Introducción a la Teoría de Códigos

M.A. García, L. Martínez, T. Ramírez

Facultad de Ciencia y Tecnología. UPV/EHU

Resumen Teórico
Apartado A2 del Anexo:
Construcción de cuerpos finitos

Mayo de 2017

A.2. Construcción de cuerpos finitos

En la sección anterior vimos cómo, dado un número primo p, el cociente $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo finito de cardinal p. Ahora veremos cómo se pueden construir cuerpos finitos de cardinal una potencia p^n de un primo p tomando un cociente apropiado del anillo de polinomios $\mathbb{Z}/p\mathbb{Z}[x]$ en la indeterminada x con coeficientes en $\mathbb{Z}/p\mathbb{Z}$ entre el ideal formado por los polinomios múltiplos de un polinomio irreducible de grado n. Primero necesitaremos dar algunas definiciones:

Definición Sea K un cuerpo, y sea $P(x) = \sum_i a_i x^i$ un polinomio no nulo de $K[x]$. El **grado de** $P(x)$ es el mayor entero no negativo n que cumple $a_n \neq 0$.

El grado de $P(x)$ se suele denotar por $\delta(P(x))$.

Es obvio que los polinomios de grado 0 son las unidades de $K[x]$. A estos se les llaman **polinomios constantes no nulos** (el polinomio nulo también es constante, pero no se le asigna grado).

Definición Sea K un cuerpo. Un polinomio $P(x) \in K[x]$ de grado estrictamente positivo es **irreducible** si $P(x) = Q_1(x)Q_2(x)$ implica que $\delta(Q_1(x)) = 0$ ó $\delta(Q_2(x)) = 0$.

Un polinomio no nulo $P(x)$ de $K[x]$, donde K es un cuerpo, se dice mónico si el coeficiente de $x^{\delta(P(x))}$ es 1_K (dicho coeficiente se llama **coeficiente director** de $P(x)$).Todo polinomio $P(x)$ de grado positivo de $K[x]$, donde K es un cuerpo, se puede descomponer de forma única, salvo por el orden de los factores, en la forma

$$P(x) = aP_1(x) \cdots P_m(x),$$

donde $m \in \mathbb{N}, a \in K$ y los polinomios $P_1(x), \ldots, P_m(x)$ son mónicos e irreducibles.

Ejemplos A.2.1

1. El polinomio $x^2 + \overline{1}$ no es irreducible en $\mathbb{Z}/2\mathbb{Z}[x]$, ya que $x^2 + \overline{1} = (x + \overline{1})^2$, pero $x + \overline{1}$ no es un polinomio constante.

2. En cambio, el polinomio $x^2 + x + \overline{1}$ sí es irreducible en $\mathbb{Z}/2\mathbb{Z}[x]$.

Cuando se trabaja en $\mathbb{Z}/p\mathbb{Z}[x]$ es habitual, cuando no hay ambigüedad, omitir las barras; así, los dos polinomios de los ejemplos se denotarían simplemente por $x^2 + 1$ y $x^2 + x + 1$.

Si K es un cuerpo y $P(x) \in K[x]$, el conjunto

$$(P(x)) = \{P(x)Q(x) \mid Q[x] \in K[x]\}$$

es un ideal, llamado el **ideal generado por el polinomio** $P(x)$. Dado un $Q(x) \in K[x]$, a la coclase $Q(x) + (P(x))$ del anillo cociente $K[x]/(P(x))$ se la suele denotar simplemente por $\overline{Q(x)}$ cuando no hay ambigüedad respecto al ideal $(P(x))$ considerado.

Proposición A.2.1 *El ideal $(P(x))$ es maximal si y sólo si el polinomio $P(x)$ es irreducible.*

De aquí, utilizando la Proposición A.1.4, se deduce lo siguiente:

Corolario A.2.1 *El anillo cociente $K[x]/(P(x))$ es cuerpo si y sólo si el polinomio $P(x)$ es irreducible.*

Ejemplo A.2.2 El cociente $\mathbb{Z}/2\mathbb{Z}[x]/(x^2+x+1)$ es un cuerpo. Si $P(x) \in \mathbb{Z}/2\mathbb{Z}[x]$ y $R(x)$ es el resto de la división de $P(x)$ entre x^2+x+1 (¡Cuidado!, la división es en $\mathbb{Z}/2\mathbb{Z}[x]$), entonces $\overline{P(x)} = \overline{R(x)}$ (aquí las barras representan coclases módulo $(P(x))$), luego

$$\mathbb{Z}/2\mathbb{Z}[x]/(x^2+x+1) = \{\overline{a+bx} \mid a, b \in \mathbb{Z}/2\mathbb{Z}\},$$

y está claro que en esta representación no hay repeticiones. Por lo tanto,

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

es un cuerpo finito con 4 elementos. Para sumar, por ejemplo, $\overline{x}$ y $\overline{x+1}$, se hace

$$\overline{x} + \overline{x+1} = \overline{2x+1} = \overline{1}.$$

Para multiplicar los mismos elementos, se hace

$$\overline{x} \cdot \overline{x+1} = \overline{x(x+1)} = \overline{x^2+x} = \overline{1},$$

ya que $x^2 + x = (x^2+x+1) + 1$.

Para garantizar la existencia de cuerpos de orden potencia de un primo usaremos lo siguiente:

Proposición A.2.2 *Si p es un número primo y $n \in \mathbb{N}$, entonces existe por lo menos un polinomio $P(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ irreducible de grado n.*

De ahí se deduce lo siguiente:

Proposición A.2.3 *Si p es un número primo y $n \in \mathbb{N}$, entonces existe un cuerpo finito de orden p^n.*

No podemos realmente aspirar a una mayor generalidad en los cardinales de los cuerpos finitos, como vemos en la siguiente proposición.

Proposición A.2.4 *Si K es un cuerpo finito, entonces $|K| = p^n$ para algún número primo p y algún número natural n.*

Para cada primo p y cada exponente n hay esencialmente un único cuerpo de orden p^n. Definiremos primero qué queremos decir con 'esencialmente uno'.

Definición Si F, K son dos cuerpos, una aplicación $f : F \longrightarrow K$ es un **isomorfismo** si es biyectiva y además satisface

1. $f(x + y) = f(x) + f(y)\ \forall x, y \in F$,
2. $f(x \cdot y) = f(x) \cdot f(y)\ \forall x, y \in F$.

Cuando existe un isomorfismo entre dos cuerpos F y K, se dice que éstos son **isomorfos**, y se denota por $F \simeq K$. Intuitivamente, esto quiere decir que tienen la misma estructura, es decir, que son indistinguibles desde el punto de vista de las propiedades algebraicas que afectan a la suma y el producto, y que se distinguen tan sólo en la forma de denotar sus elementos.

Proposición A.2.5 *Si F, K son dos cuerpos finitos del mismo cardinal, entonces F y K son isomorfos.*

De lo visto en las proposiciones A.2.3 y A.2.5 se deduce lo siguiente:

Proposición A.2.6 *Para cada número primo p y cada número natural n hay un único cuerpo de orden p^n, salvo isomorfismos.*

Dicho cuerpo se suele denotar por $\mathbb{F}_{p^n}$.