ERROR 1: aplicar criterios de irreducibilidad sobre $K \neq \mathbb{Q}$.
(Eisenstein y red. mod p <u>no</u> se pueden usar fuera de $\mathbb{Q}$)

Ejemplo: $E = \mathbb{Q}(\sqrt[6]{3}, i)$

$K = \mathbb{Q}(i)$

Sabemos que $E = K(\sqrt[6]{3})$ — Eisenstein

$\mathrm{Irr}(K, \sqrt[6]{3}) \mid \mathrm{Irr}(\mathbb{Q}, \sqrt[6]{3}) = x^6 - 3$

$\Downarrow$

$gr(\mathrm{Irr}(K, \sqrt[6]{3})) \leq 6$ (tendremos que ver que es 6)

¿Cómo se puede hacer?

$$\begin{tikzcd}
& E = F(i) = K(\sqrt[6]{3}) & \\
F = \mathbb{Q}(\sqrt[6]{3}) \arrow[ur, "(*)\ 2"] & & K = \mathbb{Q}(i) \arrow[ul] \\
& \mathbb{Q} \arrow[ul, "6"] \arrow[ur, "2"'] &
\end{tikzcd}$$

$|F:\mathbb{Q}| = 6$
y $|E:F| = 2$ porque x^2+1 no tiene raíces en $F \subseteq \mathbb{R}$ y por tanto $\underset{(*)}{\mathrm{Irr}(F,i) = x^2+1}$

Por tanto, $|E:K| = \dfrac{|E:\mathbb{Q}|}{|K:\mathbb{Q}|} = 6$

En particular, $\mathrm{Irr}(K, \sqrt[6]{3}) = x^6 - 3$

ERROR 2 | Calcular los órdenes de los elementos del grupo de Galois de una extensión.

Ejemplo: $E = \mathbb{Q}(\sqrt[6]{3}, i)$ $\quad G = Gal(E/K)$

$K = \mathbb{Q}(i)$

E/K de Galois, $|G| = 6$

$\alpha = \sqrt[6]{3}$, $\xi = \frac{1}{2} + \frac{\sqrt{3}}{2} i$

$x^6 - 3 \longrightarrow \{\alpha \xi^j \mid j = 0, \dots, 5\}$ $\quad$ Base de $E = K(\alpha)$

$\{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5$

G	α	α^3	ξ	orden
τ_0	α	α^3	ξ	1
τ_1	$\alpha\xi$	$-\alpha^3$	ξ^5	2
τ_2	$\alpha\xi^2$	α^3	ξ	$\vdots$
τ_3	$\alpha\xi^3$	$-\alpha^3$	ξ^5	
τ_4	$\alpha\xi^4$	α^3	ξ	
τ_5	$\alpha\xi^5$	$-\alpha^3$	ξ^5	

Calculando órdenes:

$\alpha \xrightarrow{\tau_1} \alpha\xi \xrightarrow{\tau_1} \tau_1(\alpha\xi) = \tau_1(\alpha)\tau_1(\xi) = \alpha\xi \boxed{\tau_1(\xi)}$?

[...]

$\Rightarrow G \cong S_3$

PARA PRÁCTICAR: $x^8 - 3$ $\quad$ con $\quad K = \mathbb{Q}(i), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3})$

Otro ejemplo: ejercicio 5c HOJA 4

$$E = \mathbb{Q}(\underbrace{x^4+4x^2+2}_{p(x)}) = \mathbb{Q}(\sqrt{-2+\sqrt{2}})$$

~~raíces d~~ Raíces de $p(x)$: $\{\pm\alpha, \pm\beta\}$ con $\alpha = \sqrt{-2+\sqrt{2}}$, $\beta = \sqrt{-2-\sqrt{2}}$

$$\alpha\beta = \sqrt{2} = \alpha^2+2 = -\beta^2-2 \Longrightarrow \boxed{\alpha = -(\beta^2+2)\beta^{-1}} \ (*)$$

$$\beta = (\alpha^2+2)\alpha^{-1} \in \mathbb{Q}(\alpha) \quad \text{y} \quad \sqrt{2} \in \mathbb{Q}(\alpha)$$

$$\Rightarrow E = \mathbb{Q}(\alpha,\beta) = \mathbb{Q}(\alpha)$$

G	α	orden
1	α	1
σ	$-\alpha$	2
τ	β	
$\sigma\tau$	$-\beta$	

$\rightarrow$ ¿pero este orden?

$$\alpha \xrightarrow{\tau} \beta \xrightarrow{\tau} ¿\tau(\beta)?$$

$\downarrow$

Hay que escribir β en función de α $\{1, \alpha, \alpha^2, \alpha^3\}$

$\rightarrow$ Sabemos que $\beta = (\alpha^2+2)\alpha^{-1}$

$$\Rightarrow \tau(\beta) = (\beta^2+2)\beta^{-1} = -\alpha \ (*)$$

$$\Rightarrow \operatorname{ord}(\tau) > 2 \Longrightarrow \operatorname{ord}(\tau) = 4$$

$$\Rightarrow \operatorname{Gal}(E/K) = C_4$$

$\boxed{\text{PRACTICAR: } x^4+6x^2+4}$ (sale $C_2 \times C_2$)

$\boxed{\text{ERROR 3}}$ No pensar al calcular las subextensiones

Ejemplo: $E = \mathbb{Q}(\sqrt[6]{3}, i)$ $\qquad |E:K| = 6$

$K = \mathbb{Q}(i)$

$$\begin{tikzcd}
 & E \arrow[dl, no head] \arrow[dr, no head] & \\
K(\sqrt{3}) \arrow[dr, no head, "2"'] & & K(\sqrt[3]{3}) \arrow[dl, no head] \\
 & K = \mathbb{Q}(i) &
\end{tikzcd}$$

normal

$K(\sqrt[3]{3})$ → No es normal, no está $\sqrt{3}$

→ Esto ya nos hubiese dicho que $Gal(E/K) \cong S_3$

subext. propios de E/K $\xleftrightarrow{\text{TFTG}}$ subgr. propios de S_3

- una única subext. de grado 2 sobre K $\Rightarrow \boxed{K(\sqrt{3})}$ ⟷ – un subgr. de orden 3 (normal)
- tres subext. de grado 3 sobre K $\boxed{\text{CONJUGADAS}}$ ⟷ – tres subgrupos de ~~de~~ orden 2 conjugados

$\Rightarrow$ tenemos una $K(\sqrt[3]{3})$ y el resto serán conjugadas

$K(\sqrt[3]{3}\,\xi^2)$, $K(\sqrt[3]{3}\,\xi^4)$

G	α	α^2
τ_0	α	α^2
τ_1	$\alpha\xi$	$\alpha^2\xi^2$
τ_2	$\alpha\xi^2$	$\alpha^2\xi^4$
τ_3	$\alpha\xi^3$	α^2
τ_4	$\alpha\xi^4$	$\alpha\xi^2$
τ_5	$\alpha\xi^5$	$\alpha\xi^4$

Ejemplo:

$$p(x) = x^4 - 2x^2 + 2 \rightsquigarrow \{\pm\sqrt{1\pm i}\}$$

$$\alpha = \sqrt{1+i}$$
$$\beta = \sqrt{1-i}$$
$$\alpha\beta = \sqrt{2}$$

$$\begin{tikzcd}
\mathbb{Q}(\alpha,\sqrt{2}) = E \\
\mathbb{Q}(\alpha) \not\ni \sqrt{2} \arrow[u, "2"] \\
\mathbb{Q} \arrow[u, "4"]
\end{tikzcd}$$

porque $p(x)$ es irred. por Eisenstein $\longleftarrow 4$

¿Cómo es D_8?

tres subext. normales de grado 2 $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2}i)$ un subext. normal de grado 4 $\mathbb{Q}(\sqrt{2}, i)$ 4 subext. de grado 4 conjugadas (dos por un lado y otros dos por otro)	$\xleftrightarrow{\text{TFTG}}$	subgr. propios de D_8 - un subgr. cíclico de orden 4 (normal) - dos 4-grupos de Klein (normales) - 5 cíclicos de orden 2 otros dos conjugados: $\mathbb{Q}(\sqrt{2}\sqrt{1+i})$, $\mathbb{Q}(\sqrt{2}\sqrt{1-i})$ 2 conjugados: $\mathbb{Q}(\sqrt{1+i})$, $\mathbb{Q}(\sqrt{1-i})$ 1 normal

$$\begin{tikzcd}
 & & \mathbb{Q}(\alpha,\sqrt{2}) & & \\
\mathbb{Q}(\sqrt{1+i}) = \mathbb{Q}(\alpha) \arrow[urr] & & \mathbb{Q}(\sqrt{2}, i) \arrow[u] & & \\
 & \mathbb{Q}(\sqrt{2}) \arrow[ur] & \mathbb{Q}(\sqrt{2}i) \arrow[u, "2"] & \mathbb{Q}(i) \arrow[ul] & \mathbb{Q}(\sqrt{1-i}) = \mathbb{Q}(\beta) \arrow[uull] \\
 & & \mathbb{Q} \arrow[uull, "4"] \arrow[ul, "2"] \arrow[u, "2"] \arrow[ur, "2"] \arrow[urr, "4"] & &
\end{tikzcd}$$

ERROR 4: No usar las hipótesis

ERROR 5: No estudiar cuerpos finitos!

Ejemplo:

$\mathbb{F}_{p^n}/\mathbb{F}_p$ ext. que siempre es Galois

$\mathbb{F}_{p^n} = \mathbb{F}_p(x^{p^n}-x) = \{$ conjunto de soluciones de $x^{p^n}-x \}$

$\Rightarrow Gal(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle Frob \rangle$ $\qquad Frob(\alpha) = \alpha^p$

Entonces $|\langle Frob \rangle| = n$

Otro ejemplo: $p \in \mathbb{F}_5[x]$ irred. de grado 12

¿$E = \mathbb{F}_5(p)$?

$\mathbb{F}_5[x] / \langle p(x) \rangle = K \leftarrow$ tiene al menos una raíz de $p(x)$ por Kronecker

alg. de la div.

$\Rightarrow |K| = 5^{12} \Rightarrow K \cong \mathbb{F}_{5^{12}}$ $\leftarrow$ Tma. clasificación de cuerpos finitos

Además sabemos que $\mathbb{F}_{5^{12}}$ es normal porque es el cuerpo de descomposición de $x^{5^{12}} - x$

$\Rightarrow$ como ~~p(x)~~ $\mathbb{F}_{5^{12}} \cong K$ tiene una raíz de $p(x)$ y es normal $\Rightarrow p$ se escinde en $K \cong \mathbb{F}_{5^{12}}$.