15. $p(x) = x^q - x \in \mathbb{F}_p[x]$ $\qquad q = p^n$

a) $q(x) \in \mathbb{F}_p[x]$ irreducible de grado $n \overset{?}{\Longrightarrow} q(x) \mid x^q - x$

Cuerpo de descomposición de $q(x)$ sobre $\mathbb{F}_p$:

$$\mathbb{F}_p \hookrightarrow \mathbb{F}_p[x] / \langle q(x) \rangle \cong \mathbb{F}_{p^n}$$

↑ $q(x)$ tiene una raíz aquí

$\alpha_1, \dots, \alpha_n$ son las raíces de $q(x)$ (distintas porque $\mathbb{F}_p$ cuerpo perfecto y $q$ irred. $\Longrightarrow$ separable)

$$q(x) = \underbrace{(x-\alpha_1)\dots(x-\alpha_n)}_{} \in \mathbb{F}_{p^n}[x]$$

$q(x) \mid x^q - x$ porque estas son algunas de las raíces que $x^p - x$

$$\boxed{\begin{array}{l}\text{RECUERDO: Si } K \text{ es perfecto y } p(x) \in K[x] \Longrightarrow \\ \Longrightarrow p(x) \text{ es separable (todos sus factores irred. tienen raíces distintas)}\end{array}}$$

Podemos suponer p. ej. que $\deg(q_1(x)) \neq \deg(q_2(x))$

$$K \xrightarrow{\deg(q_1)} K[T]/\langle q_1(T)\rangle \longrightarrow \text{cuerpo de desc. de } q_1$$

$p(x)$ factoriza en factores lineales

$\wr\|$ $\longrightarrow$ isomorfos porque son cuerpos de $char(\cdot) = p$

$$K \xrightarrow{\deg(q_2)} K[T]/\langle q_2(T)\rangle$$

$p(x)$ factoriza en factores lineales

$\longrightarrow$ cuerpo de desc. de $q_2$.

~~Como son únicos~~

Como el cuerpo de desc. es único salvo isom. $\Rightarrow$

$\Rightarrow$ contradicción con los grados de la extensión.

$\boxed{13.}$ $x^{12} + 2x^6 + 1 \in \mathbb{F}_3[x]$

$\downarrow$ como estamos en característica 3 $(a+b)^3 = a^3 + b^3$

$$(x^4 + 2x^2 + 1)^3 \Longrightarrow ((x^2+1)^2)^3 \Longrightarrow \text{dos raíces distintas.}$$

$\mathbb{F}_{p^n}$ $\boxed{x^{p^n} - x}$

cuerpo de descomposición de

19. $\mathrm{char}(K) = p > 0 \Longrightarrow$ ISOMORFO A $\mathbb{F}_{p^n}$ (para alg... $n$)

$a \in K$ pero $\mathbb{F}_p \subset K$.

Demostrar que $p(x) = x^p - x - a \in K[x]$ o bien se descompone en factores lineales en $K[x]$ o bien es irreducible en $K[x]$.

$$p'(x) = p\,x^{p-1} - 1 = -1 \quad (\bar{p} = \bar{0} \text{ en } \mathbb{F}_p)$$

$\mathrm{mcd}(p(x), p'(x)) = 1 \Longrightarrow$ no tiene raíces múltiples.

1. Veamos que si $p(x)$ tiene una raíz en $K \Longrightarrow$ tiene todas las raíces en $K$.

Sup. que $\alpha \in K$ es una raíz de $p(x)$:

$$\alpha^p - \alpha - a = 0 \text{ en } K$$

Si $\beta \in \mathbb{F}_p \subset K \Longrightarrow \alpha + \beta$ también es raíz de $p(x)$: por te... Ferm... ($\beta\in$...

$$(\alpha+\beta)^p - (\alpha+\beta) - a = \alpha^p + \beta^p - \alpha - \beta - a = \beta^p - \beta = 0 \quad \forall \beta \in \mathbb{F}_p.$$

$\alpha, \alpha+1, \alpha+2, \dots, \alpha+(p-1)$ ~~son las raíces~~ de $p(x)$.

Obs: Si $\alpha$ es raíz de $p(x) \Longrightarrow \alpha \notin \mathbb{F}_p$
$(a \neq 0)$
porque todo elemento de $\mathbb{F}_p$ cumple que $\beta^p - \beta =$

2. Sup. ahora que $p(x) \in K[x]$ no tiene ninguna raíz en $K$.

$\overset{?}{\Longrightarrow}$ $p(x)$ es irreducible en $K[x]$.

Supongamos que $p(x)$ no es irred. en $K[x]$

$p(x) = q_1(x) \cdots q_r(x) \qquad q_i(x) \in K[x]$ irred.

¿Puede pasar que $\deg(q_1(x)) = \deg(q_2(x)) = \dots = \deg(q_r(x))$?

NO

10.1

$$\begin{tikzcd} M \arrow[d, dash, "\text{normal}"] \\ L \arrow[d, dash, "\text{normal}"] \\ K \end{tikzcd}$$

ormal?

Con la hipótesis de que todo $K$-aut de $L$ se extiende a uno de $M$

$p(x) = \mathrm{Irr}(\alpha, K)$

$$\begin{tikzcd} E \\ M \arrow[u] \\ L \arrow[u] \\ K \arrow[u] \end{tikzcd}$$

$p(x) = q_1(x) \cdots q_s(x)$ $L$

$gr(q_i) > 1$

$p(x)$

~~[illegible]~~ $\alpha \in M \subset E$

Supongamos $\alpha$ es raíz de $q_1(x) \Rightarrow$ todas las raíces de $q_1(x)$ estarían en $M$.

$q_2(x)$ y sea $\beta \in E$ una raíz de $q_2(x)$. $\exists$ un $\varphi \in Gal(E/K)$ tal que $\varphi(\alpha) = \beta$.

$$\begin{tikzcd} E \arrow[r, "\varphi"] & E \\ M \arrow[u, "\alpha"] \arrow[r, dashed, "\psi"] & M \arrow[u] \\ L \arrow[u] \arrow[r, "\varphi|_L \text{ extendido}"] & L \arrow[u] \\ & K \arrow[ul] \arrow[u] \end{tikzcd}$$

$\varphi(\alpha) = \beta$

$1_L : L$

$\varphi|_L \in Gal(L/K)$ ya que $L/K$ es normal.

$\varphi|_L : L[x] \longrightarrow L[x]$

$q_1(x) \longmapsto \varphi|_L(q_1(x)) = q_2(x)$

(porque $\varphi(\alpha) = \beta$)

$\psi(\alpha)$ es una raíz de $q_2(x) \Longrightarrow$

$\Longrightarrow M$ contiene todas las raíces de $q_2(x)$.

# TEOREMA ELEM. PRIMITIVO

$$\begin{tikzcd}
\mathbb{Q} \arrow[rr, hook] \arrow[dr, hook] & & \mathbb{Q}(\sqrt{2}, i, \sqrt[3]{5}) = \mathbb{Q}(\underbrace{\sqrt{2}+i}_{p(x)\text{ con } \deg(p)=4}, \underbrace{\sqrt[3]{5}}_{x^3-5}) \\
& \mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2}+i) \arrow[ur, hook] &
\end{tikzcd}$$

$$x^3-5 \longrightarrow \sqrt[3]{5}\cdot 1 = \beta, \quad \sqrt[3]{5}\,\xi_3 = b_2, \quad \sqrt[3]{5}\,\xi_3^2 = b_3$$

$$\mathbb{Q} \hookrightarrow \mathbb{Q}(\sqrt{2}) \hookrightarrow \mathbb{Q}(\sqrt{2}, i)$$

$$(\sqrt{2}+i)^2 = x^2$$

$$x^2 - 1 + 2i\sqrt{2} \in \mathbb{Q}(\sqrt{2}i)$$

$$\alpha = \sqrt{2}+i \qquad -\sqrt{2}-i = a_2$$

$$a_3 = \sqrt{2}-i \qquad -\sqrt{2}+i = a_4$$

Buscamos $c \neq \dfrac{\alpha - \alpha_i}{b_j - \beta}$

$$\sqrt{2}+i - \begin{pmatrix} -\sqrt{2}-i \\ +\sqrt{2}-i \\ -\sqrt{2}+i \end{pmatrix} = \begin{matrix} 2\sqrt{2} \\ 2i \\ 2\sqrt{2} \end{matrix}$$

$$\cancel{\sqrt[3]{5}} \quad b_j - \beta = \sqrt[3]{5}\begin{pmatrix} \xi_3 - 1 \\ \xi_3^2 - 1 \end{pmatrix} = \begin{matrix} \sqrt[3]{5}\left(\frac{-1}{2} + \frac{\sqrt{3}}{2}i\right) \\ \sqrt[3]{5}\left(\frac{-1}{2} - \frac{\sqrt{3}}{2}i\right) \end{matrix}$$

$$\theta = \alpha + c\beta$$

$\uparrow$

Elemento primitivo

$\boxed{15.}$ $f = x^{12} + 2x^6 + 1 \in \mathbb{F}_3[x]$

Veamos las raíces en $\mathbb{F}_3$:

$$\left.\begin{array}{l} 0+0+1 \neq 0 \\ 1+2+1 = 4 = 1 \neq 0 \\ 1+2+1 \neq 0 \end{array}\right\}$$

no tiene raíces (eso no quiere decir que sea irred.)

Vemos que $f(x) \in \mathbb{F}_3[x^3]$: $(x^3)^4 + 2(x^3)^2 + 1 = (x^4)^3 + 2(x^2)^3$

$= (x^4 + 2x^2 + 1)^3 = ((x^2+1)^2)^3$

Entonces las raíces (distintas!) de $f(x)$ son las mismas que las de $x^2+1$.

$g(x) = x^2 + 1$, es irreducible en $\mathbb{F}_3$.

Sabemos que $\mathbb{F}_3(g)/\mathbb{F}_3$ es una extensión separable

$g(x)$ tiene 2 raíces distintas en su cuerpo de escisión.

Cuerpo de escisión: $\mathbb{F}_3[t]/\langle t^2+1 \rangle$ (cuerpo de 9 elementos)

Consideramos ahora $\mathbb{F}_3[x] \hookrightarrow \left(\mathbb{F}_3[t]/\langle t^2+1\rangle\right)[x]$

$$= \{\underbrace{0,1,2}_{\text{estas ya sabemos que no son raíces}}, \underbrace{t, 1+t, 2+t, 2t, 1+2t, 2+2t}_{\text{cogemos y los probamos a ver cuales son raíces}}\}$$

Descomposición de $f(x)$ en su cuerpo de escisión:

$f(x) = (x-t)^6(x-2t)^6$

$\underline{18.}$ $f(x) = X - X \in \mathbb{F}_p[X]$, con $q = p$

a) $g(x) \in \mathbb{F}_p[x]$ irred. de grado $n \Longrightarrow g \mid f$

$K := \mathbb{F}_p(f) \cong \mathbb{F}_q = \{\alpha_1, \dots, \alpha_q\}$

$$f(x) = \prod_{i=1}^{q} (x - \alpha_i)$$ Todos son raíces de $f$

¿ $g(x)$ tiene una raíz en $K$?

Teorema de Kronecker nos asegura que:

$L := \mathbb{F}_p[t]/\langle g \rangle$ es una extensión de $\mathbb{F}_p$, de grado $n$ que contiene una raíz de $g$.

$g \in L[x]$ tiene una raíz en $L$.

El $T^{ma}$ de clasificación de cuerpos finitos nos asegura:

$$\exists \phi : \quad \begin{array}{ccc} & \phi: K \cong L & \\ & \diagdown \quad \diagup & \\ & \mathbb{F}_p & \end{array} \qquad K[x] \longrightarrow L[x] \qquad \mathbb{F}_p \longleftarrow \boxed{g \in \mathbb{F}_p[x]}$$

Si $g$ tiene una raíz en $L$, la tiene en $K$ (imagen del isomorfismo).

~~$\exists \alpha \in K$ con $(x-\alpha) \mid g(x)$ pero $g(x)$ es irreducible $\Longrightarrow$~~

ORMA 1 $\Longrightarrow$

Como $K$ es una extensión normal $\Longrightarrow g(x)$ se escinde en $K$. $\Longrightarrow f = g \cdot \prod_{i=n+1}^{q} (x - \alpha_i)$ (alg. de la div.)

RMA 2

$$\left.\begin{array}{l}(x-\alpha) \mid g \\ (x-\alpha) \mid f\end{array}\right\} \Rightarrow (x-\alpha) \mid \underbrace{\mathrm{mcd}_{K[x]}(f, g)}_{\substack{\| \\ 1}} = \mathrm{mcd}_{\mathbb{F}_p[x]}(f, g)$$

Como $g$ irred. $\Longrightarrow g \mid f$.

b) Demuestra que el grado de todos los factores irred. de $f$ divide a $n$.

Sea $g \in \mathbb{F}_p[x]$ factor irred., con $gr(g) = d$.

$\mathbb{K} := \mathbb{F}_p(f)$ $\quad$ $g$ se escinde en $\mathbb{K}$.

Sea $\alpha \in \mathbb{K}$ una raíz de $g$, $\mathbb{F}_p(\alpha) \subseteq \mathbb{K}$.

$$\begin{tikzcd}
 & \mathbb{K} := \mathbb{F}_p(f) \arrow[dd, dash, "n"] \\
\mathbb{F}_p(\alpha) \arrow[ur, dash] \arrow[dr, dash, "d"'] & \\
 & \mathbb{F}_p
\end{tikzcd}$$

Por el T$^{ma}$ del Elem. Alg.

$$|\mathbb{F}_p(\alpha) : \mathbb{F}_p| = d.$$

$$n = |\mathbb{K} : \mathbb{F}_p| = |\mathbb{K} : \mathbb{F}_p(\alpha)| \cdot |\mathbb{F}_p(\alpha) : \mathbb{F}_p| = |\mathbb{K} : \mathbb{F}_p(\alpha)| \cdot d$$

$\boxed{21.}$ $\operatorname{char}(\mathbb{K}) = p$ $\qquad$ $f(x) = x^p - x + a$

$a \in \mathbb{K}$

Comprobar que $f$ se escinde en $\mathbb{K}$ o bien es irred.

$f$ tiene $p$ raíces distintas en $\mathbb{K}(f)$

$\{\alpha_1, \alpha_2, \dots, \alpha_p\}$ $\qquad$ $(\alpha_i - \alpha_j)^p = \alpha_i^p - \alpha_j^p = \alpha_i - \alpha_j$

Si fijamos $\alpha_1$: $(*) = \{\underline{\alpha_1}, \alpha_1 + 1, \alpha_1 + 2, \dots, \alpha_1 + (p-1)\}$

Hay dos opciones

- $\to$ $\alpha_1 \in \mathbb{K}$ : todas las raíces están en $\mathbb{K} \Rightarrow$ $\Rightarrow$ se escinde.
- $\to$ $\alpha_1 \notin \mathbb{K}$ : $[\dots] \Rightarrow$ no tiene ninguna raíz en $\mathbb{K} \Rightarrow [\dots] \Rightarrow f$ es irred.

## Pregunta extra:

¿Cuántos isomorfismos hay entre estos pares de cuerpos?

a) $\mathbb{F}_3[x]/\langle x^2+1\rangle$ y $\mathbb{F}_3[t]/\langle t^2+t+2\rangle$

b) $\mathbb{F}_3[x]/\langle x^2+1\rangle$ y $\mathbb{F}_2[t]/\langle t^3+t+1\rangle$

$\boxed{9.}$ $E = \mathbb{Q}(\sqrt[4]{2})$

$L = \mathbb{Q}(\sqrt{2})$

$K = \mathbb{Q}$

$$\begin{array}{c} E \\ | \\ L \\ | \\ K \end{array} \begin{array}{l} \left.\right\} \text{es normal } E = L(x^2-\sqrt{2}) = L(\pm\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}) \\ \left.\right\} \text{es normal } L = K(x^2-2) = \mathbb{Q}(\pm\sqrt{2}) \end{array}$$

Sin embargo, $E/K$ no es normal por que el polinomio <u>irreducible sobre $K$</u> $x^4-2$ tiene dos raíces en $E$ pero <u>no</u> se escinde en $E$ (Teorema 3.9)

<u>Ejemplo ejercicio examen</u>: Sea $f(x) = x^4-2 \in \mathbb{Q}[x]$

a) $E = \mathbb{Q}(f)$

b) $|E:\mathbb{Q}|$

c) Determinar $\alpha \in E$ tal que $\mathbb{Q}(\alpha) = E$

a) Las raíces de $f$ son $\{\pm\sqrt[4]{2}, \pm\sqrt[4]{2}\,i\}$, entonces $E = \mathbb{Q}(\pm\sqrt[4]{2}, \pm\sqrt[4]{2}\,i) = \mathbb{Q}(\sqrt[4]{2}, i)$

b) $\mathbb{Q} \subseteq \mathbb{Q}(i), \mathbb{Q}(\sqrt[4]{2}) \subseteq E$

$$\begin{array}{l} E = \mathbb{Q}(\sqrt[4]{2})(i) \\ | \quad 2 = gr(Irr(\mathbb{Q}(\sqrt[4]{2}), i)) = gr(x^2+1) \\ \mathbb{Q}(\sqrt[4]{2}) \\ | \quad 4 = gr(Irr(\mathbb{Q}, \sqrt[4]{2})) = gr(x^4-2) = 4 \\ \mathbb{Q} \end{array}$$

$\pm i \notin \mathbb{Q}(\sqrt[4]{2})$

c) Hay dos formas:

c1] Usando la dem. del T.E.P. caso infinito

$E = \mathbb{Q}(\underset{\alpha}{\underset{\shortparallel}{i}}, \underset{\beta}{\underset{\shortparallel}{\sqrt[4]{2}}})$ $\quad \alpha_1 = i \quad \alpha_2 = -i \leftarrow$ raíces de $x^2+1$

$\beta_1 = \sqrt[4]{2} \quad \beta_2 = -\sqrt[4]{2} \quad \beta_3 = \sqrt[4]{2}\,i \quad \beta_4 = -\sqrt[4]{2}\,i \leftarrow$

raíces de $x^4-2$

Escoger $c \in \mathbb{K}$ tal que $c \neq \frac{\beta - \beta_j}{\alpha - \alpha_2}$ $j = 1,2,3,4$

$\alpha = \alpha_1$

$\beta = \beta_1$

podeis ver que $c = -1$ sirve

(hay que comprobarlo calculando los cocientes de diferencias

Por la prueba del T.E.P., $E = \mathbb{Q}(\alpha - \beta) = \mathbb{Q}(-\alpha - \beta) =$
$= \mathbb{Q}(\alpha + \beta) = \mathbb{Q}(\sqrt[4]{2} + i)$

c.2] Usando todo lo que hemos visto:

$$8 \left\{ \begin{array}{l} E = L(\sqrt[4]{2}) \\ \quad | \\ L = \mathbb{Q}(i) \\ \quad | \; \} 2 \\ \mathbb{Q} \end{array} \right.$$

Por b) $|E : \mathbb{Q}| = 8$

$|\mathbb{Q}(i) : \mathbb{Q}| = 2 \Rightarrow |E : L| = 4$

$\Rightarrow Irr(L, \sqrt[4]{2}) = x^4 - 2$

$\alpha = \sqrt[4]{2} + i$, por el T.E.Alg. queremos ver que $gr(Irr(\mathbb{Q}, \alpha)) = 8$

$Irr(L, \sqrt[4]{2}) = x^4 - 2 = f$

$p(x) = (x-i)^4 - 2 = f(x-i)$

$\alpha$ es una raíz de $p \in L[x]$, $p \notin \mathbb{Q}[x]$

Por el ejercicio 32 a) de la hoja 1, $p$ es irreducible sobre $L$, es decir, $p(x) = (x-i)^4 - 2 = Irr(L, \alpha)$

$$\begin{array}{ll} E & \\ | & \\ L & p = Irr(L, \alpha) \notin \mathbb{Q}[x] \\ | & \\ \mathbb{Q} & q = Irr(\mathbb{Q}, \alpha) \in \mathbb{Q}[x] \end{array}$$

Sabemos que $p | q$ en $L \Rightarrow \underset{4}{\underset{\shortparallel}{gr(p)}} < gr(q)$

Por el ejercicio 16.c) de la H2, $gr(q) \big| |E : \mathbb{Q}| = 8 \Rightarrow$
$\Rightarrow gr(q) = gr(Irr(\mathbb{Q}, \alpha)) = 8 \Rightarrow E = \mathbb{Q}(\alpha)$

d) Ahora decide si $\sigma: \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{2})$ se
$\qquad\qquad\qquad\qquad\quad \sqrt{2} \longmapsto -\sqrt{2}$

puede extender a un isomorfismo de $\mathbb{Q}(\sqrt[4]{2})$ o de $\overset{\mathbb{Q}(\sqrt[4]{2}i}{\overset{\shortparallel}{E}}$.

$\to$ TEO. 3.12

Recordar que si $E/K$ es normal y $M/K$ es normal, entonces todo $\sigma \in Gal(M/K)$ se puede extender a $Gal(E/K)$.

$$\begin{array}{l} M = \mathbb{Q}(\sqrt[4]{2}) \\ \quad | \\ \; = \mathbb{Q}(\sqrt{2}) \\ \quad | \;\} \text{ es normal} \\ \mathbb{Q} \end{array} \qquad \text{(no es normal)}$$

$M = \mathbb{Q}(\sqrt[4]{2})$

$E/\mathbb{Q}$ es normal

$M/\mathbb{Q}$ no es normal

$\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ es normal

$\sigma$ <u>no</u> se puede extender a un isomorfismo de $M$

<u>R.A.</u> Supongamos $\tau: M \longrightarrow M$ es una extensión de $\sigma$

Entonces $\tau(\sqrt[4]{2}) = \begin{cases} \sqrt[4]{2} \\ \text{o} \\ -\sqrt[4]{2} \end{cases}$, porque $\tau$ lleva raíces de pol. sobre $\mathbb{Q}$ en raíces de pol. sobre $\mathbb{Q}$.

$$\tau(\sqrt{2}) = \tau((\sqrt[4]{2})^2) = \tau(\sqrt[4]{2})^2 = (\pm\sqrt[4]{2})^2 = \sqrt{2}$$

$$\overset{\shortparallel}{\sigma(\sqrt{2})} = -\sqrt{2} \neq \sqrt{2}$$

Por otro lado:

$$\begin{array}{l} E \\ | \\ \mathbb{Q}(\sqrt{2}) \\ | \;\} \text{ normal} \\ \mathbb{Q} \end{array} \qquad \text{normal (}E/\mathbb{Q}\text{)}$$

Por el teo. 3.12 $\sigma$ se extiende a un isom. $\omega$ de $E$

$\left( \begin{array}{l} \sigma \in Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \\ \omega \in Gal(E/\mathbb{Q}) \end{array} \right)$

<u>TEOREMA 3.12</u> (REFORMULACIÓN): $E/K$ es normal, $K \subseteq L \subseteq E$, $L/K$ es normal $\Longleftrightarrow$ todo elemento de $\sigma \in Gal(L/K)$ se puede extender a $Gal(E/K)$.

Otra forma: Sea $\omega \in Gal(E/\mathbb{Q})$ tal que $\omega(\sqrt[4]{2}) = \sqrt[4]{2}\, i$

(Existe uno porque $\sqrt[4]{2}$ y $\sqrt[4]{2}\, i$ son raíces del mismo polinomio irreducible)

Entonces $\omega(\sqrt{2}) = \omega((\sqrt[4]{2})^2) = \omega(\sqrt[4]{2})^2 = (\sqrt[4]{2}\, i)^2 =$
$= -\sqrt{2} = \sigma(\sqrt{2})$. ∎

$\boxed{0.}$ Todos son verdaderos

10. f) $E/L$ y $L/K$ son extensiones normales. Si todo $\sigma \in Gal(L/K)$ se extiende a $E$ ($Gal(E/K)$) entonces $E/K$ es normal.

Sol. en moodle.

Obs: Se puede usar para ver que $\sigma \in Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ $\sigma(\sqrt{2}) = -\sqrt{2}$. No se puede extender a $M = \mathbb{Q}(\sqrt[4]{2})$

Por 10.f, si se extendiera, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ es normal. #

$\boxed{4.}$ $K = \mathbb{F}_2[x] / \langle y^3+y+1 \rangle$ es cuerpo de escisión de

$\underbrace{x^3+x+1}$ y $\underbrace{x^3+x^2+1}$ → Son irreducibles porque no tienen raíces!

Sol:

$$K = \{\bar{0}, \bar{1}, \bar{y}, \overline{y+1}, \overline{y^2}, \overline{y^2+1}, \overline{y^2+y}, \overline{y^2+y+1}\}$$

Por Kronecker, $y \in K$ es raíz de $x^3+x+1$

También sabemos que si $\sigma \in Gal(K/\mathbb{F}_2)$ entonces $\sigma(y)$ es raíz de $x^3+x+1$

$\varphi = Frob \in Gal(K/\mathbb{F}_2)$, $\varphi^2 \in Gal(K/\mathbb{F}_2)$

$\varphi(y) = y^2$ es otra raíz. → aplicamos Frob again!

$\varphi^2(y) = \varphi(y^2) = y^4 = y \cdot y^3 = y^2+y.$

Elevamos a $p=2$ porque $\mathbb{F}_2$ tiene característica 2.