AMPLIACIÓN DE MATEMÁTICAS

INTRODUCCIÓN.

Dada una ecuación algebraica o polinómica

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$$

¿cuándo esta ecuación tiene solución? El problema de saber si hay soluciones y como hallarlas es el problema primigenio del álgebra.

Ejemplo 1. *Consideramos la ecuación* $x^2 - 2 = 0$.

- Si consideramos que $x^2 - 2 \in \mathbb{Q}[x]$ y buscamos raíces en el cuerpo $\mathbb{Q}$ no las encontraremos ya que **no** existe $r \in \mathbb{Q}$ de modo que $r^2 = 2$.

  En este caso el polinomio es irreducible en $\mathbb{Q}[x]$.
- Si consideramos que $x^2 - 2 \in \mathbb{R}[x]$, entonces $\sqrt{2}, -\sqrt{2} \in \mathbb{R}$ son las dos raíces que puede tener como máximo un polinomio de grado 2. Además el polinomio se puede **descomponer** sobre el cuerpo $\mathbb{R}$.

El que un polinomio $p(x) \in \mathbb{F}[x]$, $\mathbb{F}$ cuerpo, tenga raíces (y por tanto que la ecuación polinómica $p(x) = 0$ tenga solución) va a depender del cuerpo $\mathbb{F}$ donde estemos trabajando (donde pertenezcan los coeficientes del polinomio).

Lo que vamos a ver es que siempre se puede encontrar un cuerpo, más grande o igual a $\mathbb{F}$, donde el polinomio p tiene tantas raíces como su grado (**cuerpo de descomposición).**

Hay una relación profunda entre la **Teoría de Cuerpos** y las raíces de un polinomio (y por tanto de la **descomposición** de polinomios).

Vamos a estudiar como podemos acrecentar los cuerpos para poder descomponer polinomios. Estas ideas algebraicas, que vamos a desarrollar, tienen aplicaciones en la Teoría de Códigos y en **Criptografía**.

En particular, veremos someramente en el apéndice final del Tema el llamado **cifrado en flujo** (L.F.S.R.).

Referencias

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