

Obs. Sea $E = k(\theta)$ de Galois y sea $H \leq \text{Gal}(E/k)$

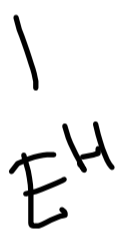
Tenemos $E = k(\theta)$ ¿cómo caracterizar E^H ?



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

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

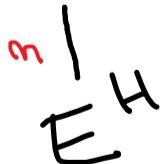
Pues $\text{Gal}(E/E^H) = H$ y luego

$$E^H(\theta)$$


, con lo cual $m_{\theta, E^H} = \prod_{\sigma: E^H(\theta) \rightarrow E^H} (x - \sigma(\theta))$

Supongamos $m_{\theta, E^H} = x^m + Q_{m-1}x^{m-1} + \dots + Q_0$,

$Q_i \in E^H$ consideremos.

$$E = k(\theta)$$


$$F = k(Q_0, Q_1, \dots, Q_{m-1})$$


$\therefore E^H = k(Q_0, \dots, Q_{m-1}) = k(\text{coeff's de } m_{\theta, E^H})$

Pues: $m_{\theta, F} = m_{\theta, E^H}$

ya que θ es root en E^H

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

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

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

$\subset E^H$?

$$\text{Trasposiciones: } \begin{cases} \rho^2 s \cdot \sqrt[4]{2} \mapsto -\sqrt[4]{2} \\ i \mapsto -i \\ \\ \rho^2 \cdot \sqrt[4]{2} \mapsto -\sqrt[4]{2} \\ i \mapsto i \end{cases}$$

E^H

2 |

\mathbb{Q}

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

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

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

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

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

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

— x —

Obs: Sea $f = (x - \alpha_1) \dots (x - \alpha_n) \in K[x]$, con f separable, $\alpha_i \in \bar{K}$. 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 $\sigma \in S_m$, entonces $\sigma(\sqrt{\Delta(f)}) = \text{sgn}(\sigma) \sqrt{\Delta(f)}$

Entonces $\sigma(\sqrt{\Delta(f)}) = \sqrt{\Delta(f)} \Leftrightarrow \sigma \in A_m$
 si $\text{car}(K) \neq 2$

Def: Si $E = \text{cdol de } f \text{ sobre } K$.

$$\text{Gal}(E/K) \subseteq A_m \Leftrightarrow \sqrt{\Delta(f)} \in K$$

Proposición: Si $f \in K[x]$, irred, $\text{car}(K) \neq 2$,
 $E = \text{cdol de } f \text{ sobre } K$, $g_c(f) = 3$:

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

En el caso $n=3$, fue ya solucionado

Prop. $\mathbb{Q}(\zeta_p)$, $f = x^p - 1$, $p \neq 2$,
 \downarrow
 \mathbb{Q} $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \simeq \mathbb{Z}/(p-1)\mathbb{Z}$

Entonces; la única subext cuadrática es.

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

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

$$= \left(\sqrt{(\zeta_p, \dots, \zeta_p^p)} \right)^2 = \sqrt{3} = \sqrt{3p}$$

$$\det \begin{bmatrix} 1 & \omega & \omega^2 & \dots & \omega^{p-1} \\ \omega & \omega^2 & \omega^3 & \dots & \omega^p \\ \omega^2 & (\omega^2)^2 & (\omega^3)^2 & \dots & (\omega^p)^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \omega^{p-1} & (\omega^2)^{p-1} & (\omega^3)^{p-1} & \dots & (\omega^p)^{p-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & \omega & \omega^2 & \dots & \omega^{p-1} \\ 1 & \omega^2 & (\omega^2)^2 & \dots & (\omega^2)^{p-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^p & (\omega^p)^2 & \dots & (\omega^p)^{p-1} \end{bmatrix}$$

$$= \det \begin{bmatrix} p & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 0 \end{bmatrix} = p \cdot p^{p-1} \cdot (-1)^{\frac{p-1}{2}}$$

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

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

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

O sea, tengo

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

$$\mathbb{Q}(\sqrt{\Delta(\mathbb{F})})$$

$$= \mathbb{Q}(\sqrt{p}) \text{ ó } \mathbb{Q}(\sqrt{-p})$$

2 |

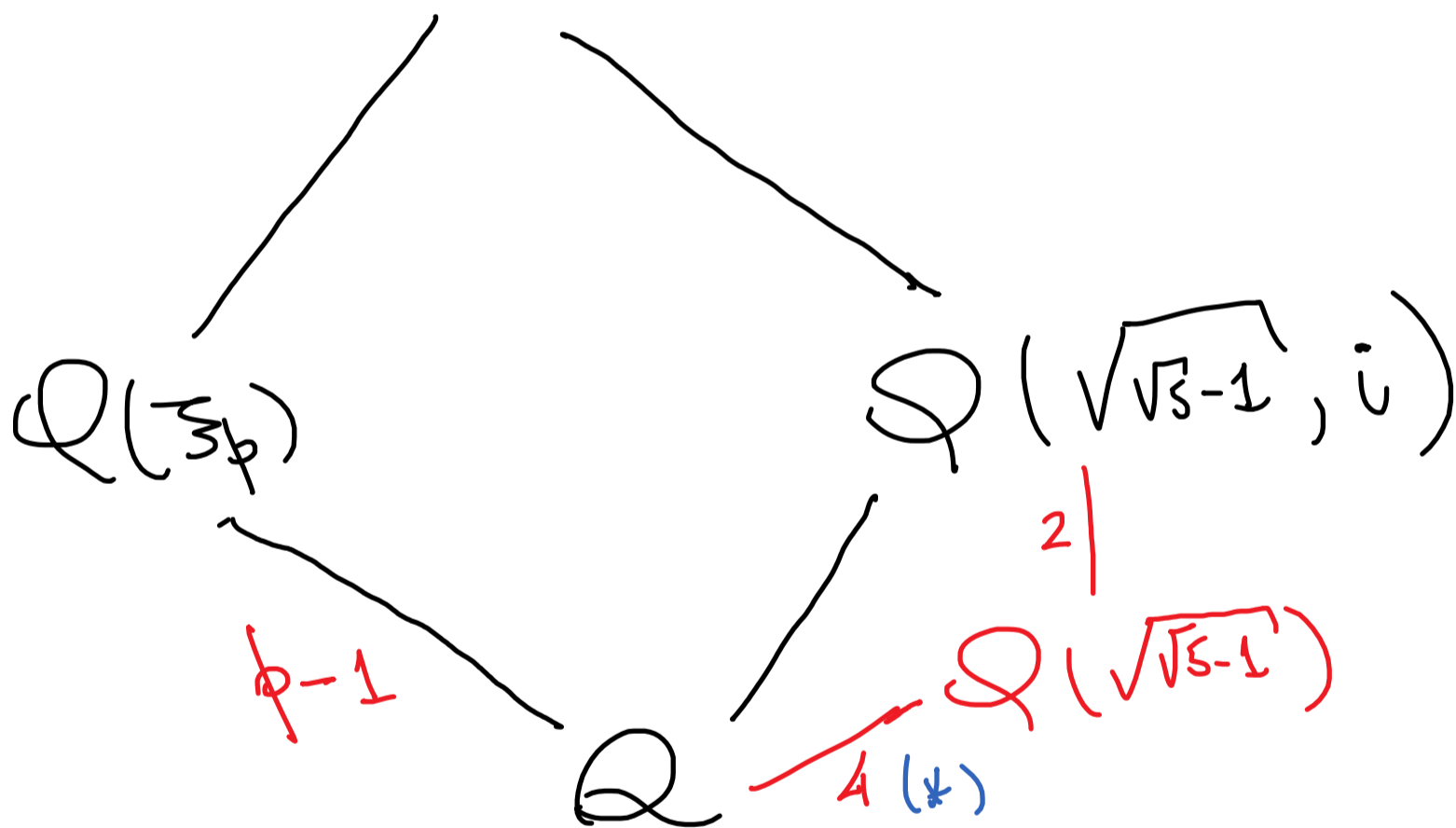
$$\mathbb{Q}$$



E : $f = (x^p - 1) \cdot (x^4 + 2x^2 - 4)$; sea $p \neq 5$
 $E = \text{cdd de } f \text{ sobre } \mathbb{Q}$. Poloson $(\text{sol}(E/\mathbb{Q}))$

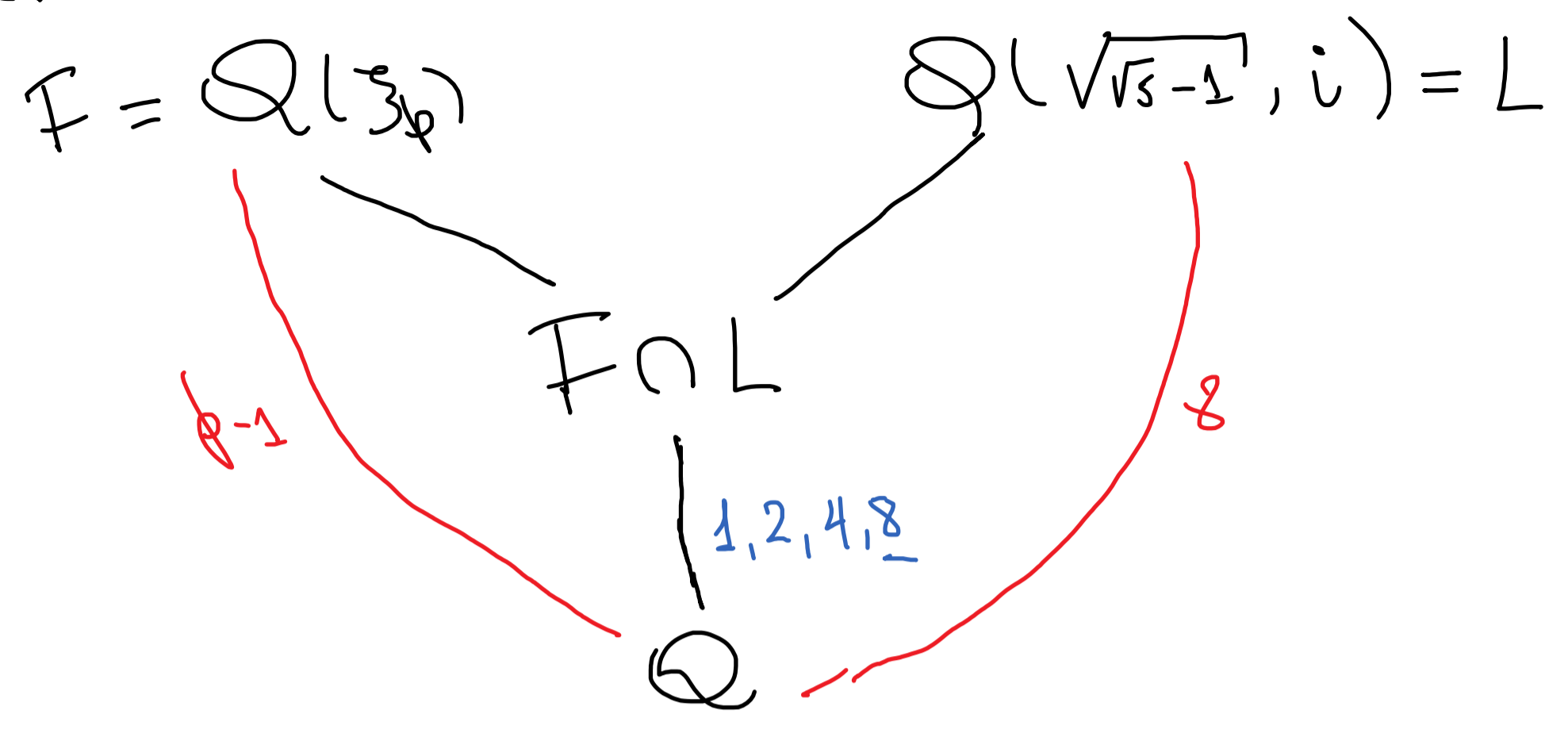
Resulta: $g = (x \pm \sqrt{\sqrt{5}-1}) (x \pm \sqrt{\sqrt{5}-1} i)$

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



(*) $\mathbb{Q}(\sqrt{\sqrt{5}-1})$
 $2 \downarrow \rightarrow \text{Bug } \sqrt{\sqrt{5}-1} \notin \mathbb{Q}(\sqrt{5})$
 $\mathbb{Q}(\sqrt{5})$
 $2 \downarrow$
 \mathbb{Q}

Ahora:



Si es 8: $F \cap L = L \Rightarrow L \subseteq F$
 $\Rightarrow \sqrt{5} \in \mathbb{Q}(\zeta_p)$

Prop. $\mathbb{Q}(\sqrt{\pm p}) \subseteq \mathbb{Q}(\zeta_p)$ 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: $F \cap L = \mathbb{Q}(\sqrt{\pm p})$

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

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

$8 \mid \Rightarrow \mathbb{Q}(\sqrt{\pm p}, \sqrt{5}, i) = L$
 (los números al final)

Si es 4. $F \cap L$, existe segun una subext.
 $4 \mid$ cuadrática y sig como antes
 \mathbb{Q}

(Nota que esto también aplica al caso 8)

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

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

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

↕
subgrupo

t: Pues $\left\{ \begin{array}{l} \text{Gal}(L/\mathbb{Q}) \cong D_4 \\ \text{Gal}(\mathbb{Q}(\sqrt{p}, \sqrt{5}, i)) \end{array} \right.$

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