FDFDαH

Apellidos y nombre

AMPLIACIÓN DE MATEMÁTICAS 2019-2020
TRABAJO PRÁCTICO 12: Cuerpos finitos

Da un ejemplo de cuerpo con característica 3 y 81 $= 3^4$ elementos. ¿Es posible encontrar algún ejemplo de cuerpo que tenga exactamente 187 elementos?

¡Basta encontrar un polinomio de grado 4 irreducible en $\mathbb{Z}_3$

↳ por ejemplo: $x^4+1$ (no tiene raíces en $\mathbb{Z}_3$ y no es producto de pol. de grado 2 en $\mathbb{Z}_3$)

Luego $\mathbb{F} = \mathbb{Z}_3[x]/(x^4+1)$ es un cuerpo de característica 3 con $3^4 = 81$ elementos

Como 187 no es potencia de un primo, no podemos encontrar cuerpos con ese número de elementos.

¿Es $\mathbb{Q}[x]/(x^3-9x^2+27x-27)$ un cuerpo? ¿Y $\mathbb{Q}[x]/(x^2-x-1)$? En los casos afirmativos indica su característica y su dimensión como espacio vectorial sobre $\mathbb{Q}$.

$x^3-9x^2+27-27 = (x-3)^3$ es reducible $\Rightarrow$

$\Rightarrow \mathbb{Q}[x]/(x^3-9x^2+27x-27)$ no es cuerpo.

$x^2-x-1=0 \Leftrightarrow x = \frac{1\pm\sqrt{5}}{2} \notin \mathbb{Q} \rightsquigarrow$ Este polinomio no tiene raíces racionales

↳ $\mathbb{Q}[x]/(x^2-x-1)$ es un cuerpo de característica 0 y dimensión 2.

Consideramos $\alpha = [x^3]$ como elemento de $\mathbb{Z}_7[x]/(x^2-x+4)$ (que, por si lo dudabas, es un cuerpo finito). Calcula el representante de $\alpha$ que tenga orden menor que 2 y, si existe, el inverso de $[x^3+x^2+x]$ utilizando el **Algoritmo Extendido de Euclides**.

polinomio irreducible de grado 2 en $\mathbb{Z}_7$ (no tiene raíces)

Siempre existe inverso en los cuerpos

$[x^2-x+4]=0 \Rightarrow [x^3-x^2+4x]=0$

↳ $[x^2]=[x-4]$

↳ $[x^3] = [x^2-4x] = [x-4-4x] = [4x-4]$

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

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

↳ Luego: $[-x-1]^{-1} = [-x+2]$

cuerpo de $2^3 = 8$ elementos

Estudia el anillo $\mathbb{Z}_2[x]/\left(x^3 - x + 1\right)$. Escribe las tablas de adición y multiplicación.

| $+$ | $0$ | $1$ | $x$ | $x+1$ | $x^2$ | $x^2+1$ | $x^2+x$ | $x^2+x+1$ |
|---|---|---|---|---|---|---|---|---|
| $0$ | $0$ | $1$ | $x$ | $x+1$ | $x^2$ | $x^2+1$ | $x^2+x$ | $x^2+x+1$ |
| $1$ | $1$ | $0$ | $x+1$ | $x$ | $x^2+1$ | $x^2$ | $x^2+x+1$ | $x^2+x$ |
| $x$ | $x$ | $x+1$ | $0$ | $1$ | $x^2+x$ | $x^2+x+1$ | $x^2$ | $x^2+1$ |
| $x+1$ | $x+1$ | $x$ | $1$ | $0$ | $x^2+x+1$ | $x^2+x$ | $x^2+1$ | $x^2$ |
| $x^2$ | $x^2$ | $x^2+1$ | $x^2+x$ | $x^2+x+1$ | $0$ | $1$ | $x$ | $x+1$ |
| $x^2+1$ | $x^2+1$ | $x^2$ | $x^2+x+1$ | $x^2+x$ | $1$ | $0$ | $x+1$ | $x$ |
| $x^2+x$ | $x^2+x$ | $x^2+x+1$ | $x^2$ | $x^2+1$ | $x$ | $x+1$ | $0$ | $1$ |
| $x^2+x+1$ | $x^2+x+1$ | $x^2+x$ | $x^2+1$ | $x^2$ | $x+1$ | $x$ | $1$ | $0$ |

| $\cdot$ | $0$ | $1$ | $x$ | $x+1$ | $x^2$ | $x^2+1$ | $x^2+x$ | $x^2+x+1$ |
|---|---|---|---|---|---|---|---|---|
| $0$ | $0$ | $0$ | $0$ | $0$ | $0$ | $0$ | $0$ | $0$ |
| $1$ | $0$ | $1$ | $x$ | $x+1$ | $x^2$ | $x^2+1$ | $x^2+x$ | $x^2+x+1$ |
| $x$ | $0$ | $x$ | $x^2$ | $x^2+x$ | $x+1$ | $1$ | $x^2+x+1$ | $x^2+1$ |
| $x+1$ | $0$ | $x+1$ | $x^2+x$ | $x^2+1$ | $x^2+x+1$ | $x^2$ | $1$ | $x$ |
| $x^2$ | $0$ | $x^2$ | $x+1$ | $x^2+x+1$ | $x^2+x$ | $x$ | $x^2+1$ | $1$ |
| $x^2+1$ | $0$ | $x^2+1$ | $1$ | $x^2$ | $x$ | $x^2+x+1$ | $x+1$ | $x^2+x$ |
| $x^2+x$ | $0$ | $x^2+x$ | $x^2+x+1$ | $1$ | $x^2+1$ | $x+1$ | $x$ | $x^2$ |
| $x^2+x+1$ | $0$ | $x^2+x+1$ | $x^2+1$ | $x$ | $1$ | $x^2+x$ | $x^2$ | $x+1$ |

Calcula $[x^2+1]^{4466}$ en $\underbrace{\mathbb{Z}_5[x]/\left(x^3 + x + 1\right)}$ (¿Es un cuerpo?) utilizando el **Teorema de Lagrange**.

↳ cuerpo pues $x^3+x+1$ es irreducible en $\mathbb{Z}_5$ y tiene cardinal $5^3 = 125$

$\boxed{\text{Teorema de Lagrange}}$: $[a]^{124} \equiv 1 \pmod{5}$

$$4466 = 36 \cdot 124 + 2$$

Luego: $[x^2+1]^{4466} = \left(\cancel{[x^2+1]^{124}}^{\,1}\right)^{36} \cdot \left([x^2+1]^2\right) =$

$= [x^4 + 2x^2 + 1] = [x \cdot (-x-1) + 2x^2 + 1] =$

$= [-x^2 - x + 2x^2 + 1] = [x^2 - x + 1]$