Extensiones algebraicas (en general):

Def. E/k algebraica, $\alpha \in E$.

i) $\alpha \in E$ es separable si $m_{\alpha,k}$ tiene raíces simples

ii) $\alpha \in E$ es puramente inseparable si $m_{\alpha,k}$ tiene una única raíz

Prop α es pi $\iff \exists\, n$ / $\alpha^{p^n} \in k$, si $\mathrm{car} k = p$

$\iff \mathrm{Hom}_k\{k(\alpha), \bar{k}\} = \{Id\}$

Def: $E_s := \{\alpha \in E : \alpha$ es sep. sobre $k\}$

$E_i := \{$ " p.i. " $\}$

Obs $E_s \cap E_i = k$

Ej $F_2(\sqrt[6]{t}) = E$ ¿Sep? ¿P.i?

$m_{\sqrt[6]{t},k} = x^6 - t = (x^3)^2 - t$

$= (x^3 - \sqrt{t})^2$,

que no tiene raíces simples ni una única raíz. De hecho tiene 3 raíces, que son las de $x^3 - \sqrt{t}$

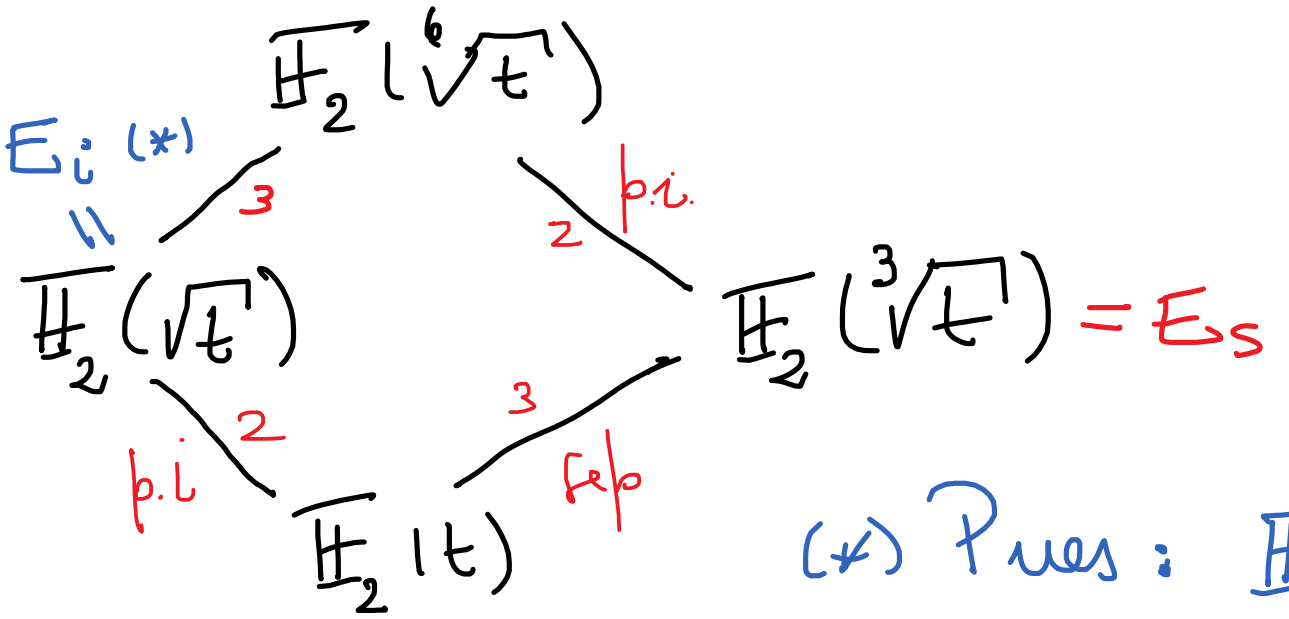
$\overline{F_2}(t) = k$

Calculemos E_s y E_i

Escribo $f = m_{\sqrt[6]{t},k} = g(x^{p^e}) = g(x^{2^e})$:

$$f = m_{\sqrt[6]{t},k} = x^6 - t = (x^2)^3 - t,$$

y llamo $g = x^3 - t$, que es sep e irred, y $f = g(x^2)$ con $e = 1$



(*) Pues: $\mathbb{F}_2(\sqrt[6]{t})$ | sep → $m_{\sqrt[6]{t},\mathbb{F}_2(\sqrt{t})} = x^3 - \sqrt{t}$

$\mathbb{F}_2(\sqrt{t})$

| p.i

$\mathbb{F}_2(t)$

Veamos que (ejercicio)

E
| sep
F
| p.i
k

$\Rightarrow$ $F = E_i$

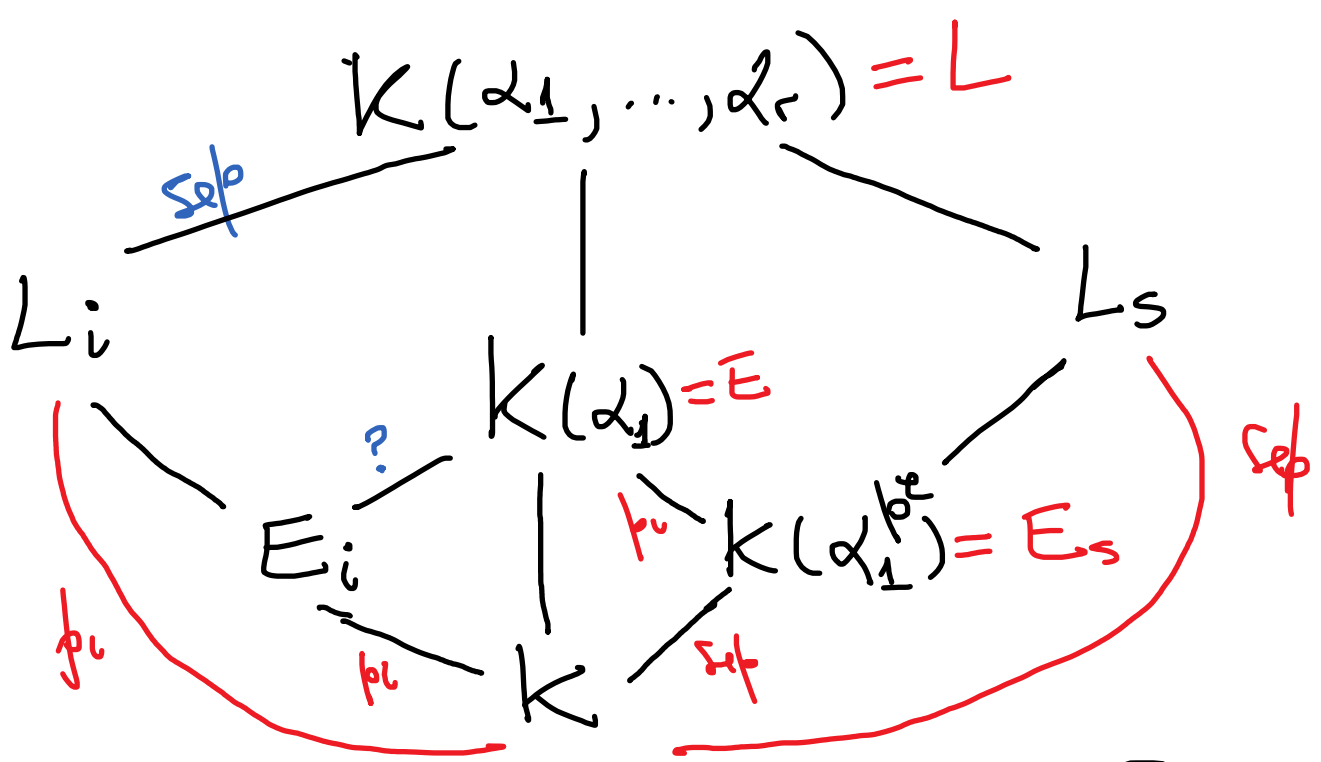
$\not\Rightarrow$ (ie E | ⇝ No siempre sep E_i | p.i k)

Prop L/K es normal si vale "$\Leftarrow$"

En general: $\operatorname{car} k = p$, $f \in k[x]$ irred, con

$f = g(x^{p^e})$, g irred y sep. Digamos

$$f = \left((x-\alpha_1)\cdot\ldots\cdot(x-\alpha_r)\right)^{p^e}$$



Llamo $h = (x-\alpha_1)\cdots(x-\alpha_r) = \sum_{j=0}^{r} a_j x^j \in L[x]$

Pero $h^{p^e} = f \in k[x]$. Osea: $a_j^{p^e} \in k$

$\Rightarrow$ a_j son $p.i$ sobre k $\Rightarrow$ $a_j \in L_i$

Tengo entonces: $k[a_0,\ldots,a_r] \subseteq L_i$

L
|
L_i
|
$k[a_0,\ldots,a_r]$

sep, pues: L es el cuad de h sobre k y h es separable

son iguales! $\Leftarrow$ sep | p.i

Otro $L_1 = K(\text{coeffs de } h)$.

Ej. $f = x^{2p} + uvx^p + v \in \overline{\mathbb{F}_p(u,v)}[x]$, $p \neq 2$.

($\overline{\mathbb{F}_p(u,v)}$ = K)

$$= \big((x-\alpha_1)(x-\alpha_2)\big)^p, \quad \alpha_1, \alpha_2 \in \overline{K}$$

($(x-\alpha_1)(x-\alpha_2)$ = h)

$$= \left(x^2 + \sqrt[p]{u}\sqrt[p]{v}\,x + \sqrt[p]{v}\right)^p$$

Otra $K(\text{coeff's de } h) = K(\sqrt[p]{u}, \sqrt[p]{v})$

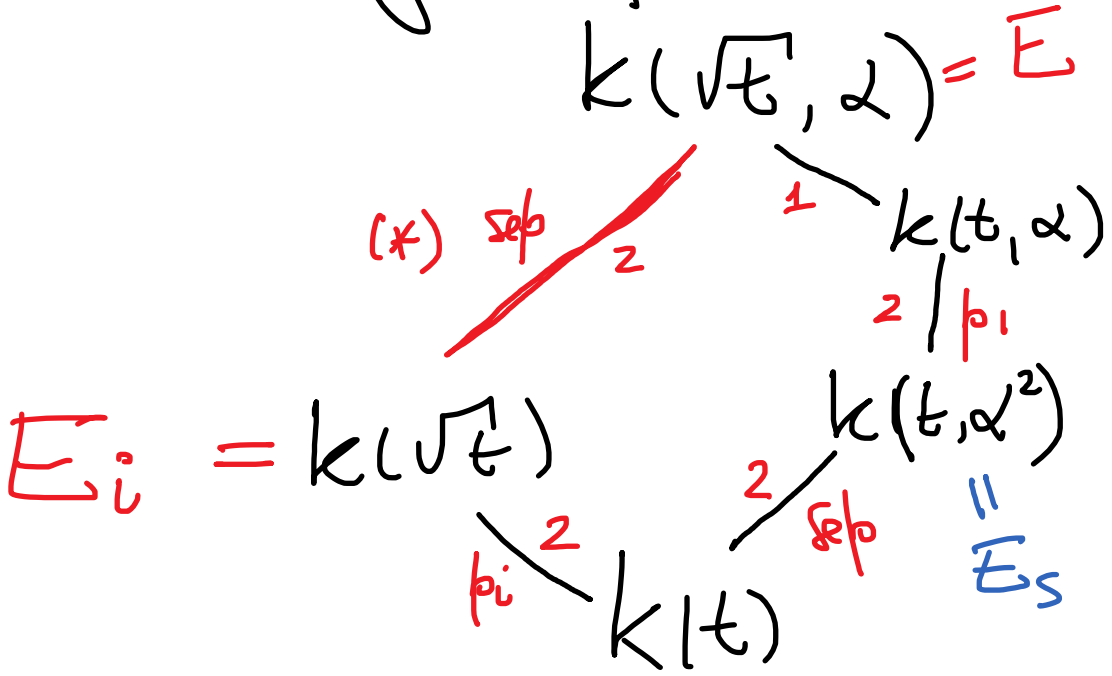
Luego: si $L = K(\alpha_1, \alpha_2)$, entonces:

$$L_i = K(\sqrt[p]{u}, \sqrt[p]{v}) = \overline{\mathbb{F}_p}(\sqrt[p]{u}, \sqrt[p]{v})$$

Ej. $f = x^4 + tx^2 + t \in k(t)[x]$, con

car $k = 2$. $E = k(\sqrt{t}, \alpha)$, con $\alpha \in \overline{k}$,

raíz de f Hallar E_s y E_i



(*) Pues

$f = \left(x^2 + \sqrt{t}\,x + \sqrt{t}\right)^2$, y

$x^2 + \sqrt{t}\,x + \sqrt{t} \in k(\sqrt{t})[x]$

es irreducible (Eisenstein)

y separable.

Obs. Si $\operatorname{car} k = p$, $k^{p^{-\infty}} = \{x \in \overline{k} \;\; \sigma(x) = x, \; \forall \sigma \in \operatorname{Gal}(\overline{k}/k)\}$

Vimos que: $k^{p^{-\infty}} \supseteq \{x \in \overline{k} \;\; \exists n \,/\, x^{p^n} \in k\}$

Ej. "$\subseteq$"

Ej. a) $\alpha \in \overline{k}$, sep sobre k, $\beta \in \overline{k}$, p.i sobre k. Entonces: $k(\alpha,\beta) = k(\alpha+\beta)$

Dem.

$k(\alpha,\beta) = k(\alpha+\beta)(\alpha)$ $\quad = k(\alpha\beta)$ (si $\alpha\beta \neq 0$)

$= k(\alpha+\beta)(\beta)$

$k(\alpha+\beta)$ sep

k pi

$\Rightarrow$ son iguales!

k

b) $k \subseteq L \subseteq F$ //// F/L normal, L/k p.i. Entonces: F/k normal

F / L / k

Sea $\sigma : F \xrightarrow[k]{} \overline{k}$. Entonces: $\sigma|_L : L \xrightarrow[k]{} \overline{k}$ es la identidad, pues $\operatorname{Hom}_k\{L, \overline{k}\} = \{Id\}$

Luego: $\sigma \in \operatorname{Hom}_L(F, \overline{L}) = \operatorname{Aut}_L(F)$

$\Rightarrow \sigma(F) \subseteq F$ ✓

c) $K \subseteq L \subseteq F$, L/K f.c, $\alpha \in F$ sep sobre K. Entonces $m_{\alpha,L} = m_{\alpha,K}$

F
$|$
L
$|$

Sabemos que $m_{\alpha,L} \mid \underbrace{m_{\alpha,K}}_{\text{raíces simples}}$

$\Rightarrow m_{\alpha,L}$ tiene raíces simples. Sea e tq $(m_{\alpha,L})^{p^e} \in K[x]$ Digamos.

$m_{\alpha,K} = m_{\alpha,L} \cdot h$ en $L[x]$

$\Rightarrow \underbrace{(m_{\alpha,K})^{p^{\tilde{e}}}}_{\in K[x]} = \underbrace{(m_{\alpha,L})^{p^{\tilde{e}}}}_{\in K[x]} \cdot \underbrace{h^{p^{\tilde{e}}}}_{\in K[x]}$ en $K[x]$,

para algún $\tilde{e}$

$\Rightarrow m_{\alpha,K} \mid (m_{\alpha,L})^{p^{\tilde{e}}}$ ó $m_{\alpha,K} \mid h^{p^{\tilde{e}}}$

$m_{\alpha,K}$ es irred. Pero considerando $(m_{\alpha,K} : (m_{\alpha,L})^{p^{\tilde{e}}})$,

$m_{\alpha,K} \mid (m_{\alpha,L})^{p^{\tilde{e}}}$, entonces las raíces de $m_{\alpha,K}$ son raíces de $m_{\alpha,L}$; y listo ∎

d) $K \subseteq L \subseteq F$, finitas, F/L sep. Entonces.

$F = L F_s$ y $[F : L] = [F_s : K]$