# AMPLIACIÓN DE MATEMÁTICAS

## CUERPOS DE DESCOMPOSICIÓN.

Vamos a hablar de forma abstracta del **cuerpo** donde un polinomio tiene tantas raíces como indica su grado.

**Definición 1.** *Sea $f \in \mathbb{F}[x]$, un polinomio con coeficientes en un cuerpo. Sea $\mathbb{K}$ una extensión del cuerpo $\mathbb{F}$ de modo que $f$ se descompone en producto de factores lineales (es decir de grado 1) de $\mathbb{K}[x]$. En estas condiciones se dice que:*

**a:** *$f$ es **descomponible** en $\mathbb{K}$.*

**b:** *$\mathbb{K}$ es el **cuerpo de descomposición** de $f$, si $f$ es descomponible en $\mathbb{K}$ y **no** existe otro cuerpo $\mathbb{K}'$ de modo que*

$$\mathbb{F} \subset \mathbb{K}' \subset \mathbb{K}$$

*y tal que $f$ sea descomponible en $\mathbb{K}'$.*

**Ejemplo 1.** *$\mathbb{C}$ es el cuerpo de descomposición del polinomio $x^2 + 1 \in \mathbb{R}[x]$.*

**Observación 1.** *Por el Teorema de Kronecker sabemos que siempre podemos encontrar un cuerpo donde un polinomios puede ser descompuesto.*

Veamos que siempre podemos encontrar el cuerpo de descomposición para un polinomio dado.

**Definición 2.** *Sea $\mathbb{F}$ un cuerpo y $A$ un subconjunto cualquiera. Denotamos por*

$$\mathbb{F}(A) = \bigcap_{\mathbb{F} \bigcup A \subset \mathbb{K}; \mathbb{K} cuerpo} \mathbb{K}.$$

*$\mathbb{F}(A)$ es el menor cuerpo que contiene a $\mathbb{F}$ y a $A$, donde las operaciones de suma y productos son las mismas en todos los cuerpos que aparecen involucrados en la definición (así $\mathbb{F}$ es un subcuerpo de cada $\mathbb{K}$).*

**Ejemplo 2.** *Sea el cuerpo* $\mathbb{Q}$ *y sea* $\alpha$ *de modo que* $\alpha^2 = 2$. *Entonces claramente* $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$.

**Definición 3.** **a:** $\mathbb{F}(A)$ *es la menor extensión del cuerpo* $\mathbb{F}$ *de modo que están contenidos todos los elemento de* $A$.

**b:** *Si* $A = \{a\}$, *con* $a \notin \mathbb{F}$, $\mathbb{F}(a)$ *se llama extensión simple del cuerpo* $\mathbb{F}$.

**Ejemplo 3.** *El cuerpo* $\mathbb{Q}[\sqrt{2}]$ *es una extensión simple del cuerpo de los números racionales* $\mathbb{Q}$.

**Teorema 1.** *Sea* $f \in \mathbb{F}[x]$, *con* $\mathbb{F}$ *un cuerpo. Sea* $\mathbb{K}$ *una extensión del cuerpo* $\mathbb{F}$ *de modo que* $f$ *es descomponible en* $\mathbb{K}$,

$$f(x) = c(x - a_1)(x - a_2).....(x - a_n) \in \mathbb{K}[x].$$

**a:** $\mathbb{F}(a_1, ..., a_n)$ *es el* ***cuerpo de descomposición*** *de* $f$.

**b:** *Salvo isomorfismo, el cuerpo de descomposición de un polinomio es único.*

***Demostración:***

**a:** Un cuerpo $\mathbb{K}$ donde $f$ es descomponible siempre se puede encontrar por el Teorema de Kronecker. Luego $\mathbb{F}(a_1, ..., a_n)$ está bien definido de modo que $\mathbb{F}$ es un subcuerpo de $\mathbb{F}(a_1, ..., a_n)$ y además $f$ es descomponible en el cuerpo $\mathbb{F}(a_1, ..., a_n)$. Ahora, por el teorema de Factorización Única de polinomios, todo cuerpo en el que se descomponga $f$ tiene que contener a $a_1, a_2, ..., a_n$. Lo cuál quiere decir que incluye al cuerpo $\mathbb{F}(a_1, ..., a_n)$, por definición de este último.

**b:** Esta prueba es aún más abstracta y queda fuera de nuestro alcance $\square$

**Teorema 2.** *Sea* $\mathbb{K}$ *una extensión del cuerpo* $\mathbb{F}$. *Sea* $\alpha \in \mathbb{K}$ *un elemento* ***transcendente*** *de* $\mathbb{K}$ *sobre* $\mathbb{F}$ *(es decir que no existe ningún polinomio de* $\mathbb{F}[x]$ *del cuál es raíz* $\alpha$*). Entonces la extensión simple* $\mathbb{F}(\alpha)$ *es isomorfo al cuerpo de fracciones del anillo* $\mathbb{F}[x]$. *(****Notación:*** *este cuerpo de fracciones se denota por* $\mathbb{F}(x)$*).*

***Demostración:*** $\mathbb{F}(x)$ es el cuerpo de fracciones del dominio de integridad $\mathbb{F}[x]$ (ver la definición de este cuerpo en el Apéndice del Tema de Anillos).

$\mathbb{F}(\alpha)$ es un cuerpo, y así para todo $n \in \mathbb{N}$ y para todo $a_0, a_1, ..., a_n \in \mathbb{F}$

$$0 \neq a_0 + a_1\alpha + a_2\alpha^2 + ... + a_n\alpha^n \in \mathbb{F}(\alpha),$$

por ser $\alpha$ transcendente. Así existe el inverso de

$$a_0 + a_1\alpha + a_2\alpha^2 + ... + a_n\alpha^n$$

en $\mathbb{F}(\alpha)$. Ahora ya es "fácil" ver que la aplicación

$$\begin{array}{rccc} h & : & \mathbb{F}(x) & \to & \mathbb{F}(\alpha) \\ & & \frac{b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0}{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0} & \to & h\left(\frac{b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0}{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0}\right) \\ & & & = & (b_0 + b_1\alpha + ... + b_m\alpha^m)(a_0 + a_1\alpha + ... + a_n\alpha^n)^{-1} \end{array}$$

es un isomorfismo de cuerpos $\square$

## Referencias

Departamento de Análisis Matemático, Facultad de Matemáticas, Universidad Complutense, 28040 Madrid, Spain

*E-mail address*: Cesar_Ruiz@mat.ucm.es