Obs. Sea $\begin{array}{c} E = k(\theta) \\ | \\ k \end{array}$ de Galois y sea $H \leq Gal(E/k)$

Tenemos $\begin{array}{c} E = k(\theta) \\ | \\ E^H \\ | \\ k \end{array}$ ¿Cómo caracterizar E^H?

$$E^H = \{ x \in E \quad \sigma(x) = x, \forall \sigma \in H \}$$

Observemos que: $m_{\theta, E^H} = \prod_{\sigma \in H} (x - \sigma(\theta))$

Pues. $Gal(E/E^H) = H$ y tengo

$\begin{array}{c} E^H(\theta) \\ | \\ E^H \end{array}$, con lo cual: $m_{\theta, E^H} = \prod_{\sigma : E^H(\theta) \xrightarrow[E^H]{} \overline{E^H}} (x - \sigma(\theta))$

Supongamos $m_{\theta, E^H} = x^n + a_{n-1} x^{n-1} + \cdots + a_0$,

$a_i \in E^H$ Consideremos:

$$\begin{tikzcd}[row sep=small]
E = k(\theta) \arrow[d, dash, "n"'] \arrow[dd, dash, bend left, "n"] \\
E^H \arrow[d, dash] \\
F = k(a_0, a_1, \dots, a_{n-1}) \arrow[d, dash] \\
k
\end{tikzcd}$$

Pues: $m_{\theta, F} = m_{\theta, E^H}$, ya que es irred en E^H

$\therefore E^H = k(a_0, \dots, a_{n-1}) = k(\text{coeff's de } m_{\theta, E^H})$

Ej $E = \mathbb{Q}(\sqrt[4]{2}, i)$ (E = cdd de x^4+2)

$$\mathrm{Gal}(E/\mathbb{Q}) \simeq D_4, \text{ con } \begin{cases} \rho: \sqrt[4]{2} \mapsto -\sqrt[4]{2}\, i \\ \quad\; i \mapsto i \\ \\ s: \sqrt[4]{2} \mapsto \sqrt[4]{2} \\ \quad\; i \mapsto -i \end{cases}$$

Sea $H = \{e, s, \rho^2 s, \rho^2\} \leq D_4$

¿E^H? Tenemos: $\begin{cases} \rho^2 s: \sqrt[4]{2} \mapsto -\sqrt[4]{2} \\ \qquad i \mapsto -i \\ \\ \rho^2: \sqrt[4]{2} \mapsto -\sqrt[4]{2} \\ \qquad i \mapsto i \end{cases}$

$$\begin{array}{c} E^H \\ 2\,| \\ \mathbb{Q} \end{array}$$

Tenemos: $E = \mathbb{Q}(\underbrace{\sqrt[4]{2} + i}_{\theta})$ (Verificar)

$$\Rightarrow m_{\theta, E^H} = \prod_{\sigma \in H} (x - \sigma(\theta))$$

$$= (x-\theta)(x - s(\theta))(x - \rho^2 s(\theta))(x - \rho^2(\theta))$$

$$= (x - (\sqrt[4]{2} + i))(x - (\sqrt[4]{2} - i))(x - (-\sqrt[4]{2} - i))(x - (-\sqrt[4]{2} + i))$$

$$\dots = x^4 + 2x^2 + 3 + 2\sqrt{2}$$

Luego $E^H = \mathbb{Q}(\sqrt{2})$.

— x —

Obs: Sea $f = (x-\alpha_1)\dots(x-\alpha_n) \in K[x]$, con f separable, $\alpha_i \in \overline{K}$. Tenemos

$$\Delta(f) := \prod_{i<j} (\alpha_i - \alpha_j)^2 \in K$$

$$\Rightarrow \sqrt{\Delta(f)} = \prod_{i<j} (\alpha_i - \alpha_j).$$

Sea $\sigma \in S_n$, entonces $\sigma(\sqrt{\Delta(f)}) = \mathrm{sg}(\sigma)\sqrt{\Delta(f)}$

Entonces si $\sigma(\sqrt{\Delta(f)}) = \sqrt{\Delta(f)} \iff \sigma \in A_n$

si $\mathrm{car}(K) \neq 2$

Osea: Si $E =$ cdd de f sobre K.

$$\mathrm{Gal}(E/K) \subseteq A_n \iff \sqrt{\Delta(f)} \in K.$$

Consecuencia: Si $f \in k[x]$, irred, $\mathrm{car}(k) \neq 2$, $E =$ cdd de f sobre K, $\mathrm{gr}(f) = 3$:

$$\mathrm{Gal}(E/K) \simeq \begin{cases} S_3 & \text{si } \sqrt{\Delta(f)} \notin K \\ A_3 & \text{si } \sqrt{\Delta(f)} \in K \end{cases}$$

En el caso $n=3$, que ya sabíamos

<u>Prop.</u> $\mathbb{Q}(\xi_p)$, $f = x^p - 1$, $p \neq 2$,

$$\begin{array}{c} \mathbb{Q}(\xi_p) \\ \big| \, p-1 \\ \mathbb{Q} \end{array} \qquad \mathrm{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q}) \simeq \mathbb{Z}/(p-1)\mathbb{Z}$$

Entonces, la única subext cuadrática es:

$$\begin{cases} \mathbb{Q}(\sqrt{p}) & \text{si } p \equiv 1 \ (4) \\ \mathbb{Q}(\sqrt{-p}) & \text{si } p \equiv 3 \ (4) \end{cases}$$

<u>Dem</u> $$\Delta(f) = \prod_{\substack{i<j \\ i,j \in \{1,\dots,p\}}} (\xi_p^i - \xi_p^j)^2 = \left[\prod_{i<j} (\xi_p^i - \xi_p^j) \right]^2$$

$$= \left(V(\xi_p, \dots, \xi_p^p) \right)^2 = \quad \xi = \xi_p$$

$$\det\left(\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ \zeta & \zeta^2 & \zeta^3 & \cdots & \zeta^p \\ \zeta^2 & (\zeta^2)^2 & (\zeta^3)^2 & & (\zeta^p)^2 \\ \vdots & & & & \\ \zeta^{p-1} & (\zeta^2)^{p-1} & (\zeta^3)^{p-1} & \cdots & (\zeta^p)^{p-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & \zeta & \zeta^2 & \cdot & \zeta^{p-1} \\ 1 & \zeta^2 & (\zeta^2)^2 & & (\zeta^2)^{p-1} \\ & & & & \\ 1 & \zeta^p & (\zeta^p)^2 & \cdots & (\zeta^p)^{p-1} \end{bmatrix}\right)$$

$$= \det\begin{bmatrix} p & 0 & 0 & \cdots & 0 \\ 0 & 0 & & 0 & p \\ 0 & 0 & \cdots & p & 0 \\ & & \iddots & & \\ 0 & p & \cdots & & 0 \end{bmatrix} = p\, p^{p-1} \cdot (-1)^{\frac{p-1}{2}}$$

$$= p^p \cdot (-1)^{\frac{p-1}{2}}$$

$$\Rightarrow \sqrt{\Delta(f)} = p^{\frac{p-1}{2}} \sqrt{\pm p}$$

$$= \begin{cases} p^{\frac{p-1}{2}}\sqrt{p} & \text{si } p \equiv 1\ (4) \\ p^{\frac{p-1}{2}}\sqrt{-p} & \text{si } p \equiv 3\ (4) \end{cases}$$

O sea, tengo

$$\begin{array}{c} \mathbb{Q}(\zeta_p) \\ | \\ \mathbb{Q}(\sqrt{\Delta(f)}) \quad \left(= \mathbb{Q}(\sqrt{p}) \text{ ó } \mathbb{Q}(\sqrt{-p}) \right) \\ 2\,| \\ \mathbb{Q} \end{array}$$

■

Ej: $f = (x^p - 1)\cdot\underbrace{(x^4+2x^2-4)}_{g}$; $p \neq 5$ sea

E = cdd de f sobre $\mathbb{Q}$. Calcular $Gal(E/\mathbb{Q})$

Resulta: $g = (x \pm \sqrt{\sqrt{5}-1})(x \pm \sqrt{\sqrt{5}-1}\, i)$

$$\Rightarrow E = \mathbb{Q}(\xi_p, \sqrt{\sqrt{5}-1}, \sqrt{\sqrt{5}-1}\, i)$$

$$= \mathbb{Q}(\xi_p, \sqrt{\sqrt{5}-1}, i)$$

$$\begin{tikzcd}
 & E \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\xi_p) \arrow[dr, dash, "p-1"'] & & \mathbb{Q}(\sqrt{\sqrt{5}-1}, i) \arrow[dl, dash] \arrow[d, dash, "2"] \\
 & \mathbb{Q} \arrow[r, dash, "4\ (*)"'] & \mathbb{Q}(\sqrt{\sqrt{5}-1})
\end{tikzcd}$$

$(*)$ $\mathbb{Q}(\sqrt{\sqrt{5}-1})$

$2 \,|\, \longrightarrow$ Bvq $\sqrt{\sqrt{5}-1} \notin \mathbb{Q}(\sqrt{5})$

$\mathbb{Q}(\sqrt{5})$

$2 \,|$

$\mathbb{Q}$

Ahora:

$$\begin{tikzcd}[column sep=small]
F = \mathbb{Q}(\zeta_p) \arrow[dr, dash] \arrow[ddr, dash, bend right, "p-1"'] & & \mathbb{Q}(\sqrt{\sqrt{5}-1}, i) = L \arrow[dl, dash] \arrow[ddl, dash, bend left, "8"] \\
& F \cap L \arrow[d, dash, "{1,2,4,8}"] & \\
& \mathbb{Q} &
\end{tikzcd}$$

Si es 8: $F \cap L = L \Rightarrow L \subseteq F$

$\Rightarrow \sqrt{5} \in \mathbb{Q}(\zeta_p)$

Pero: $\mathbb{Q}(\sqrt{\pm p}) \subseteq \mathbb{Q}(\zeta_p)$ es la única subext cuadrática $(p \neq 5)$ Abs

Si es 2: $F \cap L \subseteq \mathbb{Q}(\zeta_p)$ es una subext cuadrática, entonces: $F \cap L = \mathbb{Q}(\sqrt{\pm p})$

$\Rightarrow \sqrt{\pm p} \in L$

$\Rightarrow \mathbb{Q}(\sqrt{\pm p}, \sqrt{5}, i) \subseteq L$

$$\begin{tikzcd}
\mathbb{Q}(\sqrt{\pm p}, \sqrt{5}, i) \arrow[d, dash, "8"'] \\
\mathbb{Q}
\end{tikzcd}$$

$\Rightarrow \mathbb{Q}(\sqrt{\pm p}, \sqrt{5}, i) = L$

(lo vemos al final)

Si es 4. $\begin{array}{c} F\cap L \\ 4 \vert \\ \mathbb{Q} \end{array}$, existe seguro una subext. cuadrática y sigo como antes

(Notar pero esto también aplica al caso 8)

Luego $F\cap L = \mathbb{Q}$

$\therefore \ Gal(E/\mathbb{Q}) \simeq Gal(F/\mathbb{Q}) \times Gal(L/\mathbb{Q})$

$\simeq \mathbb{Z}/(p-1)\mathbb{Z} \times D_4$

$D_4 \rightsquigarrow$ escribirlo

$\dagger$: Pues $\begin{cases} Gal(L/\mathbb{Q}) \simeq D_4 \\ Gal(\mathbb{Q}(\sqrt{\pm p}, \sqrt{5}, i)) \end{cases}$

$\simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$