AMPLIACIÓN DE MATEMÁTICAS

EXTENSIONES DE CUERPOS FINITOS.

Cuándo particularizamos el Teorema de Extensión de Kronecker a **Cuerpos Finitos** conseguimos los siguientes resultados.

Teorema 1. *Sea $\mathbb{F}$ un cuerpo finito y sea $f \in \mathbb{F}[x]$ un polinomio irreducible. Sabemos que cardinal de $\mathbb{F}$ es p y el grado de f es n. Entonces*

a: *$\mathbb{F}[x]/f$ es un espacio vectorial sobre el cuerpo $\mathbb{F}$ de dimensión n.*

b: *Si llamos α a la clase de la x (es decir si $\alpha = [x]$),*

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

forma una base de $\mathbb{F}[x]/f$.

c: *El cardinal de $\mathbb{F}[x]/f$ es exactamente p^n.*

d: *El orden del grupo multiplicativo $(\mathbb{F}[x]/f, \times)$ es $p^n - 1$.*

e: *Para todo $a \in \mathbb{F}[x]/f \backslash \{0\}$, $a^{p^n-1} = 1$.*

f: *Los elementos de $\mathbb{F}[x]/f$ son las p^n raíces del polinomio $x^{p^n} - x$.*

Demostración: Vimos que $\mathbb{F}[x]/f$ esta formado por las clases de los posibles restos de dividir por f en $\mathbb{F}[x]$. Es decir todos los polinomios en $\mathbb{F}[x]$ de grado menor o igual que $n-1$, es decir

$$a_0 + a_1 x + ... + a_{n-1} x^{n-1}$$

donde $a_0, a_1, ..., a_{n-1} \in \mathbb{F}$ (los coeficientes se pueden repetir y algunos pueden ser 0). Por tanto

$$\begin{aligned}
\mathbb{F}[x]/f &= \{[a_0 + a_1 x + ... + a_{n-1} x^{n-1}] \ : \ a_0, a_1, ..., a_{n-1} \in \mathbb{F}\,\} \\
&= \{a_0 + a_1[x] + ... + a_{n-1}[x]^{n-1} \ : \ a_0, a_1, ..., a_{n-1} \in \mathbb{F}\,\} \\
&= \{a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} \ : \ a_0, a_1, ..., a_{n-1} \in \mathbb{F}\,\}.
\end{aligned}$$

El conjunto anterior es como el espacio vectorial de vectores

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

con la suma de vectores y el producto de un escalar por un vector habituales. Por tanto $\mathbb{F}[x]/f$ es un espacio vectorial sobre el cuerpo $\mathbb{F}$. Su cardinal es el de $\mathbb{F}^n$, por tanto p^n. Y una base está formada, por lo visto arriba, por

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

Como el cardinal de la base es n, la dimensión del espacio vectorial es n.

Por otro lado sabemos, del Teoream de Kronecker, que $\mathbb{F}[x]/f$ es un cuerpo, por tanto $(\mathbb{F}[x]/f\backslash\{0\}, \times)$ es un grupo multiplicativo de orden $p^n - 1$. Por la teoría de grupos sabemos que cualquier elemento $a \in (\mathbb{F}[x]/f\backslash\{0\}, \times)$ elevado al orden del grupo da necesariamente el elemento neutro (1 en este caso). Además, como

$$x^{p^n} - x = x(x^{p^n-1} - 1)$$

es claro ya que todos los elementos del cuerpo $\mathbb{F}[x]/f$ son raíces del polinomio y solo éstas ya que el polinomio tiene grado p^n $\square$

Ejemplo 1. *Vamos a ver como es* $\mathbb{Z}_2[x]/(x^2 + x + 1)$.

$\mathbb{Z}_2 = \{0, 1\}$ es un cuerpo de dos elementos. El polinomio x^2+x+1 es irreducible en $\mathbb{Z}_2[x]$, ya que ni 0 ni 1 son raíces de él (en este caso, como el polinomio es de grado 2, para ser reducible necesita tener alguna raíz sobre el cuerpo $\mathbb{Z}_2$). Por el Teorema anterior $\mathbb{Z}_2[x]/(x^2 + x + 1)$ tiene $2^2 = 4$ elementos y una base del mismo es $\{1, \alpha = [x]\}$, así

$$\mathbb{Z}_2[x]/(x^2 + x + 1) = \{0, 1, \alpha, 1 + \alpha\}.$$

Las operaciones sobre $\mathbb{Z}_2[x]/(x^2 + x + 1)$ vienen dadas por las tablas:

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

$\times$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

Para construir la tabla del producto observemos que

- $\alpha^2 = 1 + \alpha$, sin más que despejar de $1 + \alpha + \alpha^2 = 0$ y notar que $1 = -1$ en $\mathbb{Z}_2$ (la clase del cero es $[0] = [x^2 + x + 1] = \alpha^2 + \alpha + 1$.
- $\alpha(1 + \alpha) = \alpha + \alpha^2 = 1$
- $(1 + \alpha)^2 = 1^2 + 2\alpha + \alpha^2 = 1 + \alpha^2 = \alpha$.

Por otro lado observamos que la diagonal de la tabla de la suma esta formada por ceros, lo que indica que la **característica** de

$$\mathbb{Z}_2[x]/(x^2+x+1)$$

es 2, como la de $\mathbb{Z}_2$. $\square$

Ejemplo 2. *Vamos a encontrar un cuerpo de* 25 *elementos.*

Para ello será suficiente con encontrar un polinomio de grado 2 irreducible en $\mathbb{Z}_5[x]$. Sea

$$\mathbb{Z}_5 = \{0,1,2,3,4\}.$$

El polinomio $x^2-2 \in \mathbb{Z}_5[x]$ es irreducible ya que no tiene ninguna raíz en $\mathbb{Z}_5$ (cualquier elemento de $\mathbb{Z}_5$ al cuadrado es distinto de 2). Por tanto el cuerpo $\mathbb{Z}_5[x]/(x^2-2)$ tiene exactamente $5^2 = 25$ elementos $\square$

Ejemplo 3. *Si* $\alpha = [x] \in \mathbb{Z}_5[x]/(x^2-2)$, *vamos a calcular* α^{51}.

α es un elemento del grupo multiplicativo

$$(\mathbb{Z}_5[x]/(x^2-2))^* = \mathbb{Z}_5[x]/(x^2-2)\backslash\{0\},$$

que tiene 24 elementos. Por tanto

$$\alpha^{51} = \alpha^{2\times 24+3} = (\alpha^{24})^2\alpha^3 = \alpha^3 = \alpha\alpha^2 = 2\alpha,$$

ya que $\alpha^2 - 2 = 0$ $\square$

Ejercicio 1. *Sea* $\mathbb{K} = \mathbb{Z}_p[x]/(x^3+x^2+2x+a)$. *Elige* p *y* a *para que* $\mathbb{K}$ *sea un cuerpo de* 27 *elementos. Si* α *es la clase de la* x, *calcula en* $\mathbb{K}$ *el inverso de* $\alpha^{1460}+\alpha^2+\alpha+2$.

Si $p = 3$ y x^3+x^2+2x+a es un polinomio irreducible sobre $\mathbb{Z}_3 = \{0,1,2\}$, tendremos que $\mathbb{K}$ es un cuerpo de 27 elementos. Elijamos a para que el polinomio no tenga raíces en $\mathbb{Z}_3$ y por ser de grado 3 será irreducible.

- $0^3+0^2+2\times 0+a = a$, luego a no puede ser cero.
- $1^3+1^2+2+a = 1+a$, luego a no puede ser $-1=2$.
- $2^3+2^2+2\times 2+a = 1+a$, luego a no puede ser $-1=2$.

Luego $a = 1$.

Ahora el grupo multiplicativo $\mathbb{K}^*$ tiene 26 elementos y $1460 = 26\times 56+4$. Por tanto

$$\alpha^{1460}+\alpha^2+\alpha+2 = (\alpha^{26})^{56}\alpha^4+\alpha^2+\alpha+2 = \alpha^4+\alpha^2+\alpha+2$$

Para calcular el inverso vamos a calcular una identidad de Bezout para los polinomios $P(x) = x^4 + x^2 + x + 2$ y $Q(x) = x^3 + x^2 + 2x + 1$ en $\mathbb{Z}_3[x]$. Empezamos dividiendo polinomios,

$$\begin{array}{l} x^4 \quad + x^2 + x + 2 \\ \underline{-x^4 - x^3 - 2x^2 - x} \\ \quad 2x^3 + 2x^2 \quad + 2 \\ \underline{-2x^3 - 2x^2 - 4x - 2} \\ \quad 2x \end{array} \qquad \begin{array}{l} |\underline{x^3 + x^2 + 2x + 1} \\ x + 2 \end{array} \qquad \begin{array}{l} x^3 + x^2 + 2x + 1 \\ 1 \end{array} \qquad \begin{array}{l} |\underline{2x} \\ 2x^2 + 2x + 1 \end{array}$$

aplicando el algoritmo de Euclides

i	0	1	2	3	4
r_i	$x^4 + x^2 + x + 2$	$x^3 + x^2 + 2x + 1$	$2x$	1	0
q_i		$x + 2$	$2x^2 + 2x + 1$	$2x$	
α_i	1	0	1	$-2x^2 - 2x - 1$	
β_i	0	1	$-x - 2$	$2x^3 + 2x$	

así

$$1 = (x^4 + x^2 + x + 2)(-2x^2 - 2x - 1) + (x^3 + x^2 + 2x + 1)(2x^3 + 2x).$$

Como $x^3 + x^2 + 2x + 1$ es la clase del cero en $\mathbb{Z}_3[x]/(x^3 + x^2 + 2x + 1)$, se sigue que

$$[x^4+x^2+x+2]^{-1} = ([x]^4+[x]^2+[x]+2)^{-1} = [-2x^2-2x-1] = \alpha^2+\alpha+2.$$

Comprobación:

$$\begin{array}{l} \quad x^4 \quad + x^2 + x + 2 \\ \times \qquad\quad x^2 + x + 2 \\ \underline{\quad 2x^4 \quad + 2x^2 + 2x + 1} \\ \quad x^5 \quad + x^3 + x^2 + 2x \\ \underline{x^6 \quad x^4 + x^3 + 2x^2} \\ x^6 + x^5 \quad + 2x^3 + 2x^2 + x + 1 \end{array} \qquad \text{y} \qquad \begin{array}{l} x^6 + x^5 \quad + 2x^3 + 2x^2 + x + 1 \\ \underline{-x^6 - x^5 - 2x^4 - x^3} \\ \quad x^4 + x^3 + 2x^2 + x + 1 \\ \underline{\quad -x^4 - x^3 - 2x^2 - x} \\ \quad 1 \end{array} \qquad \begin{array}{l} |\underline{x^3 + x^2 + 2x + 1} \\ x^3 + x \end{array}$$

Lo que prueba que efectivamente $\alpha^2 + \alpha + 2$ es el inverso del elemento $\alpha^{1460} + \alpha^2 + \alpha + 2$ □

Referencias

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

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