

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

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

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 \wedge q irred. \Rightarrow separable)

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

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

RECUERDO:

Si K es perfecto y $p(x) \in K[x] \Rightarrow$
 $\Rightarrow p(x)$ es separable (todos sus factores irred. tienen raíces distintas)

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

$K \xrightarrow{\deg(q_1)} K[T]/\langle q_1(T) \rangle \rightarrow$ cuerpo de desc. de q_1
 $\searrow \deg(q_2) \quad \swarrow$ $K[T]/\langle q_2(T) \rangle \rightarrow$ cuerpo de desc. de q_2

\cong isomorfos porque son cuerpos de $\text{char}(\cdot) = p$

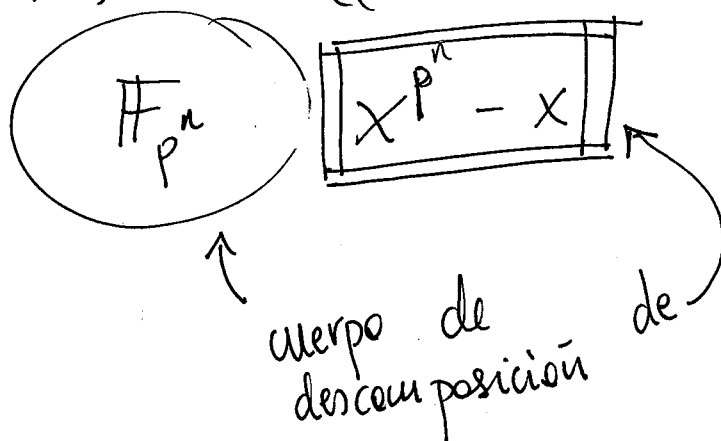
\rightarrow $p(x)$ factoriza en factores lineales

~~Cuerpo~~ son únicos
Como el cuerpo de desc. es único salvo isom. \Rightarrow
 \Rightarrow contradicción con los grados de la extensión.

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

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

$(x^4 + 2x^2 + 1)^3 \Rightarrow ((x^2 + 1)^2)^3 \Rightarrow$ as raízes distintas.



19. $\text{char}(\mathbb{K}) = p > 0 \Rightarrow \text{ISOMORFO A } \mathbb{H}_p^n$ (para alg
 $a \in \mathbb{K}$ pero $\mathbb{F}_p \subset \mathbb{K}$.

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

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

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

1. Veamos que si $p(x)$ tiene una raíz en $\mathbb{K} \Rightarrow$ tiene todas las raíces en \mathbb{K} .

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

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

Si $\beta \in \mathbb{F}_p \subset \mathbb{K} \Rightarrow \alpha + \beta$ también es raíz de $p(x)$: ^{por} _{Fe}

$$(\alpha + \beta)^p - (\alpha + \beta) - a = (\alpha^p + \beta^p - \alpha - \beta - a) = \beta^p - \beta = 0 \quad \left\{ \begin{array}{l} \text{por Fe} \\ \text{por } \beta \in \mathbb{F}_p \end{array} \right.$$

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

Obs: Si α es raíz de $p(x) \Rightarrow \alpha \notin \mathbb{F}_p$
 $(a \neq 0)$

porque todo elemento de \mathbb{F}_p cumple que $\beta^p - \beta = 0$

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

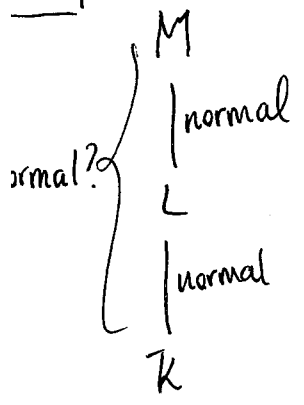
$\stackrel{?}{\Rightarrow} p(x)$ es irreducible en $\mathbb{K}[x]$.

Supongamos que $p(x)$ no es irred. en $\mathbb{K}[x]$

$$p(x) = q_1(x) \cdots q_r(x) \quad q_i(x) \in \mathbb{K}[x] \text{ irred.}$$

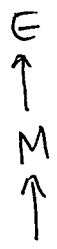
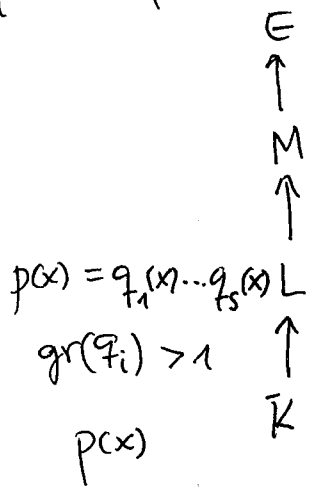
¿Puede pasar que $\deg(q_1(x)) = \deg(q_2(x)) = \dots = \deg(q_r(x))$?

NO



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

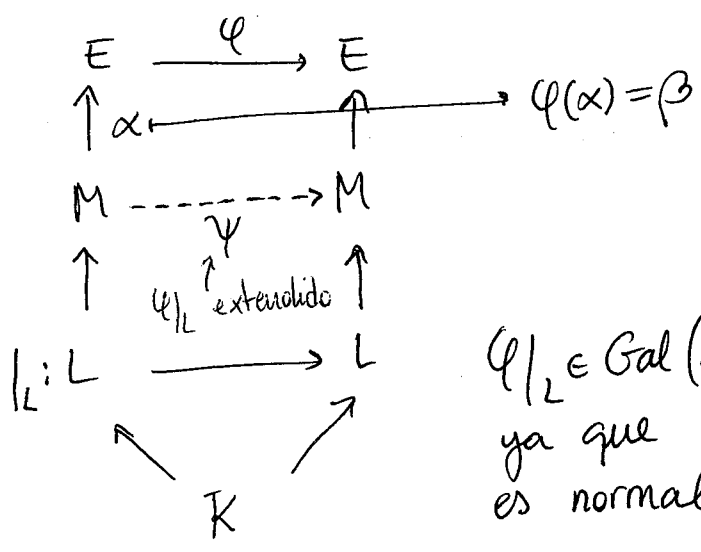
$$p(x) = \text{Irr}(\alpha, K)$$



~~Let~~ $\alpha \in M \subseteq E$

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

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



$\varphi|_L \in \text{Gal}(L/K)$
 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 $\varphi(\alpha) = \beta$)

$\psi(x)$ es una raíz de $q_2(x) \Rightarrow$
 $\Rightarrow M$ contiene todas las raíces de $q_2(x)$.

TEOREMA ELEM. PRIMITIVO

$$\mathbb{Q} \hookrightarrow \mathbb{Q}(\sqrt{2}, i, \sqrt[3]{5}) = \mathbb{Q}(\underbrace{\sqrt{2}+i}, \underbrace{\sqrt[3]{5}})$$

$$\begin{array}{c} \searrow \\ \mathbb{Q}(\sqrt{2}, i) \\ \parallel \\ \mathbb{Q}(\sqrt{2}+i) \end{array} \nearrow$$

$p(x)$
con $\deg(p)=4$

$$\begin{array}{c} x^3-5 \\ \downarrow \quad \searrow \quad \swarrow \\ \sqrt[3]{5} \cdot 1 \quad \sqrt[3]{5} \cdot \omega \quad \sqrt[3]{5} \cdot \omega^2 \\ \parallel \quad \parallel \quad \parallel \\ \beta \quad b_2 \quad b_3 \end{array}$$

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

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

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

$$\alpha = \sqrt{2} + i \quad -\sqrt{2} - i = \alpha_2$$

$$\alpha_3 = \sqrt{2} - i \quad -\sqrt{2} + i = \alpha_4$$

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

$$\sqrt{2} + i - \begin{pmatrix} -\sqrt{2} - i \\ +\sqrt{2} - i \\ -\sqrt{2} + i \end{pmatrix} = \begin{array}{l} \nearrow 2\sqrt{2} \\ \rightarrow 2i \\ \searrow 2\sqrt{2} \end{array}$$

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

$$= \sqrt[3]{5} \left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i \right)$$

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

\uparrow
Elemento primitivo

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

Veamos las raíces en \mathbb{F}_3 :

$$\left. \begin{array}{l} 0+0+1 \neq 0 \\ 1+2+1 = 4 = 1 \neq 0 \\ 1+2+1 \neq 0 \end{array} \right\} \begin{array}{l} \text{no tiene raíces} \\ \text{(eso no quiere} \\ \text{decir que sea)} \\ \text{irred.} \end{array}$$

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

$\{0, 1, 2, t, 1+t, 2+t, 2t, 1+2t, 2+2t\}$
 están ya sabemos que no son raíces

↓
 cogemos y los probamos a ver cuáles son raíces.

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

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

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

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

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

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

¿ $g(x)$ tiene una raíz en \mathbb{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 τ^{me} de clasificación de cuerpos finitos nos asegura:

$$\exists \phi: \begin{array}{ccc} \mathbb{K} & \cong & L \\ & \searrow & \swarrow \\ & \mathbb{F}_p & \end{array} \quad \begin{array}{ccc} \mathbb{K}[x] & \longrightarrow & L[x] \\ & \nwarrow & \\ & \boxed{g \in \mathbb{F}_p[x]} & \end{array}$$

Si g tiene una raíz en L , la tiene en \mathbb{K} (imagen del isomorfismo).

~~$\exists \alpha \in \mathbb{K}$ con $(x - \alpha) | g(x)$ pero $g(x)$ es irreducible \Rightarrow~~

ORMA 1

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

RMA 2

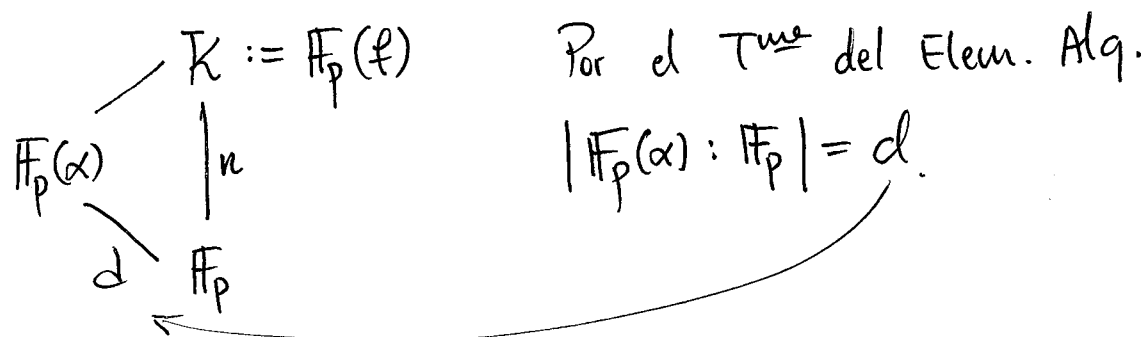
$$\left. \begin{array}{l} (x - \alpha) | g \\ (x - \alpha) | f \end{array} \right\} \Rightarrow (x - \alpha) | \underbrace{\text{mcd}_{\mathbb{K}[x]}(f, g)}_{\neq 1} = \text{mcd}_{\mathbb{F}_p[x]}(f, g) \quad \begin{array}{l} \text{Como } g \text{ irred.} \\ \Rightarrow g | f. \end{array}$$

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 $\text{gr}(g) = d$.

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

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



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

21. $\text{char}(K) = p$ $f(x) = x^p - x + a$
 $a \in K$

Comprobar que f se escinde en K o bien es irred.

f tiene p raíces distintas en $K(\ell)$

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

Si fijamos α_1 : $\circledast = \{\alpha_1, \alpha_1 + 1, \alpha_1 + 2, \dots, \alpha_1 + (p-1)\}$

Hay dos opciones

$\rightarrow \alpha_1 \in K$: todas las raíces están en $K \Rightarrow$ se escinde.
 $\rightarrow \alpha_1 \notin K$: [...] \Rightarrow no tiene ninguna raíz en $K \Rightarrow$ [...] $\Rightarrow f$ 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 $\mathbb{F}_2[t] / \langle t^3 + t + 1 \rangle$

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

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

$$K = \mathbb{Q}$$

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

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

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

Ejemplo ejercicio examen: 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) $\mathbb{Q} \subseteq \mathbb{Q}(i), \mathbb{Q}(\sqrt[4]{2}) \subseteq E$

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

$$\begin{array}{l} | \\ \mathbb{Q}(\sqrt[4]{2}) \end{array} \left. \vphantom{\begin{array}{l} | \\ \mathbb{Q}(\sqrt[4]{2}) \end{array}} \right\} 2 = \text{gr}(\text{Irr}(\mathbb{Q}(\sqrt[4]{2}), i)) = \text{gr}(x^2 + 1)$$

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

$$\begin{array}{l} | \\ \mathbb{Q} \end{array} \left. \vphantom{\begin{array}{l} | \\ \mathbb{Q} \end{array}} \right\} 4 = \text{gr}(\text{Irr}(\mathbb{Q}, \sqrt[4]{2})) = \text{gr}(x^4 - 2) = 4$$

c) Hay dos formas:

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

$$E = \mathbb{Q}(\underset{\alpha}{i}, \underset{\beta}{\sqrt[4]{2}})$$

$$\alpha_1 = i$$

$$\alpha_2 = -i$$

$$\leftarrow \text{raíces de } x^2 + 1$$

$$\beta_1 = \sqrt[4]{2}$$

$$\beta_2 = -\sqrt[4]{2}$$

$$\beta_3 = \sqrt[4]{2}i$$

$$\beta_4 = -\sqrt[4]{2}i$$

$$\leftarrow \text{raíces de } x^4 - 2$$

Escoger $c \in \mathbb{Q}$ tal que $c \neq \frac{p_j - p_i}{\alpha - \alpha_j}$ $j = 1, 2, 3, 4$
 $\alpha = \alpha_1$
 $\beta = \beta_1$

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:

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

Por b) $|E : \mathbb{Q}| = 8$
 $|\mathbb{Q}(i) : \mathbb{Q}| = 2 \Rightarrow |E : L| = 4$
 $\Rightarrow \text{Irr}(L, \sqrt[4]{2}) = x^4 - 2$

$\alpha = \sqrt[4]{2} + i$, por el T.E.Alg. queremos

ver que $\text{gr}(\text{Irr}(\mathbb{Q}, \alpha)) = 8$

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

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

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

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

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

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

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

d) Ahora decide si $\sigma: \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{2})$ se puede extender a un isomorfismo de $\mathbb{Q}(\sqrt[4]{2})$ o de E .

→ TEO. 3.12

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

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

E/\mathbb{Q} es normal

M/\mathbb{Q} no es normal

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

$$\begin{array}{l} M = \mathbb{Q}(\sqrt[4]{2}) \\ \left. \begin{array}{l} \text{no es normal} \\ \text{no es normal} \end{array} \right\} \begin{array}{l} \downarrow \\ \mathbb{Q}(\sqrt{2}) \\ \downarrow \\ \mathbb{Q} \end{array} \end{array} \quad \begin{array}{l} \text{es normal} \end{array}$$

σ no se puede extender a un isomorfismo de M .
R.A. Supongamos $\tau: M \rightarrow M$ es una extensión de σ .
 Entonces $\tau(\sqrt[4]{2}) = \begin{matrix} \swarrow \sqrt[4]{2} \\ \searrow -\sqrt[4]{2} \end{matrix}$, porque τ lleva raíces

de pol. sobre \mathbb{Q} en raíces de pol. sobre \mathbb{Q} .

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

$$\sigma(\sqrt{2}) = -\sqrt{2} \quad \swarrow \quad \text{no}$$

Por otro lado:

Por el teo. 3.12 σ se extiende a un isom. ω de E de $(\sigma \in \text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}))$
 $(\omega \in \text{Gal}(E/\mathbb{Q}))$

$$\begin{array}{l} \text{normal} \left\{ \begin{array}{l} E \\ \downarrow \\ \mathbb{Q}(\sqrt{2}) \\ \downarrow \\ \mathbb{Q} \end{array} \right\} \text{normal} \end{array}$$

TEOREMA 3.12 (REFORMULACIÓN): E/K es normal,
 $K \subseteq L \subseteq E$, L/K es normal \iff todo
 elemento de $\sigma \in \text{Gal}(L/K)$ se puede
 extender a $\text{Gal}(E/K)$.

Otra forma: Sea $\omega \in \text{Gal}(E/\mathbb{Q})$ 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)

$$\begin{aligned}\text{Entonces } \omega(\sqrt{2}) &= \omega((\sqrt[4]{2})^2) = \omega(\sqrt[4]{2})^2 = (\sqrt[4]{2}i)^2 = \\ &= -\sqrt{2} = \sigma(\sqrt{2}).\end{aligned}$$

0.] Todas son verdaderas

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

Sol. en moodle.

Obs: Se puede usar para ver que $\sigma \in \text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$
 $\sigma(\sqrt{2}) = -\sqrt{2}$. 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. ~~///~~

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

$$\underbrace{x^3 + x + 1} \quad y \quad \underbrace{x^3 + x^2 + 1}$$

Sol:

→ Son irreducibles porque no tienen raíces!

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

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

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

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

$\varphi(y) = y^2$ es otra raíz. → apliquemos 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.

