AMPLIACIÓN DE MATEMÁTICAS

EXTENSIONES FINITAS.

Todas las extensiones finitas de cuerpos son algebraicas como hemos visto. Las extensiones de cuerpos finitos, vía el Teorema de Kronecker, que son las que más nos interesan, son también finitas. Sin embargo el recíproco no es cierto.

Ejemplo 1. *Existen extensiones algebraicas de cuerpos que no son finitas.*

Veamos un ejemplo. Sea

$$A = \{x \in \mathbb{R} \ : \ x \ \text{ es algebraico sobre } \ \mathbb{Q} \ \}.$$

A es un cuerpo. En efecto, sea $x_1, x_2 \in A$. Sea la extensión finita de $\mathbb{Q}$, $\mathbb{Q}(x_1, x_2) = \mathbb{Q}(x_1)(x_2)$. Por ser finita es algebraica y por tanto

$$\mathbb{Q} \subset \mathbb{Q}(x_1, x_2) \subset A.$$

Ahora

- $x_1 + x_2 \in \mathbb{Q}(x_1, x_2) \subset A$.
- $x_1(x_2)^{-1} \in \mathbb{Q}(x_1, x_2) \subset A$.

Lo que prueba que A es una extensión del cuerpo $\mathbb{Q}$ algebraica. Ver ahora que $[A : \mathbb{Q}] = \infty$ es un poco más complicado. No lo vemos $\square$

Observación 1. *Se puede probar que si*

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

donde $\mathbb{L}$ *es una extensión algebraica de* $\mathbb{K}$ *y ésta a su vez es una extensió algebraica de* $\mathbb{F}$, *entonces la primera* $\mathbb{L}$ *es una extensión algebraica de la última* $\mathbb{F}$.

Veremos que en el caso de cuerpos finitos esta última observación es muy fácil de probar.

Teorema 1. *Sea $\mathbb{L}$ una extensión finita del cuerpo $\mathbb{K}$ y este a su vez es una extensión finita del cuerpo $\mathbb{F}$, entonces*

$$[\mathbb{L} : \mathbb{F}] = [\mathbb{L} : \mathbb{K}][\mathbb{K} : \mathbb{F}].$$

Demostración: Sean

- $\{\alpha_i \ : \ i \in I\}$ una base de $\mathbb{L}$ sobre el cuerpo $\mathbb{K}$; y
- $\{\beta_j \ : \ j \in J\}$ una base de $\mathbb{K}$ sobre el cuerpo $\mathbb{F}$.

Entonces no es difícil ver que $\{\alpha_i\beta_j \ : \ i \in I, j \in J\}$ es una base de $\mathbb{L}$ sobre el cuerpo $\mathbb{F}$. Que forman un sistema de generadores es evidente. Que son linealmente independientes queda como ejercicio $\square$

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

i: *El grado de un elemento $a \in \mathbb{K}$ sobre $\mathbb{F}$ divide a $[\mathbb{K} : \mathbb{F}]$.*

ii: *Un elemento $\alpha \in \mathbb{K}$ genera todo $\mathbb{K}$ sobre $\mathbb{F}$ (es decir si $\{1, \alpha, ..., \alpha^{grad.\alpha}\}$ es una base de $\mathbb{K}$) si solo si su grado es $[\mathbb{K} : \mathbb{F}]$.*

iii: *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 $\mathbb{K}$.*

Demostración:

i: El grado de un elemento es el grado del polinomio mínimo y veíamos (en el Capítulo del Polinomio Mínimo) que éste era precisamente $[\mathbb{F}(a) : \mathbb{F}]$. Como

$$\mathbb{F} \subset \mathbb{F}(a) \subset \mathbb{K}$$

es una cadena de extensiones finitas, el teorema enterior nos dice que

$$[\mathbb{K} : \mathbb{F}] = [\mathbb{K} : \mathbb{F}(a)][\mathbb{F}(a) : \mathbb{F}].$$

ii: Por el Teorema de la Base, todas las bases de $\mathbb{K}$ sobre $\mathbb{F}$ tienen el mismo cardinal. Luego si

$$\{1, \alpha, ..., \alpha^{grad.\alpha}\}$$

es una base de $\mathbb{K}$ (al menos es una base $\mathbb{F}(\alpha)$, como vimos) si y solo si $grad.\alpha = [\mathbb{K} : \mathbb{F}]$.

iii: Si f fuese reducible sobre $\mathbb{K}$, como f tiene grado 3, existiría $\alpha \in \mathbb{K}$ raíz del polinomio. El polinomio mínimo de α sería f (no puede ser uno de segundo grado ya que entonces dividiría a f). Entonces el grado de α es tres y tendría que dividir a 2^m, según

el apartado **i**. Como esto no es posible, f es irreducible sobre $\mathbb{K}$
□

Ejemplo 2. *Dado el cuerpo* $\mathbb{Q}$, *tanto* $\mathbb{Q}[\sqrt{2}]$ *como* $\mathbb{Q}[\sqrt{3}]$ *son extensiones del cuerpo de los racionales de grado* 2. *Sin embargo* $\mathbb{Q}[\sqrt{2}]$ *y* $\mathbb{Q}[\sqrt{3}]$ *no son extensiones el uno del otro.*

Este tipo de situaciones no se dan en el caso de trabajar con cuerpos finitos, como veremos en el próximo Capítulo.

Referencias

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