Teorema Fundamental del Álgebra

Pedro Montero

Departamento de Matemática, Universidad Técnica Federico Santa María

El objetivo de esta nota es probar el Teorema Fundamental del Álgebra, enunciado por primera vez por Peter Roth en 1608, y cuya primera demostración rigurosa fue publicada en 1806 por Jean-Robert Argand.

Valparaíso, Abril 2020

Sea k un cuerpo y sea $k[X]$ el anillo de polinomios con coeficientes en k en la variable X. Decimos que k es **algebraicamente cerrado** si todo polinomio $P \in k[X]$ no-constante posee una raíz en k, es decir, existe $a \in k$ tal que $P(a) = 0$. Gracias a la división euclideana de polinomios, esto último es equivalente a que todo polinomio P no-constante posee exactamente $\mathrm{gr}(P)$ raíces en k, contándolas con múltiplicidad. Con este lenguaje, el **Teorema Fundamental del Álgebra** se enuncia de la siguiente manera.

Teorema. *El cuerpo $\mathbb{C}$ de los números complejos es algebraicamente cerrado.*

Demostración. Sea $P \in \mathbb{C}[X]$ polinomio no-constante, i.e., $\mathrm{gr}(P) \geq 1$. Sin pérdida de generalidad, podemos suponer que P es *unitario*, i.e., de la forma

$$P(X) = X^n + a_1 X^{n-1} + \ldots + a_n.$$

Supongamos por contradicción que $P(z) \neq 0$ para todo $z \in \mathbb{C}$. En particular, $P(0) = a_n \neq 0$.

Sea $|\cdot|$ la norma usual sobre $\mathbb{C}$, i.e., si $z = x + iy$ entonces $|z| = \sqrt{x^2 + y^2}$. Dado que $\lim\limits_{|z| \to \infty} |P(z)| = +\infty$, existe $R \in \mathbb{R}^{>0}$ tal que para todo $z \in \mathbb{C}$ tal que $|z| \geq R$ se tiene que $|P(z)| \geq a_n$. Notar que podemos tomar $R_0 := \max\{1, 2na\}$, donde $a = \max\limits_{i=1,\ldots,n} |a_i|$. En efecto, si $|z| \geq R_0$ y $d \in \{1, \ldots, n\}$ entonces $|z^d| \underbrace{\geq}_{R_0 \geq 1} |z| \geq 2na$, y luego

$$\left| \sum_{d=1}^{n} \frac{a_d}{z^d} \right| \leq \sum_{d=1}^{n} \frac{|a_d|}{2na} \leq \sum_{d=1}^{n} \frac{a}{2na} = \frac{1}{2}.$$

Dado que $|u + v| \geq |u| - |v|$, para $|z| \geq R_0$ se tiene que

$$|P(z)| = \underbrace{|z^n|}_{\geq 2na} \cdot \left| 1 + \sum_{d=1}^{n} \frac{a_d}{z^d} \right| \geq 2na \left(1 - \frac{1}{2} \right) = na \geq n|a_n| \geq |a_n|.$$

Sea $D = \{z \in \mathbb{C} \text{ tal que } |z| \leq R_0\}$ el disco de radio R_0 centrado en 0. Dado que D es un conjunto cerrado y acotado (i.e., compacto), el Teorema de Weierstraß asegura que la función continua $f(z) := |P(z)|$ alcanza su mínimo r_0 en D. Más aún, $r_0 > 0$ por hipótesis.

Notar además que para todo $z \notin D$ se tiene

$$f(z) = |P(z)| \geq |a_n| = |P(0)| \underbrace{\geq}_{0 \in D} r_0,$$

por lo que r_0 es un mínimo *global* de $f(z)$, i.e., $f(z) \geq r_0$ para todo $z \in \mathbb{C}$.

Sea $z_0 \in \mathbb{C}$ tal que $f(z_0) = r_0$. Luego de realizar el cambio de variable $z \mapsto z + z_0$ y definiendo $Q(z) = P(z_0)^{-1} P(z + z_0)$, podemos reducirnos al caso donde $z_0 = 1$ y donde $Q(0) = 1$ es el mínimo global de $g(z) := |Q(z)|$.

Notemos que Q es un polinomio de grado n, al igual que P. Denotemos por k el *orden de anulación* en 0 del polinomio $(Q - 1) \in \mathbb{C}[X]$, i.e.,

$$Q(X) - 1 = b_k X^k + \ldots + b_n X^n \Leftrightarrow Q(X) = 1 + b_k X^k + \ldots + b_n X^n,$$

donde $b_k \neq 0$ (por definición de orden de anulación) y $b_n \neq 0$ (por hipótesis).

Escribamos $b_k = re^{i\theta}$ con $r > 0$ y $\theta \in [0, 2\pi[$ y definamos para todo $\varepsilon \in \mathbb{R}^{>0}$

$$z_\varepsilon := \varepsilon e^{i(\pi-\theta)/k}.$$

Dado que $z_\varepsilon^k = \varepsilon^k e^{i(\pi-\theta)} = \varepsilon^k \underbrace{e^{i\pi}}_{=-1} e^{-i\theta} = -\varepsilon^k e^{-i\theta}$, tenemos que $b_k z_\varepsilon^k = re^{i\theta}(-\varepsilon^k e^{-i\theta}) = -r\varepsilon^k$, y luego

$$Q(z_\varepsilon) = 1 - r\varepsilon^k + \varepsilon^k h(\varepsilon), \quad \text{donde } h(\varepsilon) = -e^{-i\theta} \sum_{j=1}^{n-k} b_{k+j} z_\varepsilon^j = -e^{-i\theta}(b_{k+1}z_\varepsilon + \ldots + b_n z_\varepsilon^{n-k}).$$

Dado que $\lim\limits_{\varepsilon \to 0} \varepsilon^k = 0$ y $\lim\limits_{\varepsilon \to 0} h(\varepsilon) = 0$, existe $\varepsilon_0 \in]0, 1[$ tal que para todo $\varepsilon \in]0, \varepsilon_0]$ se tiene que

$$r\varepsilon^k < 1 \text{ y } |h(\varepsilon)| \leq \frac{r}{2},$$

de donde se deduce que

$$|Q(z_{\varepsilon_0})| = |1 - r\varepsilon_0^k + \varepsilon_0^k h(\varepsilon_0)| \leq |1 - r\varepsilon_0^k| + \frac{r}{2}\varepsilon_0^k = 1 - r\varepsilon_0^k + \frac{r}{2}\varepsilon_0^k = 1 - \frac{r}{2}\varepsilon_0^k < 1,$$

lo cual contradice el hecho que $1 = Q(0)$ es el mínimo global de $g(z) = |Q(z)|$. Así, concluímos que necesariamente $P \in \mathbb{C}[X]$ posee una raíz en $\mathbb{C}$. $\square$