AMPLIACIÓN DE MATEMÁTICAS

POLINOMIO MÍNIMO.

Las extensiones algebraicas de cuerpos, que son las que más nos interesan, tienen además propiedades adicionales.

Proposición 1. *Sea $\mathbb{K}$ una extensión del cuerpo $\mathbb{F}$. Sea $\alpha \in \mathbb{K}$ un* ***elemento algebraico*** *con respecto al cuerpo $\mathbb{F}$. Entonces existe un polinomo mónico e irreducible $f \in \mathbb{F}[x]$ de modo que α es raíz de él ($\overline{f}(\alpha) = 0$).*

Demostración: Por ser α un elemento algebraico, existe $h \in \mathbb{F}[x]$, mónico, de modo que α es raíz de h. Si h es irreducible ya hemos terminado la prueba. Si no, se puede descomponer en producto único de factores mónicos irreducibles

$$h(x) = f_1(x)f_2(x).....f_k(x).$$

Como $\overline{h}(\alpha) = 0$, y $\mathbb{K}$ es un cuerpo (por tanto no tiene divisores de cero), tiene que existir un j de modo que $\overline{f_j}(\alpha) = 0$. Ya hemos encontrado el polinomio mónico e irreducible que buscabamos $\square$

Definición 1. *Sea $\mathbb{K}$ una extensión del cuerpo $\mathbb{F}$. Sea $\alpha \in \mathbb{K}$ un* ***elemento algebraico*** *con respecto al cuerpo $\mathbb{F}$. Al polinomio f mónico e irreducible de menor grado de $\mathbb{F}[x]$ de modo que $\overline{f}(\alpha) = 0$ se le llama* ***polinomio mínimo*** *de α. El* ***grado*** *de α respecto del cuerpo $\mathbb{F}$ es el grado del polinomio mínimo.*

La Proposición anterior nos dice que existe un polinomio con las propiedades del polinomioo mínimo, pero que este existe y es único como sugiere la definición anterior es lo que vamos a ver a continuación.

Proposición 2. *Si f es el* ***polinomio mínimo*** *de un elemento $\alpha \in \mathbb{K}$ con respecto a un cuerpo $\mathbb{F}$ y si $g \in \mathbb{F}[x]$ verifica que $\overline{g}(\alpha) = 0$, entonces f divide a g ($f|g$).*

Demostración: Si suponemos que no, entonces

$$g(x) = q(x)f(x) + r(x)$$

y necesariamente $\overline{r}(\alpha) = 0$ con $grad.r < grad.f$, lo que contradice la definición de polinomio mínimo $\square$

Observación 1. *Ahora es claro que el polinomio mínimo existe y es único.*

Tomamos él de grado menor con las propiedades correspondientes, que sabemos que existe por la primera Proposición. Si hubiese dos, f_1 y f_2, como ambos son mónicos, de grados iguales y por la Proposición anterior se dividen mutuamente, solo puede ocurrir que sean iguales $\square$

Teorema 1. *Sea $\mathbb{K}$ una extensión del cuerpo $\mathbb{F}$. Sea $\alpha \in \mathbb{K}$ un **elemento algebraico** con respecto al cuerpo $\mathbb{F}$. Sea f el **polinomio mínimo** de α con respecto al cuerpo $\mathbb{F}$. Sea $grad.f = n$. Por último consideramos $\mathbb{F}(\alpha)$ el menor cuerpo que contiene a $\mathbb{F}$ y a α. Entonces*

- **a:** *$\mathbb{F}(\alpha)$ es una extensión **finita** del cuerpo $\mathbb{F}$ de **grado** n (es decir $[\mathbb{F}(\alpha) : \mathbb{F}] = n$).*
- **b:** *$\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ forma una base del espacio vectorial $\mathbb{F}(\alpha)$ con respecto al cuerpo $\mathbb{F}$.*

Demostración: Consideramos el conjunto

$$X = \{r = a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} \ : \ a_0, a_1, ..., a_{n-1} \in \mathbb{F} \ \}.$$

Este conjunto es un espacio vectorial con la suma y el producto por escalares de $\mathbb{F}$ como lo es

$$\mathbb{F}^n = \{(a_0, ..., a_{n-1}) \ : \ a_0, ...a_{n-1} \in \mathbb{F} \ \}.$$

Donde una base está formada por los elementos

$$\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}.$$

Es bastante claro que forman un sistema de generadores y si

$$a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} = 0$$

con no todos los coeficientes $a_0, ...a_{n-1}$ nulos, implicaría que el polinomio $a_0 + a_1x + ... + a_{n-1}x^{n-1} \in \mathbb{F}[x]$, con grado menor que n, nos permitiría encontrar un polinomio mínimo de grado menor que él de f.

Lo cuál es contradictorio. Así el sistema de generadores es linealmente independiente.

Además hemos visto que el dominio de integridad $X \subset \mathbb{K}$ es un cuerpo ya que todo elemento de X no nulo tiene inverso. En efecto, sea $r = a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} \in X$, por la definición de polinomio mínimo

$$m.c.d.(a_0 + a_1x + ... + a_{n-1}x^{n-1}, f) = 1.$$

Así el lema de Bezout nos permite encontrar $v, u \in \mathbb{F}[x]$, podemos suponer que el grado de v es menor que n (en otro caso dividiremos por f), de modo que

$$1 = v(x)(a_0 + a_1x + ... + a_{n-1}x^{n-1}) + u(x)f(x).$$

Así $\overline{v}(\alpha)$ es el inverso de r en X.

Ahora como X es un subcuerpo de $\mathbb{K}$ y contiene a $\mathbb{F}$ y α, es fácil convencerse que

$$\mathbb{F}(\alpha) = X$$

lo que prueba el teorema $\square$

Ejemplo 1. *El* ***polinomio mínimo*** *de* $\sqrt[3]{2} \in \mathbb{Q}(\sqrt[3]{2})$ *sobre* $\mathbb{Q}$ *es* x^3-2. *Y además,*

$$\mathbb{Q}(\sqrt[3]{2}) = \{a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{4} \ : \ a_0, a_1, a_2 \in \mathbb{Q} \ \}.$$

Corolario 1. *Si* f *es un polinomio irreducible de* $\mathbb{F}[x]$ *y existe su derivada* $f' \neq 0$, *entonces todas las raíces de* f *son distintas.*

Demostración: Si $f(x) = (x-\alpha)^2 g(x)$, donde α es una raíz de f en el cuerpo $\mathbb{F}(\alpha)$, entonces

$$f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 g'(x) \neq 0$$

Así el grado de f es mayor que el grado de f'. Por otro lado $\overline{f'}(\alpha) = 0$ y como f es el polinomio mínimo de α (ya que es irreducible) se tendría que $f|f'$. Esto no es posible por los grados de cada polinomio. Así llegamos a contradicción. f no puede tener raíces múltiples $\square$

Ejemplo 2. $x^3+1 = (x+1)^3 \in \mathbb{Z}_3[x]$. *Por otro lado* $(x^3+1)' = 3x^2 = 0$ *en* $\mathbb{Z}_3[x]$.

Referencias

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