Repaso: K cuerpo, $p(x) \in K[x]$ (mónico), existe una (única) extensión L/K finita t.q. $p(x)$ tiene todas sus raíces en L. $\longleftrightarrow$ $p(x) = (x-\alpha_1)\cdots(x-\alpha_n)$
$L = K[\alpha_1, \dots, \alpha_n]$

S. F/K extensión donde $p(x)$ tiene todas sus raíces,

$$\{K\text{-Morfismos de } L \text{ en } F\} = \mathrm{Hom}_K(L, F)$$

$\uparrow$ $\sigma(\ell) = \ell$

$$[L:K] \leq \mathrm{Hom}_K(L, F)$$

y vale igualdad ($\Rightarrow$) los factores irreducibles de $p(x)$ tienen todas sus raíces distintas (o sea $p(x)$ separable)

Ejercicio: L/K finita, $L = K[\alpha_1, \dots, \alpha_n]$ ($\{\alpha_1, \dots, \alpha_n\}$ base de L)
$m_{\alpha_1}(x), \dots, m_{\alpha_n}(x)$, F donde $m_{\alpha_i}(x)$ tiene todas sus raíces, $\forall\, 1 \leq i \leq n$,

$[L:K] \leq \mathrm{Hom}_K(L, F)$ y vale $=$ ($\Rightarrow$)
$m_{\alpha_i}(x)$ tiene todas las raíces distintas $\forall\, 1 \leq i \leq n$.

Def: Si L/K finita, $\alpha \in L$, el **minimal** de α, es el polinomio mónico de grado más chico en $K[x]$ que tiene a α como raíz.

Ejercicio: Probar que siempre existe y es única. Más aún, si $p(x) \in K[x]$ t.q. $p(\alpha) = 0 \Rightarrow m_\alpha(x) \mid p(x)$.

Un polinomio $p(x)$ es **separable** si todos sus factores irreducibles no tienen raíces múltiples.

Obs: si $\mathrm{car}(K) = 0 \Rightarrow$ todo es separable.

Def: Si L/K finita, se dice separable si cumple que

$\forall \alpha \in L$, $m_\alpha(x) \in K[x]$ es separable.

Prop: Si $L = K[\alpha]/K$, L/K separable $\Leftrightarrow$ $m_\alpha(x)$ separable. (sin demo).

Si F cuerpo, H grupo de automorfismos de F ("$\exists \sigma: F \to F$ morfismo de cuerpos biyectivos")

$$F^H = \{ \alpha \in F : \sigma(\alpha) = \alpha \ \ \forall \sigma \in H \}$$

Lema: F^H es un cuerpo.

D/. $0, 1 \in F^H$ ✓

- Basta ver que la suma y el producto están bien definidos en F^H

(i) $\alpha, \beta \in F^H$, ¿$\alpha+\beta \in F^H$? $\sigma(\alpha+\beta) = \sigma(\alpha)+\sigma(\beta) = \alpha+\beta \ \ \forall \sigma \in H$

(ii) $\alpha, \beta \in F^H \Rightarrow \alpha.\beta \in F^H$ (igual)

Obs: $\alpha \in F^H$, ¿$1/\alpha \in F^H$? $\sigma(\alpha \cdot 1/\alpha) = \sigma(1) = 1$

"$\alpha.\sigma(1/\alpha) = \sigma(\alpha).\sigma(1/\alpha) \Rightarrow \sigma(1/\alpha) = 1/\alpha$" ∎

$\Rightarrow$ Inversos están. (mismo con la suma). ∎

Teo (Galois): Si L/K "buena" (finita), existe una biyección entre

$\{$subextensiones $K \subset F \subset L\}$ $\leftrightarrow$ $\{$subgrupos de $Aut_K(L)\}$

$$\begin{array}{ccc} F & \longrightarrow & Aut_F(L) \\ K \subset L^H & \longleftarrow & H \end{array}$$

Teo (Artin): Si H grupo finito de automorfismos de un cuerpo F, $K = F^H$, $[F:K] \leq \#H$.

$$\begin{matrix} F \\ | \\ | \leq \#H \\ | \\ K = F^H \\ | \\ id \end{matrix}$$

D/ $H = \{\sigma_1, \dots, \sigma_n\}$, sean $\{\beta_1, \dots, \beta_m\}$ elts de F. Queremos ver que si $\boxed{m > n}$, los β_i's son K l.d.

Si fueran K-l.d., existen $\alpha_1, \dots, \alpha_m \in K$ tales que:

$$\begin{cases} \alpha_1 \beta_1 + \cdots + \alpha_m \beta_m = 0. \\ \text{Aplico } \sigma_2: \quad \alpha_1 \sigma_2(\beta_1) + \cdots + \alpha_m \sigma_2(\beta_m) = 0 \\ \vdots \\ \text{Aplico } \sigma_n: \quad \alpha_1 \sigma_n(\beta_1) + \cdots + \alpha_m \sigma_n(\beta_m) = 0 \end{cases}$$

Miramos el sistema:

$$\begin{cases} \beta_1 X_1 + \cdots + \beta_m X_m = 0 \\ \vdots \\ \sigma_n(\beta_1) X_1 + \cdots + \sigma_n(\beta_m) X_m = 0 \end{cases}$$

¿Hay solución no nula en K? n ecuaciones (en F), m incógnitas, $m > n$

Por Álgebra Lineal, existe $(\alpha_1, \dots, \alpha_m) \in F^m$ solución no trivial.

Sea $\vec{a} = (\alpha_1, \dots, \alpha_m)$ solución no trivial con el mayor número posible de coordenadas nulas. Además, puedo suponer que la primera es no nula y $\alpha_1 = 1$ (cjto de soluciones es subespacio)

Afirmo: $\vec{a} \in K^m$.

Supongamos que no, $a_2 \in F \setminus K$, $\exists i / \sigma_i(a_2) \neq a_2$

$\sigma_i(\vec{a})$ también es solución $(i=2)$

$$a_1 s_1 + \dots + a_n s_n = 0 \xrightarrow{\sigma_2} \sigma_2(a_1)\sigma_2(s_1) + \dots + \sigma_2(a_n)\sigma_2(s_n) = 0$$

σ_3 ↓

$\sigma_3(\vec{a})$ cumple 3ª ec. ; $\sigma_2(\vec{a})$ cumple 2ª ecuación.

Como $\vec{a}$ cumple todas, el vector $\sigma_i(\vec{a})$ también (aparecen en otro orden).

Obs: $\{$ coordenadas donde $\vec{a} = 0\} = \{$ coordenadas donde $\sigma_i(\vec{a}) = 0\}$

$\vec{a} - \sigma_i(\vec{a})$ → es solución. ambos lo son.

→ # coordenadas nulas > # coordenadas nulas de $\vec{a}$

$\neq 0$ ($\sigma_i(a_2) \neq a_2$)

Absurdo ☒

Corolario: F cuerpo, H grupo finito de automorfismos de F y $K = F^H$. Entonces, $Aut_K(F) = H$ y $[F:K] = \#H$.

D/

F

$|$ $Aut_K(F) \supset H$ (pues H en K es la identidad)

$K = F^H$

$$\#H \leq \#Aut_K(F) \leq [F:K] \leq \#H \Rightarrow \text{todos iguales.}$$ ☒

En el Teo de Galois, H subgrupo de $Aut_K(L)$

$$H \to L^H \to Aut_{L^H}(L) = H$$

↑ corolario. una de las composiciones da la identidad.

(vale siempre)

Hipótesis: L/k es buena si $[L:F] = \#Aut_F(L)$ $\forall$ $k \subset F \subset L$.

Afirmo: si L/k es buena, $F \to Aut_F(L) \to L^{Aut_F(L)} = F$

Pues $F \subseteq L^{Aut_F(L)} = \{\alpha \in L : \sigma(\alpha) = \alpha \ \forall \sigma \in Aut_F(L)\}$

$$[L : L^{Aut_F(L)}] \leq [L:F] \Rightarrow F = L^{Aut_F(L)}$$

$\#Aut_F(L)$ ↑ = hipótesis

$$[L:F] = [L : L^{Aut_F(L)}] \cdot [L^{Aut_F(L)} : F]$$

$\Rightarrow$ vale que la otra composición también es la identidad ☐

Ejemplo: $\mathbb{Q}$, $\mathbb{Q}(\sqrt[3]{2})$

$\mathbb{Q}(\sqrt[3]{2})$

$| 3$

$\mathbb{Q}$

$\{id\}$

$\{k \subset F \subset \mathbb{Q}(\sqrt[3]{2})\} \longleftrightarrow Aut_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}))$

$\{\mathbb{Q}, \mathbb{Q}(\sqrt[3]{2})\}$ ← imagen

2 elementos

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

$\sigma : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2})$

$\sqrt[3]{2} \to$ una raíz de $x^3 - 2$

$$m_{\sqrt[3]{2}}(\sqrt[3]{2}) = 0 = \sigma(m_{\sqrt[3]{2}}(\sqrt[3]{2})) = \sigma((\sqrt[3]{2})^3 - 2)$$

$$= \sigma(\sqrt[3]{2})^3 - 2 = m_{\sqrt[3]{2}}(\sigma(\sqrt[3]{2}))$$

Como $x^3 - 2$ tiene una sola raíz en $\mathbb{Q}(\sqrt[3]{2})$, $\sigma(\sqrt[3]{2}) = \sqrt[3]{2} \Rightarrow \sigma = id$.

Importante: $p(x) \in K[x]$, α raíz de $p(x)$ en L, $\sigma : L \to F$ K-morfismo $\Rightarrow$ $\sigma(\alpha)$ es una raíz de $p(x)$.

Def: una extensión algebraica L/K se dice **normal** si todo polinomio irreducible en $K[x]$ que tiene una raíz en L, tiene a todas sus raíces en L.

Obs: equivalentemente, $\forall \alpha \in L$, $m_\alpha(x)$ tiene todas las raíces en L.

Lema: si L/K es normal, $K \subset F \subset L \Rightarrow L/F$ es normal

$$\text{normal}\left(\begin{array}{c} L \\ | \\ F \\ | \\ K \end{array}\right)\text{normal}$$

D/ $\alpha \in L$, $m_\alpha(x) \in K[x]$ es un polinomio en $F[x]$ y α es raíz, $\boxed{m_{\alpha,F}(x) \mid m_\alpha(x)}$

Como L/K normal, todas las raíces de $m_\alpha(x)$ están en $L \Rightarrow$ las raíces de $m_{\alpha,F}(x)$ también lo están. ∎

Ejemplo:

$$\text{normal}\left[\begin{array}{c} \mathbb{Q}(\sqrt[3]{2}, \xi_3) \\ | \ 2 \\ \mathbb{Q}(\sqrt[3]{2}) \\ | \ 3 \\ \mathbb{Q} \end{array}\right]$$

$\mathbb{Q}(\sqrt[3]{2}, \xi_3)$ / $\mathbb{Q}$: normal

$\mathbb{Q}(\sqrt[3]{2})$ / $\mathbb{Q}$: no es normal, $x^3 - 2$ tiene una sola raíz.

Def: una extensión L/K algebraica se dice **Galois** si es normal y separable.

Teo: si L/K tal que L es el cuerpo de descomposición de un polinomio en $K[x]$ entonces L/K es normal. (todas son así).

D/ Sea $p(x) \in K[x]$ t.q. L es el cpo de desc. de $p(x)$.
$\rightsquigarrow$ en $L[x]$, $p(x) = (x - \alpha_1) \cdots (x - \alpha_n)$

$\rightarrow$ $L = K[\alpha_1, \dots, \alpha_n]$.

Sea $\beta \in L$. $m_\beta(x) \in K[x]$ irreducible. Supongamos que $m_\beta(x)$ no se factoriza linealmente en L.

Sea M = cpo de descomposición de $m_\beta(x) \in L[x]$

M — $m_{\beta(x)} \in L[x]$

L — $\}$

K — $m_{\beta(x)} \in K[x]$

Digamos $\gamma \in M$ raíz de $m_\beta(x)$ que no está en L.

Objetivo: construir un K-morfismo de L en M, $\beta \to \gamma$.

$$\begin{array}{ccc} L & \xrightarrow{\tilde{\sigma}} & L[\gamma] \\ | & & | \\ K[\beta] & \xrightarrow[\sigma]{\simeq} & K[\gamma] \\ | & & | \\ K & \xrightarrow{id} & K \end{array}$$

$K[\beta] \simeq K[x]/m_\beta(x)$

El K-morfismo $\sigma : K[\beta] \to K[\gamma]$ se extiende a un K-morfismo $\tilde{\sigma} : L \to L[\gamma] \subset M$ (ver clase 2).

Por otro lado, $L = K[\alpha_1, \dots, \alpha_n]$ (α_i raíces de $p(x)$), $\tilde{\sigma}(\alpha_i) = \alpha_j \Rightarrow \tilde{\sigma}(L) = L$

$\beta \in L \Rightarrow \tilde{\sigma}(\beta) = \gamma \in L$. Abs!.

Teo: Si L/K finita, L/K es Galois $\iff [L:K] = \#Aut_K(L)$

Coro: La hipótesis $[L:F] = \#Aut_F(L)$ $\forall K \subset F \subset L$ vale $\iff L/K$ es Galois.

Demo (Teo). $\Rightarrow$) $L = K[\alpha_1, \dots, \alpha_n]$, cpo de descomposición de $m_{\alpha_1}(x) \cdot \dots \cdot m_{\alpha_n}(x) = p(x) \Rightarrow [L:K] \geq \#Aut_K(L)$ y vale la igualdad $\iff p(x)$ es separable. ✓

$L \subset M$ = cpo de desc. de $m_\alpha(x)$ hipótesis.

$\Leftarrow$) Supongamos $L = K[\alpha]$, $\#\mathrm{Aut}_K(L) \overset{=}{\leq} \#\mathrm{Hom}_K(L, M) \overset{=}{\leq} [L:K]$

La última es igualdad $\Rightarrow$ $m_\alpha(x)$ es separable.

La segunda igualdad $\Rightarrow$ $m_\alpha(x)$ es separable $\Rightarrow$ L/K separable.

$\#\mathrm{Aut}_K(L) = \#\{\text{raíces de } m_\alpha(x) \text{ en } L\} = [L:K] = gr(m_\alpha(x))$

σ^6 está determinado por su valor en α.

$K[\alpha] : L \simeq K[x]/m_\alpha(x) \simeq K[\beta]$ para β cualquier raíz de $m_\alpha(x)$ en M.

$\Rightarrow L$ = cuerpo de descomposición de $m_\alpha(x) \Rightarrow L/K$ normal

Teo: Si L/K Galois, $G = Gal(L/K) = \mathrm{Aut}_K(L)$, hay una biyección entre:

$$\{K \subset F \subset L\} \longrightarrow \{H < Gal(L/K)\}$$

$$F \longrightarrow \mathrm{Aut}_F(L)$$

$$F^H \longleftarrow H$$

$$Gal\begin{bmatrix} L \\ | \\ F \\ | \\ K \end{bmatrix} Gal \quad ??$$

Además, F/K es Galois $\Leftrightarrow$ H es un subgrupo normal de G.