Cuerpos finitos

En este capítulo veremos cómo se pueden construir cuerpos finitos. En la primera sección se explica un ejemplo y en la segunda se explica el caso general.

Un ejemplo de cuerpo finito de ocho elementos

Empezamos con un ejemplo de cómo se construye un cuerpo de ocho elementos, a partir de los anillos de polinomios vistos en el capítulo anterior.

El número 8 es 2^3.

- la base 2 indica que vamos a trabajar en el conjunto $\mathbb{Z}_2[x]$, de polinomios con coeficientes en $\mathbb{Z}_2$
- el exponente 3 nos indica el grado de un polinomio irreducible que vamos a emplear para definir la segunda operación; en este ejemplo tomaremos el polinomio $p(x) = x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$

Para definir un cuerpo necesitamos un conjunto y dos operaciones:

- El conjunto, en este caso, está formado por los polinomios de $\mathbb{Z}_2[x]$ de grado menor que tres. Lo llamaremos K_8, porque tiene ocho elementos:

$$K_8 = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$$

- La primera operación es la suma habitual de polinomios. Es fácil comprobar que esta operación es una clausura, es asociativa y conmutativa, tiene elemento neutro (el polinomio nulo), y que todos los elementos tienen simétrico (en este caso particular, como los coeficientes están en $\mathbb{Z}_2[x]$, cada polinomio es simétrico de sí mismo). Por tanto, K_8, con la suma, tiene estructura de grupo conmutativo. Además, dado que sus elementos, salvo el neutro, tienen orden 2, podemos decir que es isomorfo a $C_2 \times C_2 \times C_2 = C_2^3$.
- Para la segunda operación no podemos tomar el producto habitual de polinomios, porque no es una clausura. Vamos a tomar, de forma similar a lo que se hacía en la aritmética modular, el producto *módulo* el polinomio $p(x)$ que hemos elegido antes. Así pues, el producto de dos polinomios será el resto de dividir el producto habitual por el polinomio $p(x)$.

Ejemplo 1. *Vamos a hacer el producto módulo $p(x)$ de los polinomios x^2+1 y x^2+x. El producto habitual es $(x^2+1)(x^2+x) = x^4+x^3+x^2+x$. La división euclídea de este polinomio entre p(x) es $x^4+x^3+x^2+x = (x^3+x^2+1)x+x^2$. El resto es x^2 y, por tanto, $(x^2+1)(x^2+x) = x^2$.*

Como el resto tiene grado menor que el grado de $p(x)$, que es tres, es un polinomio de K_8, con lo que este producto que hemos definido es una clausura. Además es asociativo, conmutativo y tiene elemento neutro: el polinomio 1.

Además, podemos comprobar que todos los elementos de $K_8 - \{0\}$ tienen inverso:

- El polinomio 1, como siempre pasa con el elemento neutro de cualquier grupo, es inverso de sí mismo.

- x y x^2+x son inversos el uno del otro, porque $x(x^2+x)=x^3+x^2$, y el resto de dividir x^3+x^2 por x^3+x^2+1 es 1. O, visto de otra forma: como $x^3+x^2+1=0$ porque el resto de dividir este polinomio por sí mismo es 0, entonces $x^3+x^2=1$ (recordemos que $-1=1$ porque estamos en $\mathbb{Z}_2$).
- Los polinomios $x+1$ y x^2 son, también, inversos el uno del otro: $(x+1)(x^2)=x^3+x^2=1$
- Finalmente, con los otros dos polinomios, x^2+1 y x^2+x+1, sucede lo mismo: $(x^2+1)(x^2+x+1)=x^4+x^3+x^2+x+1=(x^3+x^2+1)x+1=1$

Así pues, el conjunto $K_8-\{0\}$, con el producto módulo $p(x)$, tiene estructura de grupo conmutativo.

Se puede comprobar que este producto es distributivo respecto de la suma, con lo que K_8 es un cuerpo.

Ejercicio 2. *Haz la tabla de la suma en K_8 (grupo aditivo) y del producto módulo $p(x)$ en $K_8-\{0\}$ (grupo miltiplicativo).*

Ejercicio 3. *Repite el proceso descrito y construye un cuerpo de nueve elementos, tomando como polinomio irreducible $p(x)=x^2+x+2$.*

Fijémonos, por último, en el grupo multiplicativo $K_8-\{0\}$. Es un grupo conmutativo de siete elementos. Sus elementos, salvo el 1, tienen todos orden 7 (recordemos que el orden de un elemento tiene que ser un divisor del orden del grupo). Es decir, es cíclico, isomorfo a C_7.

En particular, el polinomio x tiene orden 7 y es, por tanto, generador: $K_8=<x>$. Con las potencias de x recorremos todos los elementos:

$$x,\ x^2,\ x^3=x^2+1,\ x^4=x^2+x+1,\ x^5=x+1,\ x^6=x^2+x,\ x^7=1$$

Podemos usar esto para simplificar los cálculos, como podemos ver en el siguiente ejemplo.

Ejemplo 4. *Vamos a hacer la operación $(x^2+1)^5(x+1)^7(x^2+x)^{-5}$:*

$$(x^2+1)^5(x+1)^7(x^2+x)^{-5}=(x^3)^5(x^5)^7(x^6)^{-5}=x^{15}x^{35}x^{-30}=x^{20}=x^6=x^2+x$$

Construcción de cuerpos finitos

El proceso descrito en el apartado anterior se puede generalizar, y nos da una caracterización de los cuerpos finitos y una forma de obtenerlos y describirlos.

Sea K un cuerpo finito. Vamos a llamar característica de K al orden de 1 (el elemento neutro del grupo multiplicativo) en el grupo aditivo. La denotaremos por p.

Lema 5. *La característica p de un cuerpo es un número primo.*

Vamos a demostrarlo. Si no lo fuera, $p=a\cdot b$, con $1<a,b<p$. Como p es el orden del elemento 1 en el grupo aditivo, tenemos $p=\overbrace{1+\ldots+1}^{p}=0$. Por tanto, $a\cdot b=0$ y, como un cuerpo no tiene divisores de cero, alguno de los dos factores es cero. Supongamos que lo es a. Entonces $\overbrace{1+\ldots+1}^{a}=0$ con lo que el orden no sería p. □

Ejemplo 6. *La característica del cuerpo K_8 del apartado anterior es* 2.

Entonces, el número de elementos de K tiene que ser un múltiplo de p. De hecho, se puede demostrar que es una potencia de p.

Ejemplo 7. *Hay cuerpos de* 2, 3, 4, 5, 7, 8, 9, 11, 13, 15, 16, 17, 19 . . . *elementos. Pero no los hay de* 6, 10, 12, 14, 18, 20 . . . *elementos.*

Así pues, un cuerpo finito tiene p^r elementos. Además, salvo isomorfismos, sólo existe un cuerpo de orden p^r.

Para construirlo prodecemos como en el ejemplo del apartado anterior. Partimos de un polinomio irreducible $p(x) \in \mathbb{Z}_p[x]$ de grado r. El conjunto y las dos operaciones serían los siguientes.

- Como conjunto tomamos el formado por los polinomios de grado menor que r, con coeficientes en $\mathbb{Z}_p$:

$$K = \{a_0 + a_1 + \ldots + a_{r-1}x^{r-1} \mid a_0, a_1, \ldots, a_{r-1} \in \mathbb{Z}_p\} \subset \mathbb{Z}_p[x]$$

- La primera operación es la suma habitual de polinomios.
- La segunda operación es el producto módulo $p(x)$.

Teorema 8. *El conjunto de polinomios de grado menor que r, con la suma habitual de polinomios y el producto módulo un polinomio irreducible $p(x)$ de grado r, tiene estructura de cuerpo.*

Solo demostraremos la existencia de los elementos inversos para la segunda operación. El resto de las propiedades son fáciles de verificar.

Sea $q(x) \in K - \{0\}$. Como $p(x)$ es irreducible y su grado es mayor que el grado de $q(x)$, el máximo común divisor mónico de estos dos polinomios tiene que ser 1. Planteamos una identidad de Bézout $p(x)a(x) + q(x)b(x) = 1$. Esta igualdad se reduce, módulo $p(x)$, a $q(x)b(x) = 1$, porque $p(x) = 0$. Por tanto, hemos demostrado que $q(x)$ tiene inverso, que es $b(x)$. □

La demostración anterior nos da la forma de encontrar el inverso de un polinomio en el cuerpo K: tenemos que hallar una identidad de Bézout para este polinomio y el polinomio irreducible y su coeficiente será el polinomio inverso.

Ejemplo 9. *En el cuerpo K_{27} formado por los polinomios de $\mathbb{Z}_3$ de grado menor que* 4, *con la suma habitual y el producto módulo $x^3 + 2x + 1$, queremos hallar el inverso de $x^2 + 1$. Una identidad de Bézout es $(x^3 + 2x + 1)(x + 2) + (x^2 + 1)(2x^2 + x + 2) = 1$ y, por tanto, $(x^2 + 1)^{-1} = 2x^2 + x + 2$.*

El cuerpo K así construido se denomina *cuerpo cociente* $\mathbb{Z}_p[x]/p(x)$. Como acabamos de ver, el hecho de que $p(x)$ sea irreducible es determinante para la existencia de los elementos inversos. Si no fuera irreducible, no todos los polinomios serían inversibles y hablaríamos del *anillo cociente* $\mathbb{Z}_p[x]/p(x)$.

Fijémonos ahora en el grupo aditivo $(K, +)$. Todos los polinomios, salvo el nulo, tienen orden p, porque los coeficientes están en $\mathbb{Z}_p$, y en este grupo el orden de todos los elementos, salvo el 0, es p. Por tanto el grupo aditivo es isomorfo a C_p^r.

En cuanto al grupo multiplicativo $(K - \{0\}, \times)$ es un grupo conmutativo de orden $p^r - 1$ que resulta ser cíclico. Es decir, tiene generadores que, en este contexto, se denominan *elementos primitivos*. Si se da la circunstancia de que el polinomio x es uno de ellos, es decir, si $K =< x >$, entonces el polinomio de partida, $p(x)$, se dice que es un *polinomio irreducible primitivo*.

Ejemplo 10. *En el cuerpo K_8 del primer apartado el polinomio $x^3 + x^2 + 1$ es irreducible primitivo, porque habíamos visto que x era un generador.*

Ejercicio 11. *Comprueba que, en $\mathbb{Z}_3[x]$, el polinomio $x^2 + 2x + 2$ del ejercicio 3 es irreducible primitivo y que $x^2 + 1$ es irreducible, pero no primitivo.*