. Their sums are denoted by $\exp(x)$ and $\log(x)$, respectively. Since the product is commutative, it is easy to prove that $\exp(x+y) = \exp(x) \cdot \exp(y)$ for all x and y in $\mathbb{R}^n$. Furthermore, we never have $\exp(x) = 0$, because $\exp(x) \cdot \exp(-x) = \exp(x-x) = \exp(0) = 1$. We have thus defined a continuous group homomorphism $\exp : (\mathbb{R}^n, +) \longrightarrow (\mathbb{R}^n \setminus \{0\}, \cdot)$.

It can be proved, just as it is in the case of matrices (see [1, sec. 2.1] or [3, sec. 4.B]), that

$$\exp\bigl(\log(x)\bigr) = x \quad (x \in \mathbb{R}^n,\ \|x-1\| < 1) \tag{1}$$

and

$$\log\bigl(\exp(x)\bigr) = x \tag{2}$$

for any x in $\mathbb{R}^n$ such that $\|\exp(x)-1\|<1$.

It follows from (1) that, if V is a neighborhood of 0, then $\exp(V)$ is a neighborhood of 1. Therefore, since exp is also a group homomorphism, it is an open mapping. It can be deduced from this fact that exp is surjective. Indeed, if $G=\exp(\mathbb{R}^n)$, then G is an open subgroup of $(\mathbb{R}^n\setminus\{0\},\cdot)$, and if x belongs to $(\mathbb{R}^n\setminus\{0\})\setminus G$, then

$$G\cdot x\subset\left(\mathbb{R}^n\setminus\{0\}\right)\setminus G.$$

Accordingly, the complement of G in $\mathbb{R}^n\setminus\{0\}$ is also an open set. Therefore, since $\mathbb{R}^n\setminus\{0\}$ is connected, the complement of G must be empty. In other words, $\exp(\mathbb{R}^n)=\mathbb{R}^n\setminus\{0\}$.

It is a consequence of (2) that $\ker(\exp)$ is discrete, and it is well known (see [2, chap. 7, sec. 1.1] or [4, sec. 1.12]) that, unless $\ker(\exp)=\{0\}$, this implies the existence of linearly independent vectors $v_1,\dots,v_m$ in $\mathbb{R}^n$ ($m\geq 1$) such that $\ker(\exp)=\bigoplus_{k=1}^m\mathbb{Z}v_k$. A second application of the fact that exp is an open mapping shows that it induces a homeomorphism from $\mathbb{R}^n/\ker(\exp)$ (which is homeomorphic to $(S^1)^m\times\mathbb{R}^{n-m}$) onto $\mathbb{R}^n\setminus\{0\}$. But if $n>2$, the space $\mathbb{R}^n\setminus\{0\}$ would be 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, it would have to be the case that $\ker(\exp)=\{0\}$. Therefore, $\mathbb{R}^n\setminus\{0\}$ would be homeomorphic to $\mathbb{R}^n$. However, this is impossible. This can be proved using homology groups, and it also follows from the fact that in $\mathbb{R}^n$ every compact set K is a subset of some other compact set whose complement is connected, whereas in $\mathbb{R}^n\setminus\{0\}$ this is not true (consider, for instance, $K=S^{n-1}$, the unit sphere in $\mathbb{R}^n$). Therefore, $n=2$ and the theorem is proved.

References

1. A. Baker, *Matrix Groups: An Introduction to Lie Group Theory*, Springer-Verlag, Berlin, 2003

2. N. Bourbaki, *General Topology, Chapters 5–10*, Springer-Verlag, Berlin, 1998

3. M. L. Curtis, *Matrix groups*, 2nd ed., Springer-Verlag, Berlin, 1987

4. J. J. Duistermaat and J. A. C. Kolk, *Lie Groups*, Springer-Verlag, Berlin, 2000

Departamento de Matemática Pura, Faculdade de Ciências da Universidade do Porto, Rua do Campo Alegre 687, 4169–007 Porto, Portugal

jcsantos@fc.up.pt