Ejercicio 2.1.

Encuentra una raiz primitiva de $\mathbb{F}_{16} = \frac{\mathbb{F}_2[x]}{x^4+x^3+x^2+x+1}$.

↑ Si α es una raiz de $x^4+x^3+x^2+x+1$ sobre $\mathbb{F}_2$,

entonces $\mathbb{F}_{16} = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+1, x^3+x^2+x+1\}$.

Veamos que $[x+1]$ es un elemento primitivo:

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

$[x+1]^3 = [x+1][x^2+1] = [x^3+x^2+x+1]$

$[x+1]^4 = [x^2+1][x^2+1] = [x^4+1] = [x^3+x^2+x]$.

$[x+1]^5 = [x+1][x^3+x^2+x] = [x^4+x^3+x^2+x^3+x^2+x] =$

$= [x^4+x] = [x^3+x^2+1]$.

$[x+1]^6 = [x+1][x^3+x^2+1] = [x^4+x^3+x+x^3+x^2+1] =$

$[x^4+x^2+x+1] = [x^3]$

$[x+1]^7 = [x^4+x^3] = [x^2+x+1]$.

$[x+1]^8 = [x+1][x^2+x+1] = [x^3+x^2+x+x^2+x+1] = [x^3+1]$

$[x+1]^9 = [x+1][x^3+1] = [x^4+x+x^3+1] = [x^2]$

$[x+1]^{10} = [x+1][x^2] = [x^3+x^2]$

$[x+1]^{11} = [x+1][x^3+x^2] = [x^4+x^3+x^3+x^2] = [x^4+x^2] =$

$[x^3+x+1]$.

$[x+1]^{12} = [x+1][x^3+x+1] = [x^4+x^2+x+x^3+x+1] =$

$= [x]$.

$[x+1]^{13} = [x^2+x]$

$[x+1]^{14} = [x+1][x^2+x] = [x^3+x^2+x^2+x] = [x^3+x]$

$[x+1]^{15} = [x+1][x^3+x] = [x^4+x^2+x^3+x] = \underline{\underline{[1]}}$.

a

Ejercicio 2.2

K extensión de $\mathbb{F}_2$, de grado $n>1$. $p(x) \in \mathbb{F}_2[x]$ no nulo.

① Si $\alpha \in K$ es raíz de $p(x)$, entonces $\{\alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \ldots\}$ son todas las raíces de $p(x)$ en K.

$\nearrow \frac{K}{\mathbb{F}_2}$ es una extensión, $[K:\mathbb{F}_2]=n$.

Si α es una raíz de $p(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n$

entonces $\alpha^n + a_1\alpha^{n-1} + \ldots + a_{n-1}\alpha + a_n = 0$.

Veamos que α^{2^i} es raíz de $p(x)$.

Sabemos que $0 = (\alpha^n + a_1\alpha^{n-1} + \ldots + a_{n-1}\alpha + a_n)^{2^i} =$

$= \alpha^{2^i n} + (2^i a_1)\cdot\alpha^{2^i n-1} + (2^i a_2 + \binom{2^i}{2} a_1^2)\alpha^{2n-2} +$

$+ (2^i a_3 + \binom{2^i}{3} a_1^3 + 2\binom{2^i}{2} a_1 a_2)\alpha^{2n-3} + \ldots + a_n^{2^i} =$ ↙ reduciendo módulo 2.

$= \alpha^{2^i n} + a_1^{2^i}\alpha^{2^i n - 2^i} + a_2^{2^i}\cdot\alpha^{2^i n - 2\cdot 2^i} + \ldots + a_n^{2^i} =$ ↙ $a_i \in \mathbb{F}_2$

$= (\alpha^{2^i})^n + a_1(\alpha^{2^i})^{n-1} + \ldots + a_n = p(\alpha^{2^i}) = 0$

Luego α^{2^i} es raíz de $p(x)$.

□

② β es raíz primitiva de K, que es raíz de $p(x) \Rightarrow$ el grado de $p(x)$ es al menos n.

③ Si β es raíz primitiva de K, entonces

$K = \{\beta, \beta^2, \beta^3, \ldots, \beta^n\}$ siendo n el grado de la extensión.

Por ser β raíz de $p(x) \Rightarrow$ las raíces de $p(x)$ son

$\beta, \beta^2, \beta^4, \ldots, \beta^{2^n}$ y son distintos. $\Rightarrow$

En K hay al menos n elementos distintos $\Rightarrow$
$[K:\mathbb{F}_2] \geq n$.