Teorema de Galois:

Def. E/k es de Galois si es normal y separable

Prop. E/k de Galois finita.

i) $\mathrm{Hom}_k(E/k, \bar{k}/k) = \mathrm{Gal}(E/k)$

ii) $|\mathrm{Gal}(E/k)| = [E:k]$

iii) $\exists\, \theta \in E$ tq $E = k(\theta)$

iv) E es cdd de un $f \in k[x]$

Obs. $f \in K[x]$ separable $\Rightarrow \mathrm{Gal}(f/k) \leq S_n$, con $n = \mathrm{gr}(f)$ y $\mathrm{Gal}(f/k) = \mathrm{Gal}(E/k)$, con E cdd de f

Correspondencia de Galois: Dada E/k de Galois, finita.

$$\left\{ \text{Subext de } E/k \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{Subgrupos de} \\ \mathrm{Gal}(E/k) \end{array} \right\}$$

$$F/k \longmapsto \mathrm{Gal}(E/F)$$

$$\left\{ x \in E : \sigma(x) = x,\ \forall \sigma \in H \right\} =: E^H \longleftarrow H$$

y además: F/k es normal $\Longleftrightarrow \mathrm{Gal}(E/F) \triangleleft \mathrm{Gal}(E/k)$

y en tal caso: $Gal(F/K) \simeq \dfrac{Gal(E/K)}{Gal(E/F)}$

<u>Grupos de Galois</u>: $f \in K[x]$ sep, notamos $E = cdd$

1) $gr(f) = 2$; irreducible.

$$Gal(E/K) \simeq \mathbb{Z}/2\mathbb{Z}$$

2) $gr(f) = 3$, irreducible ; car$(k) \neq 2$

$f = (x-\alpha)(x-\beta)(x-\gamma)$; $\alpha, \beta, \gamma \in E$

$E = k(\alpha, \beta, \gamma)$

$[E:k] = \begin{cases} 3, & \text{si } \sqrt{\Delta} \in K \quad (1) \\ 6, & \text{si } \sqrt{\Delta} \notin K \quad (2) \end{cases}$

1 ó 2

$K(\alpha)$

3

K

(1) $Gal(E/K) \simeq \mathbb{Z}/3\mathbb{Z}$

(2) $Gal(E/K) \simeq S_3 \ (\simeq D_3)$

Pues: (a) $k(\alpha)/K$ es una subext <u>no</u> normal, entonces $\exists \ H \leq Gal(E/K)$ <u>no</u> normal. Como todos los subgrupos de $\mathbb{Z}/6\mathbb{Z}$ son normales, $Gal(E/K) \not\simeq \mathbb{Z}/6\mathbb{Z}$.

(b) O bien: $Gal(E/K) \leq S_3$, y tienen el mismo cardinal (6)

3) $f = x^n - 1$, $K = \mathbb{Q}$

$E = \mathbb{Q}(\xi_n)$ y $Gal(E/\mathbb{Q}) \simeq (\mathbb{Z}/_n\mathbb{Z})^\times$

Pues: $Gal(E/\mathbb{Q}) = \{\sigma_j \, , (j:n) = 1\}$,

con $\sigma_j : \xi_n \longmapsto \xi_n^j$

Ej. $f = x^8 - 1$, $Gal(E/\mathbb{Q}) \simeq (\mathbb{Z}/_8\mathbb{Z})^\times$

$$\simeq \mathbb{Z}/_2\mathbb{Z} \oplus \mathbb{Z}/_2\mathbb{Z}$$

¿Cuáles son las subextensiones de $E/\mathbb{Q}$?

$$\begin{tikzcd} E = \mathbb{Q}(\xi_8) \arrow[d, dash, "4"'] \\ \mathbb{Q} \end{tikzcd}$$

Como $\mathbb{Z}/_2\mathbb{Z} \oplus \mathbb{Z}/_2\mathbb{Z}$ tiene 3 subgrupos propios, hay 3 subext (propias)

Tenemos $\xi_8 = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i$

$\xi_8^{-1} = \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2} i$

$$\Rightarrow \begin{cases} \xi_8 + \xi_8^{-1} = \sqrt{2} \\ \xi_8^2 = i \\ \xi_8 - \xi_8^{-1} = \sqrt{2} i \end{cases}$$

$$\begin{tikzcd} & E \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\ \mathbb{Q}(\sqrt{2}) \arrow[dr, dash, "2"'] & \mathbb{Q}(i) \arrow[d, dash, "2"] & \mathbb{Q}(\sqrt{2} i) \arrow[dl, dash, "2"] \\ & \mathbb{Q} & \end{tikzcd}$$

4) $f = x^4 - 12$, $k = \mathbb{Q}$, $k = \mathbb{Q}(i)$

$$f = (x - \sqrt[4]{12})(x - \sqrt[4]{12}\, i)(x + \sqrt[4]{12})(x + \sqrt[4]{12}\, i)$$

$$\Rightarrow \quad E = \mathbb{Q}(\sqrt[4]{12}, \sqrt[4]{12}\, i) = \mathbb{Q}(\sqrt[4]{12}, i)$$

$$\begin{tikzcd}
 & E \arrow[dl, dash, "\cancel{4} \text{ ó } 2"'] \arrow[dr, dash, "4"] & \\
\mathbb{Q}(\sqrt[4]{12}) \arrow[dr, dash, "4"'] & & \mathbb{Q}(i) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

(min: $x^4 - 12$) $\quad [E : \mathbb{Q}] = 8$

Grupos de orden 8 :

<u>Abelianos</u>: $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

<u>No abelianos</u>: D_4, $\mathcal{H}$

Pero $\mathbb{Q}(\sqrt[4]{12})/\mathbb{Q}$ es <u>NO</u> normal

$\Longrightarrow \operatorname{Gal}(E/\mathbb{Q}) \simeq D_4$, pues los otros grupos no tienen subgrupos no normales

<u>$k = \mathbb{Q}(i)$</u> : $|\operatorname{Gal}(E/\mathbb{Q}(i))| = 4$ $\left(\simeq \mathbb{Z}/4\mathbb{Z} \text{ ó } \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \right)$

y precisamente $\operatorname{Gal}(E/\mathbb{Q}(i)) = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}$,

Con
$$\begin{cases} \sigma_0 : \sqrt[4]{12} \longmapsto \sqrt[4]{12} & : \text{orden } 1 \\ \sigma_1 : \sqrt[4]{12} \longmapsto \sqrt[4]{12}\, i & : \text{orden } 4 \\ \sigma_2 : \sqrt[4]{12} \longmapsto -\sqrt[4]{12} & : \text{orden } 2 \\ \sigma_3 : \sqrt[4]{12} \longmapsto -\sqrt[4]{12}\, i & : \text{orden } 4 \end{cases}$$

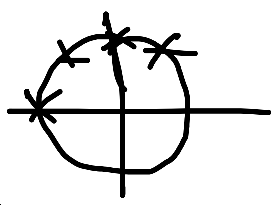
$$\sigma_1 : \sqrt[4]{12} \longmapsto \sqrt[4]{12}\, i \longmapsto \sqrt[4]{12}\, i\, i = -\sqrt[4]{12} \longmapsto -\sqrt[4]{12}\, i \longmapsto \sqrt[4]{12}$$

Luego: $\mathrm{Gal}(E/\mathbb{Q}(i)) \simeq \mathbb{Z}/4\mathbb{Z}$

5) $f = x^4 + 2$, $K = \mathbb{Q}$

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

Con $\sqrt[4]{-2} = \sqrt[4]{2} \cdot \xi_8$



$$\begin{tikzcd}[column sep=small] & \mathbb{Q}(\sqrt[4]{2}\,\xi_8, i) \arrow[dl, dash, "1 \text{ ó } 2"'] \arrow[dr, dash] & \\ \mathbb{Q}(\sqrt[4]{2}\,\xi_8) \arrow[dr, dash, "4"'] & & \mathbb{Q}(i) \arrow[dl, dash, "2"] \\ & \mathbb{Q} & \end{tikzcd}$$

$$\xi_8 = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i$$

Pero, ¿afirmo que: $\underbrace{\mathbb{Q}(\sqrt[4]{2}\,\xi_8, i)}_{E_1} = \underbrace{\mathbb{Q}(\sqrt[4]{2}, i)}_{E_2}$

Pues $\subseteq)$ $\xi_8 = \dfrac{(\sqrt[4]{2})^2}{2} + \dfrac{(\sqrt[4]{2})^2}{2} i \in E_2$

$\supseteq)$ $(\sqrt[4]{2})^2 \left(\dfrac{1}{2} + \dfrac{i}{2}\right) = \xi_8 \Longrightarrow \sqrt[4]{2} = \dfrac{2\overbrace{\xi_8^2}^{=i}}{(1+i)\sqrt[4]{2}\,\xi_8} \in E_1$

Entonces

$$\begin{tikzcd}[column sep=small]
 & \mathbb{Q}(\sqrt[4]{2}, i) \arrow[dl, dash, "2"'] \arrow[dr, dash, "4"] & \\
\mathbb{Q}(\sqrt[4]{2}) \arrow[dr, dash, "4"'] & & \mathbb{Q}(i) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

y $\mathrm{Gal}(E/\mathbb{Q}) \simeq D_4$ (idem antes)

Por ejemplo: $\mathrm{Gal}(E/\mathbb{Q}) \longrightarrow D_4$

$$\sigma \longmapsto \rho$$
$$\tau \longmapsto s \quad ,$$

con $\sigma : \sqrt[4]{2} \longmapsto -\sqrt[4]{2}\, i$

$\qquad\quad i \longmapsto i$

$$s\rho = \rho^3 s$$

$\tau : \sqrt[4]{2} \longmapsto \sqrt[4]{2}$

$\qquad i \longmapsto -i \quad ,$

pues resulta: $\tau\sigma = \sigma^3 \tau$ y uno puede ver que