4.3. Cuerpos finitos

Sean $p \in \mathbb{N}$ primo y $h \in \mathbb{Z}_p[x]$ polinomio irreducible de $\mathbb{Z}_p[x]$.

Si $\operatorname{gr}(h) = m \Rightarrow \mathbb{Z}_p[x]/(h)$ es un cuerpo con p^m elementos.

Cuerpo de Galois

Para cada $p \in \mathbb{N}$ primo y cada $m \in \mathbb{N}$ existe, salvo isomorfismos, un único cuerpo de orden $p^m \in \mathbb{N}$, que se denomina **Cuerpo de Galois** y nota por $\mathbb{F}_{p^m}$.
$\mathbb{F}_{p^m} \approx \mathbb{Z}_p[x]/(h)$, siendo $h \in \mathbb{Z}_p[x]$ polinomio irreducible en $\mathbb{Z}_p[x]$, de grado m.

Estructura del grupo aditivo de un cuerpo finito

$(\mathbb{K}, +, \cdot)$ cuerpo finito de característica $p \in \mathbb{N}$ primo $\Rightarrow$ El grupo aditivo $(\mathbb{K}, +)$ es isomorfo a un producto directo de grupos cíclicos de orden p:

$$\mathbb{K} \approx \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$$

El orden de $\mathbb{K}$ es p^m para algún $m \in \mathbb{N}$

Estructura del grupo de unidades de un cuerpo finito

$(\mathbb{K}, +, \cdot)$ cuerpo finito de característica $p \in \mathbb{N}$ primo $\Rightarrow$

El grupo de unidades $(\mathbb{K}^*, \cdot)$ es cíclico: $\mathbb{K}^* \approx \mathbb{Z}_{p^m - 1}$

Polinomio primitivo

Un polinomio $h \in \mathbb{Z}_p[x]$ irreducible, es un **polinomio primitivo** si el polinomio x es un generador del grupo de unidades $(\mathbb{K}^*, \cdot)$, siendo

$$\mathbb{K} = \mathbb{Z}_p[x]/(h)$$

4.3.8. Problemas

1. En cada uno de los siguientes casos, demostrar que el anillo $(\mathbb{F},+,\cdot)$ es un cuerpo, describir sus elementos, indicar el número de elementos y determinar el resultado de las operaciones indicadas:

   a) $\mathbb{F}=\mathbb{Z}_2[x]/\left(x^2+x+1\right)$
      1) $x^3(x+1)+x+1$
      2) $x^2(x+1)+1$
      3) $x^3(x+1)+x^2+1$

   b) $\mathbb{F}=\mathbb{Z}_3[x]/\left(x^2+x+2\right)$
      1) $(x+2)(2x+2)+x+1$
      2) $(2x+1)-(x+1)\,(2x+1)$
      3) $(2x+1)\,(x+2)$
      4) $x^{-1}-(2x+2)^{-1}$

   c) $\mathbb{F}=\mathbb{Z}_2[x]/\,(s)$ siendo $s=x^4+x^3+1\in\mathbb{Z}_2[x]$,
      1) $(x^2+x+1)^{-1}$
      2) $(x^3+x+1)\,(x^2+1)$

   d) $\mathbb{F}=\mathbb{Z}_5[x]/\left(x^2+x+2\right)$ 1) $(2x+3)^{-1}$

2. Demostrar que $k=x^3+x^2+1\in\mathbb{Z}_2[x]$ es irreducible en $\mathbb{Z}_2[x]$ y usarlo para construir un cuerpo de orden 8. Estudiar si $k\in\mathbb{Z}_2[x]$ es un polinomio primitivo.

3. Sea $\mathbb{F}=\mathbb{Z}_3[x]/\left(x^2+2x+2\right)$

   a) Comprobar que el grupo de unidades $(\mathbb{F}^*,\cdot)$ es cíclico. ¿Qué elementos de $\mathbb{F}$ son generadores del grupo de unidades? ¿Es el polinomio x^2+2x+2 primitivo?

   b) ¿Qué elementos de $\mathbb{F}$ admiten raíz cuadrada en $\mathbb{F}$?

   c) Comprobar que el producto de todos los elementos del grupo de unidades $(\mathbb{F}^*,\cdot)$ es 2.