ÁLGEBRA LINEAL.

DESCOMPOSICIÓN DE POLINOMIOS.

La descomposición de números naturales en factores primos, tiene su análogo en polinomios en la su descomposición como producto de polinomios sin raíces. El problema de la descomposición de números o polinomios es central en la **Criptografía**.

El polinomio x^2+2x+2 no se puede escribir como $x^2+2x+2=(x-a)(x-b)$, con $a,b\in\mathbb{R}$. Es un polinomoo no descomponible en $\mathbb{R}$. Sin embargo el **Teorema Fundamental del Álgebra** nos dice que:

.-*todo polinomio* $a_nx^n+a_{n-1}x^{n-1}+....+a_1x+a_0$, *con coeficientes reales,* $a_0,a_1,....,a_n\in\mathbb{R}$, *tiene al menos una raíz compleja.*

.-*Y por tanto, todo polinomio* $a_nx^n+a_{n-1}x^{n-1}+....+a_1x+a_0$, *con coeficientes reales,* $a_0,a_1,....,a_n\in\mathbb{R}$, *tiene exactamente n raíces (reales o complejas; algunas pueden ser iguales).*

Ejemplo 1. *La ecuación polinómica* $x^2+2x+2=0$, *con coeficientes reales, tienen* ***dos soluciones complejas conjugadas****:* $-1+i$ *y* $-1-i$.

Este no es un hecho aislado.

Proposición 1. *Sea* $a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=0$ *una ecuación polinómica de grado n, con coeficientes* $a_0,a_1,...,a_n\in\mathbb{R}$. *Si* $z\in\mathbb{C}$ *es una solución de la ecuación, entonces su conjugado* $\overline{z}$ *también lo es.*

Demostración: Por ser z una raíz del polinomio

$$0=a_0+a_1z+...+a_nz^n.$$

Tomando conjugados y aplicando las propiedades de la conjugación,

$$\overline{0}=\overline{a_0+a_1z+...+a_nz^n}=\overline{a_0}+\overline{a_1z}+...+\overline{a_nz^n}$$

$$= a_0 + a_1\overline{z} + ... + a_n\overline{z^n} = a_0 + a_1\overline{z} + ... + a_n\overline{z}^n.$$

Lo que prueba que $\overline{z}$ es una raíz del polinomio $\square$

Esto no ocurre si los coeficientes del polinomio son complejos (no todos reales).

Ejemplo 2. *Sea la ecuación* $z^2 + iz + 2 = 0$.

Demostración: Como $\mathbb{C}$ es un cuerpo, la fómula para resolver esta ecuación es la misma que conocemos para $\mathbb{R}$

$$z = \frac{-i \pm \sqrt{i^2 - 8}}{2} = (\frac{-1}{2} \pm \frac{3}{2})i,$$

dos raíces complejas que **no son conjugadas** $\square$

Ejemplo 3. *Si* $x^2 + ax + b$, *es un polinomio de segundo grado con coeficientes en* $\mathbb{R}$ *y sin raíces reales, entonces existen* $\alpha+\beta i, \alpha-\beta i \in \mathbb{C}$ *raíces del polinomio. Además*

$$x^2+ax+b = (x-(\alpha+\beta i))(x-(\alpha-\beta i)) = x^2-2\alpha x+\alpha^2+\beta^2 = (x-\alpha)^2+\beta^2.$$

Despejando se tiene que

$$\alpha = -\frac{a}{2} \qquad y \qquad \beta = \sqrt{b-\alpha^2} = \sqrt{b - \frac{a^2}{4}}.$$

Referencias

Departamento de Análisis Matemático y Matemática Aplicada, Facultad de Matemáticas, Universidad Complutense, 28040 Madrid, Spain
E-mail address: Cesar_Ruiz@mat.ucm.es