AMPLIACIÓN DE MATEMÁTICAS

APLICACIÓN: DUPLICACIÓN DEL CUBO.

Hemos visto el siguiente resultado.

Corolario 1. *Sea* $\mathbb{K}$ *una* ***extensión finita*** *del cuerpo* $\mathbb{F}$.

Si $[\mathbb{K} : \mathbb{F}] = 2^m$ *y* $f \in \mathbb{F}[x]$ *es un polinomio irreducible de grado* 3, *entonces* f *también es irreducible sobre* $\mathbb{K}$.

Lo anterior nos permite dar una solución (negativa) a uno de los problemas famosos de la Grecia Clásica, el de la **Duplicación del Cubo**.

Nota Histórica: *En el año 429 a. C., Pericles, gobernador de Atenas por esa época, muere víctima de la peste que atacaba muy severamente la ciudad. A raíz de este suceso algunos de los habitantes deciden ir a la ciudad de Delfos para hacer consultas al Oráculo de Apolo y saber cómo poder detener la epidemia. La respuesta a la consulta del Oráculo es que deben elaborar un nuevo altar en forma de cubo cuyo volumen duplique el del altar que ya existe. Lo intentaron, es muy seguro, pero también fue igualmente cierto que no lograron evitar el desastre por este medio. La pandemia se disipó con el tiempo, pero el problema matemático planteado permaneció.*

Problema: *Dado un cubo de volumen* 1 *(o equivalentemente un segmento de longitud* 1*) hay que construir con* ***regla y compás*** *otro cubo de volumen* 2 *(o equivalentemente, construir un segmento de longitud* $\sqrt[3]{2}$*). Ver la figura.*

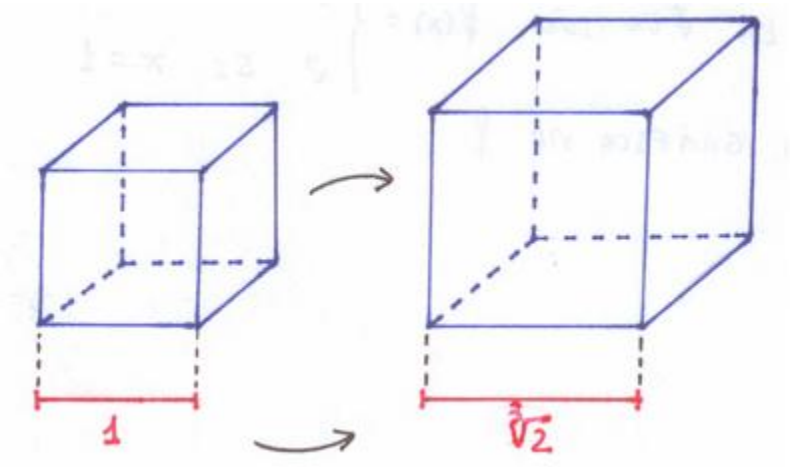

FIGURA 1. Duplicación del cubo.

Al disponer solo de **regla y compás** queremos decir que solo trabajamos sobre los números racionales. Para calcular el valor $\sqrt[3]{2}$, tendríamos que resolver la ecuación $x^3 - 2 = 0$. Pero el polinomio $x^3 - 2$ es irreducible y la ecuación no se puede resolver en $\mathbb{Q}$.

En general, las ecuaciones de las circunferencias (**compás**) son de grado 2 y las de las rectas (**regla**) son de grado 1. Así sus intersecciones son ecuaciones de grado 2^m. Ésto implica que los métodos de construcción griegos (con la ayuda de la regla y el compás) funcionan sobre cuerpos de grado 2^m sobre $\mathbb{Q}$.

La irreducibilidad de $x^3 - 2$ sobre $\mathbb{Q}$, implica que $\mathbb{Q}(\sqrt[3]{2})$ tiene grado 3 sobre $\mathbb{Q}$. Así, no es posible encontrar una ecuación polinómica sobre un cuerpo de orden 2^m que tenga por raíz a $\sqrt[3]{2}$. Lo que implica que **no** se puede duplicar el cubo solo con regla y compás $\square$

Ejemplo 1. $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ *es un cuerpo de grado* 4 *con respecto a* $\mathbb{Q}$.

En efecto,

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}[\sqrt{2}][\sqrt{3}] = \mathbb{Q}(\sqrt{2} + \sqrt{3}).$$

La primera igualdad nos convence del grado de la extensión. Veamos la segunda.

$$(\sqrt{2} + \sqrt{3})^3 - 9(\sqrt{2} + \sqrt{3}) = 2\sqrt{2} \qquad \Rightarrow \qquad \sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3}).$$

Por otro lado

$$\sqrt{3} = (\sqrt{2} + \sqrt{3}) - \sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3}) \ \square$$

Este ejemplo muestra algo más. Que una extensión algebraica $\mathbb{F}(\alpha_1, ..., \alpha_k)$, se puede ver en algunos casos como una extensión simple $\mathbb{F}(\alpha)$. En el caso de cuerpos finitos esto siempre es posible. Es encontrar elementos **primitivos.** Lo vamos a ver en lo que sigue. Adémas estos elementos primitivos son muy útiles en Criptografía.

Referencias

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