AMPLIACIÓN DE MATEMÁTICAS

EXTENSIONES FINITAS. POLINOMIO MÍNIMO.

Las extensiones de cuerpos finitos tienen unas características especiales. Además son importantes las propiedades de los cuerpos finitos, en particular sus cardinales y como son sus grupos multiplicativos. En los siguiente capítulos iremos desarrolando estas ideas y sus aplicaciones.

El cardinal de un cuerpo finito y sus extensiones está relacionado con la **característica** del mismo.

Proposición 1. *Sea $\mathbb{F}$ un cuerpo finito de característica p y sea $f \in \mathbb{F}[x]$ un polinomio irreducible sobre $\mathbb{F}$ de grado k. Entonces*

a: *el anillo $\mathbb{F}[x]$ y el cuerpo $\mathbb{F}[x]/f$ tienen ambos* ***característica*** *p.*

b: $Card.\mathbb{F}[x]/f = (Card.\mathbb{F})^k$.

Demostración:

a: Al estudiar Anillos vimos que p es siempre un primo y que si $Char.\mathbb{F} = p$, entonces $Char.\mathbb{F}[x] = p$.

Por otro lado $\mathbb{F}$ es un subcuerpo de $\mathbb{F}[x]/f$. Ahora para todo $u \in \mathbb{F}[x]/f$ no nulo con

$$0 = u + u + ...{}_{n-\text{veces}}.. + u = u(1 + 1 + ...{}_{n-\text{veces}}.. + 1),$$

como $1 \in \mathbb{F}$ y la característica de $\mathbb{F}$ es p, parece claro que $n = p$.

b: Vimos que una base del espacio vectorial $\mathbb{F}[x]/f$ respecto del cuerpo $\mathbb{F}$ esta formada por

$$\{1, [x], [x]^2, ..., [x]^{k-1}\}.$$

Luego todas las combinaciones lineales que podemos hacer con la base anterior usando como coeficientes los elementos de $\mathbb{F}$ son precisamente $(Card.\mathbb{F})^k = Card.\mathbb{F}[x]/f$ $\square$

De forma general siempre se tiene que

Observación 1. *Si* $\mathbb{F}$ *es un* ***subcuerpo*** *de* $\mathbb{K}$ *o equivalentemente si* $\mathbb{K}$ *es una* ***extensión de cuerpo*** *de* $\mathbb{F}$, *entonces* $\mathbb{K}$ *es un espacio vectorial con respecto al cuerpo* $\mathbb{F}$. *Además la característica de* $\mathbb{F}$ *se transmite a* $\mathbb{K}$.

En efecto, consideramos en $\mathbb{K}$ su **suma**. Ahora, para todo $r \in \mathbb{F}$ y para todo $a \in \mathbb{K}$ $r \times a$, el producto de ambos en $\mathbb{K}$ lo consideramos un **producto por escalares**. Así es fácil ver que efectivamente $\mathbb{K}$ es un espacio vectorial con respecto al cuerpo $\mathbb{F}$

La cuestión de la característica se ve de forma análoga a la prueba de la Proposición anterior $\square$

Los cuerpos finitos siempre tienen una característica no nula y eso permite dar una relación entre la característica y el cardinal.

Teorema 1. *Sea* $\mathbb{F}$ *un cuerpo finito con* $Char.\mathbb{F} = p$. *Entonces*

a: $(\mathbb{Z}_p, + \times)$ *es un subcuerpo de* $\mathbb{F}$.

b: *Existe* $n \in \mathbb{N}$, *de modo que* $Card.\mathbb{F} = p^n$.

Demostración:

a: Se considera la aplicación

$$\begin{array}{rccc} i & : & \mathbb{Z}_p & \to & \mathbb{F} \\ & & n & \to & i(n) = 1 + 1 + ...{}_{n-\text{veces}}.. + 1. \end{array}$$

Es fácil ver que es un homomorfismo de cuerpos y además es inyectivo. En efecto, si $i(n) = i(m)$, con $m < n < p$, se tiene que

$$(n - m) \times 1 = 0,$$

lo cuál implicaría que la característica de $\mathbb{F}$ es menor que p y esto no es posible. Luego identificando $n \in \mathbb{Z}_p$ con $i(n)$, se tiene que $\mathbb{Z}_p$ es un subcuerpo de $\mathbb{F}$.

b: Por la observación de arriba, $\mathbb{F}$ es un espacio vectorial sobre el cuerpo $\mathbb{Z}_p$. Además como $\mathbb{F}$ es finito su dimensión también lo es. Supongamos que esta dimensión es n (lo que quiere decir que toda base esta formada por n vectores linealmente independientes). Luego todas las combinaciones lineales que podemos hacer con la base anterior y usando como coeficientes los elementos de $\mathbb{Z}_p = \{0, 1, ..., p - 1\}$ son precisamente

$$(Card.\mathbb{Z}_p)^n = p^n = Card.\mathbb{F} \ \square$$

Hay distintos tipos de extensiones de cuerpos. En concreto.

Definición 1. *Sea $\mathbb{F}$ un cuerpo y $\mathbb{K}$ una extensión del primer cuerpo.*

a: *Un elemento $a \in \mathbb{K}$ se llama* ***algebraico****, con respecto al subcuerpo $\mathbb{F}$, si existe un polinomio $f \in \mathbb{F}[x]$ de modo que a es raíz de f, ($\overline{f}(a) = 0$).*

b: *Los elemento de $\mathbb{K}$ que* ***no*** *son algebraicos se llaman* ***transcendentes.***

c: *Una extensión de cuerpo $\mathbb{K}$ con respecto al cuerpo $\mathbb{F}$ se dice que es una* ***extensión algebraica*** *si todos los elementos de $\mathbb{K}$ son algebraicos.*

d: *Una extensión de cuerpo $\mathbb{K}$ de $\mathbb{F}$ se llama transcendente si al menos un elemento de $\mathbb{K}$ es transcendente.*

e: *Se llama* ***grado*** *de la extensión a la* ***dimensión*** *del espacio vectorial $\mathbb{K}$ respecto del cuerpo $\mathbb{F}$. (****Notación:*** $[\mathbb{K} : \mathbb{F}] = \dim \mathbb{K}$*).*

f: *Se dice que una extensión de cuerpo es* ***finita*** *si* $[\mathbb{K} : \mathbb{F}] = \dim \mathbb{K} < \infty$.

Las propiedades en general de las extensiones de cuerpos se pueden ver en el Apéndice anterior. Por ejemplo, allí se prueba que

Proposición 2. *Toda extensión finita $\mathbb{K}$ de un cuerpo $\mathbb{F}$ es algebraica.*

Esta noción la vamos a emplear para definir el **polinomio mínimo.** Aunque nosotros nos vamos a concentrar a partir de aquí en las extensiones finitas de cuerpos finitos.

Corolario 1. *Sea $\mathbb{K}$ una extensión finita de un cuerpo $\mathbb{F}$ finito y de característica p. Entonces*

a: $Card.\mathbb{K} = (Card.\mathbb{F})^{[\mathbb{K}:\mathbb{F}]} = p^{[\mathbb{F}:\mathbb{Z}_p][\mathbb{K}:\mathbb{F}]}$

b: *$\mathbb{K}$ es una extensión algebraica de $\mathbb{F}$.*

Demostración: El apartado **a** es una reformulación de la proposición de arriba con la notación de la definición. El apartado **b** es simplemente la segunda Proposición $\square$

Corolario 2. *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 $\square$

Según la definición de arriba, si $\mathbb{K}$ es un a extensión finita del cuerpo $\mathbb{F}$, entonces para todo $\alpha \in \mathbb{K}$ existe un polinomio $f \in \mathbb{F}[x]$ de modo que $\overline{f}(\alpha) = 0$. Podemos pedir más propiedades al polinomio f.

Observación 2. *f puede ser mónico e irreducible y si además es de grado mínimo es único.*

En efecto, f puede ser descompuesto según el Teorema de Factorización Única

$$f(x) = cf_1(x).....f_k(x)$$

donde cada f_j es irreducible y mónico. Por ser $\mathbb{K}$ un cuerpo y como $\overline{f}(\alpha) = 0$, necesariamente para algún j se tiene que $\overline{f_j}(\alpha) = 0$. Este polinomio ya es mónico e irreducible. Además si tomamos el de grado mínimo, le volvemos a llamar f, y otro polinomio $g \in \mathbb{F}[x]$ que verifica $\overline{g}(\alpha) = 0$, entonces $f|g$ (en otro caso $g = qf + r$ y el $grad.r < grad.f$, lo que nos lleva a que f no es él de grado mínimo). Para más detalles ver el cápitulo sobre el polinomio mínimo en el Apéndice $\square$

Lo anterior nos da pie a la siguiente definición.

Definición 2. *Sea $\mathbb{K}$ una extensión finita de un cuerpo $\mathbb{F}$. Sea $\alpha \in \mathbb{K}$, al único polinomio mónico, irreducible y de grado mínimo $f \in \mathbb{F}[x]$ se le llama **polinomio mínimo** de α con respecto a $\mathbb{F}$. Se llama grado de α a*

$$grad.f = [\mathbb{F}[x]/f : \mathbb{F}].$$

Para entender la definición de grado de un elemento algebraico de una extensión de cuerpo damos el siguiente resultado.

Teorema 2. *Sea $\mathbb{K}$ una extensión finita de un cuerpo $\mathbb{F}$. Sean $\alpha \in \mathbb{K}$, y $f \in \mathbb{F}[x]$ su **polinomio mínimo** de grado k. Se difine $\mathbb{F}(\alpha)$ el subconjunto de $\mathbb{K}$ dado por*

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

Entonces

a: $\mathbb{F}(\alpha)$ *es un subcuerpo de* $\mathbb{K}$, *extensión a su vez de* $\mathbb{F}$.
b: $\mathbb{F}(\alpha) = \{a_0 + a_1\alpha + ... + a_{k-1}\alpha^{k-1} \ : \ a_0, a_1, ..., a_{k-1} \in \mathbb{F}\}$.
c: $[\mathbb{F}(\alpha) : \mathbb{F}] = k$.
d: $\mathbb{F}[x]/f$ *es isomorfo a* $\mathbb{F}(\alpha)$.

Demostración: Para los detalles de la construcción del cuerpo $\mathbb{F}(\alpha)$ ver el capítulo del Polinomio Mínimo en el Apéndice. Para ver que $\mathbb{F}[x]/f$ es isomorfo a $\mathbb{F}(\alpha)$, dado que

$$\mathbb{F}(\alpha) = \{a_0 + a_1\alpha + ... + a_{k-1}\alpha^{k-1} \ : \ a_0, a_1, ..., a_{k-1} \in \mathbb{F}\},$$

y que

$$\mathbb{F}[x]/f = \{a_0 + a_1[x] + ... + a_{k-1}[x]^{k-1} \ : \ a_0, a_1, ..., a_{k-1} \in \mathbb{F}\},$$

identificando la α con la $[x]$, ya es fácil deducir el resultado $\square$

Referencias

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