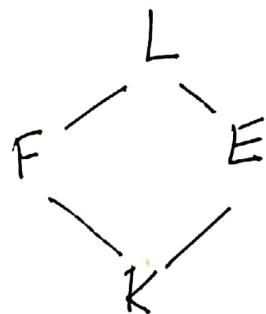


$$\sigma \zeta(\eta_5) = \eta_5^2 \quad ; \quad \sigma^r \zeta(\eta_5) = \eta_5^{2^r} \\ \sigma \zeta(\sqrt[5]{2}) = \eta_5^{2^5/2} \quad ; \quad \sigma^r \zeta(\sqrt[5]{2}) = \eta_5^{5^r/2}$$

Se obtiene $\sigma \zeta^r = \zeta^{\sigma^r}$ (grupo de 20 elementos, dado por X^r , $C_4 \times C_5$ cuando $r=1$).

[3] Supongamos $L = FE$



L/k , F/k Galoisianas, $F \cap E = K$. Entonces se tiene

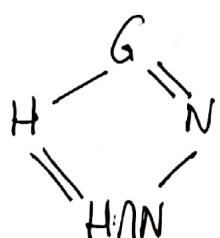
$$[L:E] = [F:K].$$

- Demostración - Sean $G = \text{Gal}(L/k)$, $H = \text{Gal}(L/E)$, $N = \text{Gal}(L/F)$.

Como $H \cap N = \{ \text{id} \}$, $HN = G$

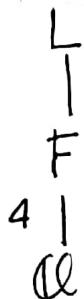
$$\therefore G \cong H \times N$$

$$\text{Además } G/N \cong H/(H \cap N) \cong H$$



[E] Encuentra todos los cuerpos intermedios entre \mathbb{Q} y $\mathbb{Q}(\sqrt{7}, \sqrt{11}, \sqrt{13})$

$$\text{Sea } F = \mathbb{Q}(\sqrt{7}, \sqrt{11})$$



$\sqrt{7} \in \mathbb{Q}(\sqrt{11})$, $\sigma(\sqrt{7}) = -\sqrt{7}$, $\sigma(a+b\sqrt{11}) = a-b\sqrt{11}$. Luego $\sqrt{7} = b\sqrt{11}$
 $\sqrt{13} \in \mathbb{Q}(\sqrt{7}, \sqrt{11})$:

$$\sqrt{13} = a + b\sqrt{7} + c\sqrt{11} + d\sqrt{77}$$

$$\sigma(\sqrt{13}) = -\sqrt{13}$$

$$\lambda_1(a + b\sqrt{7} + c\sqrt{11} + d\sqrt{77}) = a - b\sqrt{7} + c\sqrt{11} - d\sqrt{77}$$

$$\lambda_2, \lambda_3$$

$$\sigma = \lambda_1 \rightarrow \sqrt{13} = b\sqrt{7} + d\sqrt{77}$$

$$\frac{\sqrt{13}}{\sqrt{7}} = b + d\sqrt{11} \in \mathbb{Q}(\sqrt{11}) \iff$$

$$\sigma(\mathbb{Q}(\sqrt{13}))$$

$$\begin{matrix} \sigma \\ \sqrt{7} \mapsto -\sqrt{7} \\ \sqrt{11} \mapsto \sqrt{11} \\ \sqrt{13} \mapsto \sqrt{13} \end{matrix}$$

$$\begin{matrix} \lambda \\ \sqrt{7} \mapsto \sqrt{7} \\ \sqrt{11} \mapsto -\sqrt{11} \\ \sqrt{13} \mapsto \sqrt{13} \end{matrix}$$

$$\begin{matrix} \tau \\ \sqrt{7} \mapsto \sqrt{7} \\ \sqrt{11} \mapsto \sqrt{11} \\ \sqrt{13} \mapsto -\sqrt{13} \end{matrix}$$

$$G \cong C_2 \times C_2 \times C_2 \cong \mathbb{F}_2^3$$

$$\text{Recta } \langle v \rangle = \{0, v\}$$

hay 8-1=7 rectas

$$\text{Planes } T = \{(x_1, x_2, x_3) / a_1x_1 + a_2x_2 + a_3x_3 = 0\}$$

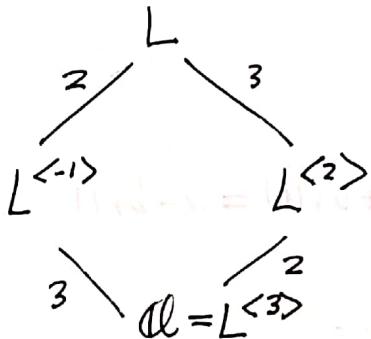
$$= \{\vec{x} / \vec{x} \cdot \vec{a} = 0\}$$

Hay 7 planes

Hay 16 cuerpos intermedios.

[5] Para $\eta_7 = e^{\frac{2\pi i}{7}}$. $L = \mathbb{Q}(\eta_7)$. $[L:\mathbb{Q}] = 6$.

$$\text{Gal}(L/\mathbb{Q}) \cong C_6 \cong (\mathbb{Z}/7\mathbb{Z})^* = \langle 3 \rangle$$



$$L^{<-1>} = \mathbb{Q}(\eta_7 + \eta_7^{-1}) = L \cap \mathbb{R}$$

$$L^{<2>} = \mathbb{Q}(\eta_7 + \eta_7^2 + \eta_7^4) = \mathbb{Q}(\sqrt{-7})$$

L

\mathbb{Q}

Tenemos $\mathbb{Q}(e^{\frac{2\pi i}{7}}) \cap \mathbb{R} = \mathbb{Q}(\cos \frac{2\pi}{7})$ ($\cos \frac{2\pi}{7}$ es algebraico)

$$L^{<-1>} = \langle \eta + \eta^{-1}, \eta^2 + \eta^{-2}, \eta^3 + \eta^{-3} \rangle_{\mathbb{Q}}$$

Tomando $a = \eta + \eta^{-1}$, calculamos $1, a, a^2, a^3$.

$$-1 = -\eta - \eta^{-1} - \eta^2 - \eta^{-2} - \eta^3 - \eta^{-3}$$

[6] $f(x)$ polinomio de grado 4 separable. L cuerpo de descomposición.

$$f(x) = (x-a_1) \dots (x-a_4)$$

$G = \text{Gal}(L/\mathbb{Q})$ actúa en $\{a_1, \dots, a_4\}$ transitivamente,

$$G \hookrightarrow S_4$$

transitiva

$$S_4, A_4, K = \langle (12)(34), (13)(24) \rangle, C_4, D_4 = \langle (1234), (14)(23) \rangle$$

Observación. L/k Galoisiana

$$\left\{ \begin{array}{l} F \text{ enteros} \\ K \subseteq F \subseteq L \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{Subgrupos} \\ H \subseteq G \end{array} \right\}$$

$$G = \text{Gal}(L/k),$$

$$H \subseteq \Gamma \iff L^H \subseteq L^\Gamma$$

donde $H \mapsto L^H$, $F \mapsto \text{Gal}(L/F)$. En particular, $H, \Gamma \leq G$

$$L^H L^\Gamma = L^{H \cap \Gamma}$$

$$L^H \cap L^\Gamma = L^{<H, \Gamma>} \leftarrow \text{subgrupo generado.}$$

Ejemplo. $L = \mathbb{Q}(\omega, \sqrt[3]{2})$, $K = \mathbb{Q}$

$$\text{Gal}(L/K) = \left\langle \sigma, \tau \mid \begin{array}{l} \sigma^2 = \text{id} \\ \tau^3 = \text{id} \\ \sigma\tau = \tau^{-1}\sigma \end{array} \right\rangle$$

$$\begin{array}{l|l} \sigma(z) = \bar{z} & \sigma\tau\sigma\tau = \text{id} \\ \tau(\sqrt[3]{2}) = \omega\sqrt[3]{2} & \sigma\tau(\omega\sqrt[3]{2}) = \omega\sqrt[3]{2} \\ \tau(\omega) = \omega & \end{array}$$

$$L^{<\sigma>} = \mathbb{Q}(\sqrt[3]{2})$$

$$L^{<\tau>} = \mathbb{Q}(\omega)$$

$$L^{<\sigma\tau>} = \mathbb{Q}(\omega, \sqrt[3]{2})$$

$$L^{<\sigma\tau^2>} = \mathbb{Q}(\omega^2\sqrt[3]{2})$$

$$L^{<\tau>} \cap L^{<\sigma\tau>} = L^{<\tau, \sigma\tau>} = L^G \Rightarrow L^{<\tau>} \cap L^{<\sigma\tau>} = \mathbb{Q}.$$

$$\mathcal{C}(\omega^3\sqrt{2}) \cap \mathbb{R} = \emptyset, \quad \mathbb{R} = \mathbb{C}^{<\tilde{\sigma}>}, \quad \tilde{\mathbb{R}} = L^{<\sigma>} = \mathbb{R} \cap L$$

$$\mathcal{C}(\omega^3\sqrt{2}) \cap \mathbb{R} = \mathcal{C}(\omega^3\sqrt{2}) \cap \tilde{\mathbb{R}} \quad (A \subseteq B, A \cap C = A \cap (B \cap C))$$

$$\mathcal{C}(\omega^3\sqrt{2}) \cap \mathbb{R} = L^{<\sigma\tau>} \cap L^{<\sigma>} = \emptyset.$$

$$|\langle H, \Gamma \rangle| \geq \frac{|H||\Gamma|}{|H \cap \Gamma|}.$$

Si L/K es Galosiana, $F, E \subseteq L$ subcuerpos, $F, E \supseteq K$
entonces

$$[L : F \cap E] \geq \frac{[L : F][L : E]}{[L : FE]}$$

$$[L : F] = \frac{[L : K]}{[F : K]}$$

$$\frac{[L : K]}{[F \cap E : K]} \geq \frac{[L : K][L : K][FE : K]}{[F : K][E : K][L : K]}$$

$$[F \cap E : K][FE : K] \leq [F : K][E : K]$$

Teorema fundamental del álgebra

Lema. Todo polinomio de grado impar con coeficientes reales tiene una raíz en \mathbb{R} .

Lema. Todo número complejo tiene una raíz cuadrada.

- Demarcación -

$$at + bi = r e^{i\alpha} = (\sqrt{r} e^{i\alpha/2})^2$$

Teatrero (fundamental del álgebra). $\mathbb{C} = \overline{\mathbb{C}}$.

- Demostración - Sea L/\mathbb{C} extensión algebraica finita. Por demostrar $L \subseteq \mathbb{C}$. Sin pérdida de generalidad, L/\mathbb{R} es Galoiana.

Definimos $G = \text{Gal}(L/\mathbb{R})$, $P \leq G$ un 2-grupo de Sylow.

$$[\mathbb{C} : \mathbb{R}] = 2 \mid [L : \mathbb{R}]$$

$$E = L^P, [L : L^P] = |P|$$

$$[L^P : \mathbb{R}] = \frac{|G|}{|P|} \leftarrow \text{impar}$$

Para $a \in L^P$, $[\mathbb{R}(a) : \mathbb{R}] \leftarrow \text{impar}$, $\text{in}_{\mathbb{R}, a}(x)$ tiene grado impar.

Ocupando la raíz,

$$[\mathbb{R}(a) : \mathbb{R}] = 1 \quad (a \in \mathbb{R})$$

Por lo tanto, $L^P = \mathbb{R}$. Luego $|G| = |P|$

$\therefore G = P$ es un 2-grupo

$H = \text{Gal}(L/\mathbb{C}) \leq G$. H es un 2-grupo.

Si $L \neq \mathbb{C}$, $H \neq \text{id}$,

$$|H| = 2^t \quad t \geq 1$$

H tiene subgrupo N de orden $|N| = 2^{t-1}$.

$E = L^N$, entonces $[E : \mathbb{C}] = 2$, pero

$$[E : \mathbb{C}]$$

$$[L^N : L^H] \stackrel{||}{=} |H/N|$$

$\therefore E = \mathbb{C}(\sqrt{2})$ algún $\neq \rightarrow \Leftarrow$ (Contradice lema).

Extensiones separables e inseparables

L/K extensión algebraica, $\alpha \in L$. $m(x) = m_{K, \alpha}(x)$

$$m(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$$

$\text{char } K = p \ (\neq 0)$

Tenemos α ^{inseparable} $\not\in K \Leftrightarrow m(x) = g(x^p)$

Sea $t \geq 0$, tal que

$$m(x) = h(x^{pt}) \text{ con } t \text{ maximal, } h \in K[x].$$

$$\alpha^{pt} \in L,$$

$$m_{K, \alpha^{pt}}(x) = h(x)$$

$$h(\alpha^{pt}) = m(\alpha) = 0$$

$h(x)$ no es polinomio en x^p . α^{pt} es separable sobre K .

$$K(\alpha)$$



$$K(\alpha^{pt})$$

sep.

$$K$$

$$[K(\alpha) : K(\alpha^{pt})] = \frac{[K(\alpha) : K]}{[K(\alpha^{pt}) : K]} = \frac{\deg m}{\deg h} = p^t$$

Luego $m_{K(\alpha^{pt}), \alpha}(x) = x^{p^t} - \alpha^{p^t}$

en la clausura algebraica: $x^{p^t} - \alpha^{p^t} = (x - \alpha)^{p^t}$

α se dice totalmente inseparable sobre K si $ir_{K,\alpha}(x)$ tiene una sola raíz en \bar{K} .

L/K se dice totalmente inseparable si cada $\alpha \in L$ es totalmente inseparable sobre K .

Proposición. Las siguientes afirmaciones son equivalentes. Si

$L = K[\alpha_1, \dots, \alpha_n]$ extensión finita de K

(1) L/K totalmente inseparable

(2) $\alpha_1, \dots, \alpha_n$ son totalmente inseparables sobre K .

(3) Todo homomorfismo $\varphi: K \rightarrow \mathcal{D}_2$, con $\mathcal{D}_2 = \bar{\mathcal{D}}_2$ se extiende de manera única a $\tilde{\varphi}: L \rightarrow \mathcal{D}_2$.

(4) Existe un único homomorfismo $\tilde{\varphi}: L \rightarrow \bar{K}$ que extiende la identidad en K ($\tilde{\varphi}|_K = id_K$).

- Demostración - (Ejercicio)

Sea L/K extensión algebraica,

$$L_{\text{sep}} = \left\{ \alpha \in L / K(\alpha)/K \text{ separable} \right\}$$

Observación. $L_{\text{sep}} \subseteq L$ subgrupo.

$\alpha, \beta \in L_{\text{sep}} \Rightarrow K(\alpha, \beta)/K$ separable

$$K(\alpha + \beta) \subseteq K(\alpha, \beta)$$

$\Rightarrow K(\alpha + \beta)/K$ separable

$\Rightarrow \alpha + \beta \in L_{\text{sep}}$.

Similamente, $\alpha - \beta, \alpha \cdot \beta, \alpha/\beta \in L_{\text{sep}}$.

$\alpha \in L$ analgüera

$$\begin{array}{ccc} \alpha^{pt} \in L_{\text{sep}} & \xrightarrow{\quad L \quad} & K(\alpha) \\ & \leftarrow \text{tot. inseparable} & | \\ & L_{\text{sep}} & | \\ & \leftarrow \text{sep} & | \\ & K & \leftarrow \text{sep} \end{array}$$

Proposición. L/L_{sep} es totalmente inseparable.

$$[K(\alpha) : K(\alpha^{pt})] = p^t$$

Sea $L_{t.i.} = \{ \alpha \in L / \begin{cases} K(\alpha)/K \text{ es} \\ \text{totalmente inseparable} \end{cases} \}$. Tenemos

$$\begin{array}{ccc} L & & \\ \searrow \text{no siempre separable.} & & \swarrow t.i. \\ L_{t.i.} & & L_{\text{sep}} \\ & \searrow t.i. & \swarrow \text{sep.} \\ & K & \end{array}$$

Ejemplo. Consideremos el anillo $\mathbb{F}_2(x, y)$

$$K = \mathbb{F}_2(u^2, v^2); \quad u = x+y$$

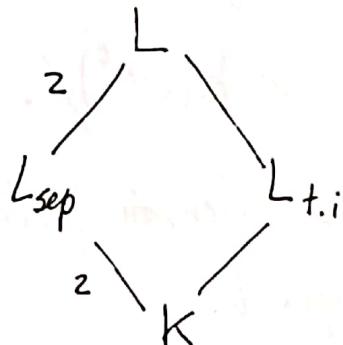
$$L = \mathbb{F}_2(x^2, y); \quad v = xy$$

$$[\mathbb{F}_2(x^2, y^2) : \mathbb{F}_2(u^2, v^2)] = 2$$

$$\text{Gal} \left(\mathbb{F}_2(x^2, y^2) / \mathbb{F}_2(u^2, v^2) \right) = S_2 = C_2$$

$$L_{\text{sep}} = \mathbb{F}_2(x^2, y^2)$$

$$\begin{aligned} u^2 &= x^2 + y^2 \\ v^2 &= x^2 y^2 \end{aligned}$$



$$L = L_{\text{sep}}(y)$$

$$\alpha \in L_{t.i} \neq L, [L_{t.i} : K] \leq 2$$

$$\alpha \notin K, m_{K, \alpha}(x) = (x - \alpha)^2 = x^2 - \alpha^2 \therefore \alpha^2 \in K$$

Tomando $\alpha = h(x^2, y)$, entonces $\alpha^2 = h(x^4, y^2)$.

$\alpha^2 \in K \Rightarrow$ simétrica en x^2 e y^2 .

$$h(x^4, y^2) = h(y^4, x^2)$$

$$\alpha^2 \in \mathbb{F}_2(x^4, y^4) \Rightarrow \alpha \in \mathbb{F}_2(x^2, y^2) \quad \left. \begin{array}{l} \alpha \text{ simétrico} \\ \end{array} \right\} \Rightarrow \alpha \in K$$

$$\therefore L_{t.i} = K$$

Tenemos $L = K(\alpha)$, $m(x) = \text{irr}_{K,\alpha}(x)$ ($p = \text{char } K$)

$$m(x) = g(x^{p^t}), t \text{ maximal}$$

luego $\text{irr}_{K,\alpha^{p^t}}(x) = g(x)$

$$K(\alpha^{p^t})/K \text{ separable.}$$

Proposición. Si L/K extensión finita totalmente inseparable, entonces $[L : K] = p^t$, algún t .

- Demarcación - Supongamos primero que $L = K(\alpha)$.

$$m(x) = \text{irr}_{K,\alpha}(x)$$

$$\text{Si } m(x) = g(x^{p^t}), t \text{ maximal} \Rightarrow \text{irr}_{K,\alpha^{p^t}}(x) = g(x), \\ K(\alpha^{p^t})/K \text{ separable.}$$

Pero L/K t.i. Luego $K(\alpha^{p^t})/K$ totalmente inseparable.

$$\therefore K = K(\alpha^{p^t})$$

$$\therefore \deg g = 1$$

$$\text{En particular, } g(x) = x - \alpha^{p^t}, m(x) = x^{p^t} - \alpha^{p^t}.$$

Supongamos ahora, $L = K(\alpha_1, \dots, \alpha_n)$, $E_i = K(\alpha_1, \dots, \alpha_i)$

L/K t.i. $\Rightarrow L/E_i$ t.i para cada i .

$$\Rightarrow E_{i+1}/E_i \text{ t.i.}$$

Pero $[E_{i+1} : E_i] = p^{t_i}$ ya que $E_{i+1} = E_i(\alpha_{i+1})$.

$$[L:K] = \prod_{i=0}^{n-1} [E_{i+1}:E_i] = p^{\sum_{i=0}^{n-1} t_i}, \quad E_0 = K$$

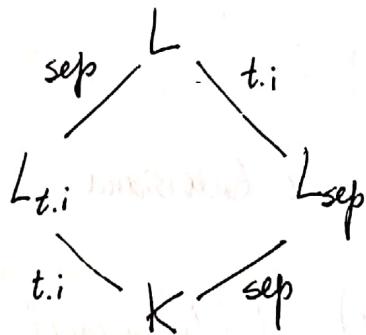
□

Observación. Si L/K t.i. y $[L:K] = p^t$, entonces para todo $\alpha \in L$, $[K(\alpha):K] = p^r$, $r < t$. $\alpha^{p^r} \in K$, luego $\alpha^{p^t} \in K$.

$$L^{p^t} = \{ \alpha^{p^t} / \alpha \in L \} \subseteq K$$

Ejemplo. $K = \mathbb{F}_2(x^2, y^2)$, $L = \mathbb{F}_2(x, y)$. L/K t.i., $[L:K] = 4 = 2^2$, pero $L^2 = K$.

Proposición. Si L/K normal, entonces $L/L_{t.i.}$ es una extensión galoisiana.



- Demostación -

$$[L:K] = n$$

$$[L_{sep}:K] = m$$

$$[L:L_{sep}] = p^t$$

Observación. $\text{id}: K \hookrightarrow \bar{K}$ se extiende de m -maneras a $\tilde{\varphi}: L_{sep} \hookrightarrow \bar{K}$. Luego hay m -extensiones $\tilde{\varphi}: L \rightarrow \bar{K}$, $\tilde{\varphi}|_K = \text{id}$.

$$L/K \text{ normal} \Rightarrow \tilde{\varphi}(L) = L$$

Por lo tanto $|\text{Gal}(L/K)| = m$.

Definimos $G := \text{Gal}(L/K)$. Sea $F = L^G$,

L/F galoisiana ; $\text{Gal}(L/F) \cong G$.

Sea $\alpha \in F$, $\tilde{\varphi}(\alpha) = \alpha$ para toda extensión de la identidad a L .

Luego hay una única extensión de la identidad en K , a $K(\alpha)$

$\therefore \alpha$ es t.i sobre K

$\therefore F/K$ t.i.

En particular, $F \subseteq L_{\text{t.i.}}$, pero L/F separable, así que

si $\alpha \in L_{\text{t.i.}}$, α t.i sobre $K \rightarrow \alpha$ t.i sobre F

$\therefore \alpha \in F$

Luego $F = L_{\text{t.i.}}$.

$\therefore L/L_{\text{t.i.}}$ es Galoisiana. \blacksquare

Observación . $L_{\text{t.i.}} = L^{\text{Gal}(L/K)}$ (L/K normal)

$\tilde{\varphi} \in \text{Gal}(L/K)$

$\tilde{\varphi}(L_{\text{sep}})/K$ separable.

$\therefore \tilde{\varphi}(L_{\text{sep}}) = L_{\text{sep}}$

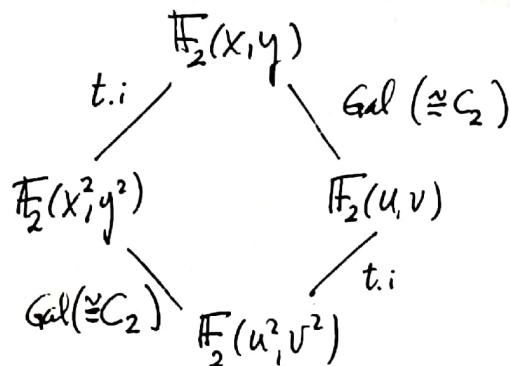
$\tilde{\varphi}(L_{\text{sep}})$

L/K separable $\Rightarrow L_{\text{sep}}/K$ Galoisiana.

$\text{Gal}(L_{\text{sep}}/K) \cong \text{Gal}(L/L_{\text{t.i.}})$

Ejemplo. $L = \mathbb{F}_2(x, y)$, $K = \mathbb{F}_2(u, v)$; $u = x+y$, $v = xy$
 x, y son raíces de $T^2 + uT + v = 0$

$$\text{Gal}(\mathbb{F}_2(x, y)/\mathbb{F}_2(u, v)) \cong S_2 \cong C_2$$



$a \in \mathbb{F}_2(x, y)$, se tiene $a = \frac{f(x, y)}{g(x, y)}$, donde

$a^2 = \frac{f(x^2, y^2)}{g(x^2, y^2)}$; luego $a^2 \in \mathbb{F}_2(x^2, y^2)$. Por lo tanto, $L = F(a)$ tiene L .

Teorema (del elemento primitivo)

Sea L/K una extensión finita, entonces existe $a \in L$ con $L = K(a)$ si y sólo si el conjunto

$$\{F \text{ anillo} / K \subseteq F \subseteq L\}$$

es finito.

- Demarcación - Supongamos que $L = K(a)$. Sea $m(x) = \text{irr}_{K,a}(x)$ y sean $\{G_1(x), \dots, G_N(x)\}$ los divisores monólicos de $m(x)$ en $L[x]$.
 $G_i(x) = x - a$, algún i (existe i)

Sea E_i el anillo generado por los coeficientes de $G_i(x)$.

Sea F un cuerpo con $K \subseteq F \subseteq L$,

$$m'(x) = m_{F,a}(x)$$

$$m'(x) \mid m(x)$$

Luego $m'(x) = G_i(x)$. Se sigue que $m'(x) \in F[x]$

$$\therefore E_j \subseteq F$$

$$[L:F] = \deg m' = \deg G_i$$

$$m_j(x) = m_{E_j,a}(x)$$

$$m_j(x) \mid G_j(x)$$

$$G_j(a) = m'(a) = 0, \quad G_j(x) \in E_j[x]$$

$$\text{Teneemos } [L:E_j] = \deg m_j \leq \deg G_i = [L:F]$$



$$\therefore [L:E_j] = [L:F]$$

$$E_j = F,$$

Supongamos que $L \neq k(a)$ para todo $a \in L$.

Caso I: K es infinito.

Sea $a \in L$, con $k(a)$ maximal, y sea $b \notin k(a)$, $a \notin k(b)$
(si no $k(a) \subseteq k(b)$)

Sea $E_\lambda = k(a + \lambda b)$, $\lambda \in K$.

Supongamos $E_\lambda = E_{\lambda'}$, $a + \lambda b \in E_\lambda$
 $a + \lambda' b \in E_{\lambda'} = E_\lambda$

Luego $b(\lambda - \lambda') \in E_\lambda$. Si $\lambda \neq \lambda'$, entonces $b \in E_\lambda$

$$\begin{aligned} & \because a \in E_\lambda \\ & \therefore k(a) \subsetneq k(a + \lambda b) \quad (\Leftrightarrow) \end{aligned}$$

Con ello, $\{E_\lambda \mid \lambda \in K\}$ es una familia infinita de cuerpos intermedios.

Caso II: K finito, luego L finito

$$K = \mathbb{F}_q, L = \mathbb{F}_{q^n}$$

$$L^* \cong C_{q^n-1} = \langle \alpha \rangle, L = k(\alpha) \quad (\Leftrightarrow)$$

Corolario. Si L/K es una extensión finita y separable, existe $\alpha \in L$ con $L = k(\alpha)$.

-Demostración- Podemos suponer L/K Galoiana.

$$\begin{array}{c} \tilde{L} \\ | \\ L \\ | \\ I \\ | \\ K \end{array} \quad \text{Gal.} \quad \begin{array}{l} \text{Basta ver que hay un} \\ \text{número finito de cuerpos} \\ \text{entre } K \text{ y } \tilde{L} \end{array}$$

$$\left\{ \begin{array}{l} \text{Cuerpo} \\ K \subseteq F \subseteq \tilde{L} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{subgrupos } H \\ \text{de } G = \text{Gal}(\tilde{L}/K) \end{array} \right\}$$

Extensiones ciclotómicas

$\eta \in L$ es raíz de la unidad si $\eta^n = 1$, algún n

Para char $L = p$, $a^p = 1$
 $(a-1)^p = 0$

$$\therefore a-1=0$$

$$\therefore a=1$$

$$\eta^{pt_m} = 1 \Rightarrow \eta^m = 1$$

El orden de una raíz de la unidad es relativamente primo con la característica.

Extensión ciclotómica. $L = K(\eta)$, η raíz de la unidad.

Si η tiene orden n , entonces las raíces de $x^n - 1 = 0$ son $1, \eta, \eta^2, \dots, \eta^{n-1} = \eta^{n-1}$.

$K(\eta)/K$ Galoiana y $\sigma \in \text{Gal}(K(\eta)/K)$, existe $\Gamma(\sigma) \in (\mathbb{Z}/n\mathbb{Z})^*$

$$\text{con } \sigma(\eta) = \eta^{\Gamma(\sigma)}$$

$$\begin{aligned}\sigma z = \sigma(z/\eta) &= \sigma(\eta^{\Gamma(\sigma)}) = (\sigma(\eta))^{\Gamma(z)} = (\eta^{\Gamma(\sigma)})^{\Gamma(z)} \\ &= \eta^{\Gamma(\sigma)\Gamma(z)}\end{aligned}$$

$$\therefore \Gamma(\sigma z) = \Gamma(\sigma)\Gamma(z)$$

$\Gamma: \text{Gal}(K(\eta)/K) \rightarrow (\mathbb{Z}/n\mathbb{Z})^*$ homomorfismo inyectivo.

$\text{Gal}\left(\frac{L(\eta)}{L}\right) \cong (\mathbb{Z}/n\mathbb{Z})^*$; $K = L^H$, con $H \leq (\mathbb{Z}/n\mathbb{Z})^*$

Extensiones de Kummer

Supongamos que $\rho \in K$, donde ρ es raíz de la unidad de grado n .

$\rho^n = 1$, $\rho^m \neq 1$, $0 < m < n$. ($p \nmid n$, $p = \text{char } K$).

Sea $a \in K$, $b = \sqrt[n]{a} \in \bar{K}$, $L = K(b)$

Si $m(x) = \text{irr}_{K,b}(x)$, entonces $m(x) \mid x^n - a$

$$x^n - a = \prod_{i=0}^{n-1} (x - \rho^i b)$$

Automáticamente, $K(b)/K$ es Galoisiana, donde $\sigma \in G = \text{Gal}(K(b)/K)$

$$\sigma(b) = \rho^i b$$

En particular, existe $\varphi: G \hookrightarrow \mathbb{Z}/n\mathbb{Z}$ ($\sigma \mapsto i$)

$$\sigma_i(b) = \rho^i b, \quad G = \{\sigma_i \mid i \in \text{im } \varphi \leq \mathbb{Z}/n\mathbb{Z}\}$$

$$\text{im } \varphi = \frac{m\mathbb{Z}}{n\mathbb{Z}}, \quad m \mid n$$

$$G = \langle \sigma_m \rangle, \quad \sigma_m(b) = \rho^m b.$$

$$\Omega_G(b) = \{b, \rho^m b, \rho^{2m} b, \dots, \rho^{m(\frac{n}{m}-1)} b\}$$

$$\text{En particular, } m(x) = (x - b)(x - \rho^m b) \dots$$

$$= (x^{\frac{n}{m}} - b^{\frac{n}{m}})$$

$$\text{Luego } b^{\frac{n}{m}} \in K. \quad [K(b):K] = \frac{n}{m}$$

Extensiones de Artin - Schreier

Sea $f(x) = x^p - x \in \mathbb{F}_p(x)$

$$x^p - x = x(x-1)(x-2)\cdots(x-(p-1))$$

Además,

$$\begin{aligned}f(x+y) &= (x+y)^p - (x+y) \\&= x^p + y^p - x - y = f(x) + f(y).\end{aligned}$$

Sean $a, b \in \bar{K}$, $\text{char } \bar{K} = p$

$$f(b) = a$$

$$f(b+1) = f(b) + f(1) = a$$

$$f(b+2) = a$$

$$\vdots$$

$$f(b+p-1) = a$$

$$f(x) - a = \prod_{i=0}^{p-1} (x - b - i)$$

$a \in K$, $b \in \bar{K}$, $K(b)/K$ Galoiana. Sea $G = \text{Gal}(K(b)/K)$

$$\sigma \in G \Rightarrow \sigma(b) = b+i, i \in \mathbb{F}_p.$$

Tenemos la inyección aditiva $\Psi: G \hookrightarrow \mathbb{F}_p$, donde

$$b \in K \Rightarrow \Psi(G) = \{0\}$$

$$b \notin K \Rightarrow \Psi(G) = \mathbb{F}_p$$

$$\therefore G \cong \mathbb{F}_p \cong C_p \text{ (aditivo)}$$

Definición. Un elemento $b \in \bar{K}$ se dice soluble por radicales sobre K si existe una sucesión de anillos

$$K = L_0 \subset L_1 \subset L_2 \subset \dots \subset L_n, b \in L_n$$

donde L_{i+1}/L_i es una extensión ciclotómica, de Kummer, o de Artin - Schreier

$$K(\sqrt{a})/K \quad , \quad K(g_0^{-1}(a))/K$$

\uparrow
 Kummer

\uparrow
 Antin-Schreier

En particular, $L_n = k(c)$, donde

$$c = h_1 \left(\sqrt[n]{h_2} \sqrt[n]{h_3} \cdots \right)$$

Ejemplo. F_1/F_2 , $F_4 = F_2(\alpha)$, $\alpha^2 + \alpha + 1 = 0$

$$\mathbb{F}_{5^5}/\mathbb{F}_5, \quad F_{5^5} = \mathbb{F}_5(\alpha), \quad \alpha^5 - \alpha + 1 = 0$$

$\beta(5) = -1$

$\alpha \notin \mathbb{F}_5$

$$\mathbb{F}_{5^3}/\mathbb{F}_5 \quad , \quad |\mathbb{F}_{5^3}| = 125 \quad , \quad \mathbb{F}_{5^3}^* \cong C_{124} = \langle a \rangle$$

$$\mathbb{F}_5^* \cong C_4 = \langle a^{31} \rangle$$

Pregunta : $\exists b \in F_{5^3}$ con $b^3 \in F_5$? ($b \notin F_5$)

- Demostre que $b \in F_5$...

$\mathbb{F}_7^3 / \mathbb{F}_7$, $2 \in \mathbb{F}_7$ raiz cúbica de 1.

$$\begin{aligned} \mathbb{F}_7^* &\cong C_{3A2} = \langle a \rangle & ; \quad b \in \mathbb{F}_7^*, \quad b \in \mathbb{F}_7^*, \quad ; \quad b = a^{19} \\ \mathbb{F}_7^* &\cong C_b = \langle a^{57} \rangle & b^3 \in \mathbb{F}_7^* \end{aligned}$$

Por lo tanto, $F_7^3 = F_7(\sqrt[3]{a^{57}}) = F_7(3)$

Definición. Sea L/K extensión Galoiana. Un 1-cociclo multiplicativo es una función $\alpha: G = Gal(L/K) \rightarrow L^*$

$$\alpha: G = Gal(L/k) \longrightarrow L^*$$

$$\alpha(\sigma) = \alpha_j$$

Tal que $\alpha_{\sigma\tau} = \alpha_\sigma(\alpha_\tau)$

Un 1-coborde es un 1-ciclo de la forma

$$\alpha_f = \sigma(b)/_b, \text{ con } b \in L^*$$

$$\alpha_{\sigma\tau} = \sigma\tau(b)/_b = \sigma(b)/_b \cdot \sigma\tau(b)/_{\sigma(b)}$$

$$= \alpha_\sigma \cdot \sigma(\alpha_\tau(b)/_b) = \alpha_\sigma \sigma(\alpha_\tau)$$

α, β son 1-ciclos, entonces

$$\gamma = \alpha\beta, \quad \gamma_\sigma = \alpha_\sigma \cdot \beta_\sigma$$

$$(\alpha^{-1})_\sigma = \alpha_\sigma^{-1}$$

Ejercicio. El conjunto de ciclos es un grupo abeliano.

$$\sigma(bc)/_{bc} = \sigma(b)/_b \cdot \sigma(c)/_c$$

Si definimos

$$C_1 = (L/K, L^*) = \left\{ \begin{array}{l} \text{grupo de} \\ \text{ciclos} \end{array} \right\}$$

$$B_1 = (L/K, L^*) = \left\{ \begin{array}{l} \text{grupo de} \\ \text{cobordes} \end{array} \right\}$$

entonces

$$H_1(L/K, L^*) := C_1(L/K, L^*) / B_1(L/K, L^*)$$

grupo de Cohomología Galoiana.

Teorema (90 de Hilbert). $H_1(L/K, L^*) = \{i\}$, para toda extensión Galoiana finita L/K .

- Demostración - Supongamos que L/K es cíclica, con $\text{Gal}(L/K) = \langle \sigma \rangle$

$$\alpha \in L^* \quad ; \quad \alpha_f^2 = \alpha_\sigma \sigma(\alpha_\sigma) = \alpha \sigma(\alpha)$$

$$\alpha_{\sigma^3} = \alpha_{\sigma \circ \sigma^2} = \alpha_{\sigma} \sigma(\alpha_{\sigma^2}) = \alpha \sigma(\alpha \sigma(\alpha)) = \alpha \sigma(\alpha) \sigma^2(\alpha)$$

$$\alpha_{\sigma^t} = \alpha \sigma(\alpha) \sigma^2(\alpha) \dots \sigma^{t-1}(\alpha)$$

$$\begin{array}{c} \alpha_{\sigma^n} = \alpha \dots \overset{n-1}{\sigma}(\alpha) = 1 \\ \parallel \\ \alpha_{id} \end{array}, \quad \alpha_{id} = 1 \quad (\text{demostrar!})$$

definimos la norma de α por $N(\alpha) = \alpha \sigma(\alpha) \dots \sigma^{n-1}(\alpha)$, la cual cumple $N(\alpha\beta) = N(\alpha)N(\beta)$.

Existe un cociente con $\alpha' = \alpha$ si $N(\alpha) = 1$.

T.90 H \Rightarrow Si α tiene norma 1 (caso cíclico), entonces $\alpha' = \alpha = \frac{\sigma(b)}{b}$.

Teorema. Sea L/K una extensión cíclica de grado n , donde K contiene una raíz n -ésima primitiva de 1. Entonces L/K es una extensión de Kummer.

- Demarcación - $N(\eta) = 1$, η raíz primitiva

$$\sigma^i(\eta) = \eta, \quad N(\eta) = \eta \dots \eta \quad (n-\text{veces})$$

T.90 H $\Rightarrow \exists b$ con $\eta = \frac{\sigma(b)}{b}$, de manera equivalente

$$\sigma(b) = \eta b$$

$$\sigma(b) = \eta^n b^n = b^n$$

$$\therefore b^n = a \in K$$

$$\therefore b = \sqrt[n]{a}$$

$$\sigma(b) = \eta b \Rightarrow [K(b):K] = n$$

$$\therefore L = K(b) = K(\sqrt[n]{a}) \quad \square$$

Teorema.

$$H^1(L/K, L) = \{0\}$$



Grado de clases de
cociclos aditivos.

Un 1-cociclo aditivo es una función

$$\alpha: G \rightarrow L$$

$$\alpha(\sigma) = \alpha_\sigma$$

$$\alpha_{\sigma\tau} = \alpha_\sigma + \sigma(\alpha_\tau)$$

y un 1-coborde aditivo es $\alpha'_\sigma = \sigma(b) - b$

Si L/K es cíclica, existe un cociclo aditivo α con $\alpha_0 = a$.

$$\alpha_{\sigma^n} = a + \underbrace{\sigma(a) + \dots + \sigma^{n-1}(a)}_{\text{tr}(a)} = 0$$

$a = \alpha_0$ algún cociclo ssi $\text{tr}(a) = 0$.

Si L/K es cíclica de grado p , $p = \text{char } K$

$$\text{tr}(1) = 0$$

$$\therefore 1 = b - \sigma(b)$$

$$\sigma(b) = b - 1$$

$$\sigma(f(b)) = f(\sigma(b)) = f(b-1) = f(b) - f(1)$$

$$\therefore f(b) \in K, b \notin K$$

$$[K(b) : K] = p, \quad f(b) = a$$

$$\text{Luego } L = K(b) = K(f^{-1}(a))$$

$$\sum_{\tau \in G} \alpha_\tau = \sum_{\tau \in G} \alpha_{\sigma\tau} = \sum_{\tau \in G} \alpha_\tau \sigma(\alpha_\tau) = \alpha_\sigma \sigma\left(\sum_{\tau \in G} \alpha_\tau\right)$$

$$b = \sum_{\tau \in G} \alpha_\tau \Rightarrow b = \alpha_\sigma \sigma(b)$$

$$b^{-1} \text{ amplio } \alpha_\sigma = \sigma(b)b^{-1}, b \in L^* \text{ si } b \neq 0.$$

$$\sum_{\tau \in G} \tau(c) \alpha_\tau = \sum_{\tau \in G} \sigma \tau(c) \alpha_{\sigma\tau} = \sum_{\tau \in G} \sigma(\tau(c)) \alpha_\sigma \sigma(\alpha_\tau) = \alpha_\sigma \sigma\left(\sum_{\tau \in G} \tau(c) \alpha_\tau\right)$$

Lema. Si L/K es una extensión Galoisiana, $G = \text{Gal}(L/K)$, entonces los elementos de G son l.i. sobre L .

$$\sum_{\tau \in G} \alpha_\tau (\tau(c)) = 0 \quad \forall c \Rightarrow \alpha_\tau = 0 \quad (\Leftrightarrow)$$

Si $\sum_{\tau \in G} \alpha_\tau (\tau(c)) \neq 0$, definimos $b^{-1} = \sum_{\tau \in G} \alpha_\tau (\tau(c))$, de donde $b^{-1} = \alpha_\sigma \sigma(b^{-1})$

$\alpha_\sigma = \sigma(b)b^{-1}$ es un cociente.

Proposición. $H^0(L/K, L^*) = \{ \bar{1} \} \quad (\text{T.90.H})$

Proposición. $H^0(L/K, L) = \{ \bar{0} \}$

$$-b = \sum_{\tau \in G} \tau(c) \alpha_\tau = \sum_{\tau \in G} \sigma \tau(c) \alpha_{\sigma\tau} = \sum_{\tau \in G} \sigma(\tau(c)) (\alpha_\sigma + \sigma(\alpha_\tau))$$

$$= \alpha_\sigma \sigma\left(\sum_{\tau \in G} \tau(c)\right) + \sigma\left(\sum_{\tau \in G} \tau(c) \alpha_\tau\right)$$

$$-b = \alpha_\sigma \sigma(t(c)) + \sigma(-b), \text{ si } t(c) = 1$$

$$\alpha_\sigma = \sigma(b) - b$$

$$t_1(c) = \sum_{\gamma \in G} \tau(\gamma c) \quad \left| \begin{array}{l} \exists d \text{ con} \\ a = t_1(d) \neq 0 \\ t_1\left(\frac{a}{d}\right) = 1 \end{array} \right. \quad \left(\begin{array}{l} \text{La traza es } k\text{-lineal e invariante} \\ \text{bajo automorfismos} \end{array} \right)$$

-Demostración del Lema -

$$\text{Pd: } \underbrace{\sum_{\gamma \in G} a_\gamma \tau(c)}_{(*)} = 0 \quad \forall c \Rightarrow a_\gamma = 0$$

Si w_1, \dots, w_n es una k -base de L , entonces $(*)$ es equivalente a

$$\sum_{\gamma \in G} a_\gamma \tau(w_i) = 0 \quad \forall i \quad (*)$$

Basta probar que si $G = \langle \sigma_1, \dots, \sigma_n \rangle$

$$\det \begin{pmatrix} \sigma_1(w_1) & \dots & \sigma_n(w_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(w_n) & \dots & \sigma_n(w_n) \end{pmatrix} \neq 0$$

Pues $(*)$ se re-escribe

$$\sum \vec{a} = 0$$

$$\text{con } \vec{a} = \begin{pmatrix} a_{\sigma_1} \\ \vdots \\ a_{\sigma_n} \end{pmatrix}. \text{ Luego } \vec{a} = 0.$$

Teo. elemento primitivo $\Rightarrow \exists \lambda \in L$ con $L = k(\lambda)$

$$w_i = \lambda^{i-1}$$

$$\Rightarrow \sum \begin{pmatrix} \sigma_1(1) & \sigma_2(1) & \dots & \sigma_n(1) \\ \sigma_1(\lambda) & \sigma_2(\lambda) & \dots & \sigma_n(\lambda) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\lambda)^{n-1} & \sigma_2(\lambda)^{n-1} & \dots & \sigma_n(\lambda)^{n-1} \end{pmatrix}$$

Si $\det \omega = 0$, existe $c_1, \dots, c_n \in L$ con

$$\sum_{i=1}^n c_i \sigma_j(\lambda)^{i-1} = 0 \quad \forall j$$

$\sigma_1(\lambda), \dots, \sigma_n(\lambda)$ son raíces de $f(x) = \sum_{i=1}^n c_i x^{i-1}$ ($\deg f = n-1$)
 \Leftrightarrow .

$$\therefore \det \omega \neq 0.$$

Corolario. Si L/K Galoiana, existe $\lambda \in L$ con $t_k(\lambda) = 1$.

Si definimos $B: L \times L \rightarrow K$, $B(\alpha, \beta) = t_k(\alpha \cdot \beta)$ (forma cuadrática)

B es regular si $\forall \alpha \in L$, $\exists \beta \text{ s.t. } B(\alpha, \beta) \neq 0$

Si $t_k(\lambda) = 1$, $t_k(\alpha \cdot \frac{\lambda}{\alpha}) = 1$. La forma traza es regular.

w_1, \dots, w_n base de L

$$t_k(w_i, w_j) = \sum_{k=1}^n \sigma_k(w_i, w_j) = \sum_{k=1}^n \sigma_k(w_i) \sigma_k(w_j)$$

$$\begin{pmatrix} t_k(w_1, w_2) & \dots & t_k(w_1, w_n) \\ \vdots & \ddots & \vdots \\ t_k(w_n, w_1) & \dots & t_k(w_n, w_n) \end{pmatrix} = \Omega \Omega^t$$

matriz de Gramm

(tiene determinante no nulo).

El determinante de esta matriz de Gramm se conoce como el discriminante de la forma (o de la extensión L/K).

Proposición. Sea $f \in K[x]$, separable, y sea L/K su cuerpo de descomposición. Entonces son equivalentes:

- (1) $\text{Gal}(L/K)$ es soluble.
- (2) $f(x)=0$ es soluble por radicales.

- Demostración - 2) \Rightarrow 1) (Caso I: K contiene suficientes raíces de la unidad)

α raíz de f , $\alpha \in L_n$, donde

$$K = L_0 \subseteq L_1 \subseteq L_2 \subseteq \dots \subseteq L_n$$

$$L_{i+1} = L_i(\sqrt[i]{\alpha}) \quad \text{o} \quad L_{i+1} = L_i(\sqrt[i]{g^i(\alpha)})$$

1) Podemos suponer que L_n contiene a todas las raíces. $L \subseteq L_n$.

2) Podemos suponer que L_n/K es Galoiana.

$$L_n = K[a_1, \dots, a_m], \quad b_i \text{ raíz de } \text{irr}_{K, a_i}(x)$$

(La cadena puede incluir $L'_n = K[b_1, \dots]$ conjugado de L_n por el mismo argumento.)

$$\text{sea } \overline{G} = \text{Gal}(L_n/K),$$

$$H_i = \text{Gal}(L_n/L_i)$$

$$H_n = \{ \text{id} \} \leq H_{n-1} \leq H_{n-2} \leq \dots \leq H_1 \leq H_0 = \overline{G}$$

$$H_i/H_{i+1} \cong \text{Gal}(L_{i+1}/L_i)$$

$$\cong C_{r_i}$$

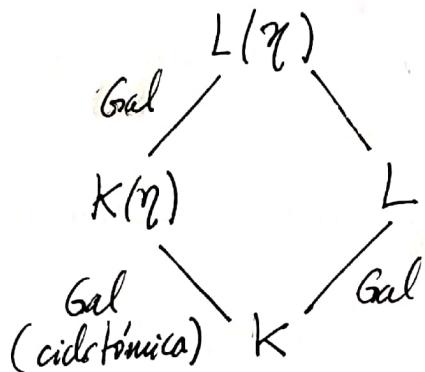
Luego \bar{G} es soluble

$$\text{Gal}(L/k) \cong \bar{G} / \text{Gal}(L_n/L)$$

es soluble.

(fin de caso I)

Caso II : Caso general



$\text{Gal}(L(\eta)/K(\eta))$ soluble (caso anterior)

$\text{Gal}(K(\eta)/K)$ soluble (extensión ciclotómica)

$\Rightarrow \text{Gal}(L/K)$ soluble

$\Rightarrow \text{Gal}(L/k)$ soluble.

Vemos que $f(x)=0$ es soluble por radicales si: $\text{Gal}(L/K)$ es soluble, donde L es el cuerpo de descomposición.

Ejemplo. A_n es simple si $n \geq 5$, A_n y S_n no son solubles.

$L = F(x_1, \dots, x_n)$, S_n actúa en L por permutaciones, $\sigma(x_i) = x_{\sigma(i)}$ i $\sigma(h(x_1, \dots, x_n)) = h(x_{\sigma(1)}, \dots, x_{\sigma(n)})$

L^{S_n} = cuerpo de funciones simétricas

$L^{S_n} = F(\sigma_1, \dots, \sigma_n) =: K$, donde

$$\sigma_1 = x_1 + x_2 + \dots + x_n$$

$$\sigma_2 = x_1 x_2 + x_1 x_3 + \dots + x_{n-1} x_n$$

:

$$\sigma_n = x_1 x_2 \dots x_n$$

$\text{Gal}(L/K) = S_n$, x_1, \dots, x_n son raíces de

$$\prod_{i=1}^n (T - x_i) = T^n + \sum_{i=1}^n \sigma_i (-1)^i T^{n-i} = f(T) \quad (*) \quad , \quad f(T) = 0$$

no es soluble por radicales.

Proposición. Para cada extensión E/F y $a_1, \dots, a_n \in E$ existe $\varphi: F(\sigma_1, \dots, \sigma_n) \rightarrow E$ homomorfismo tal que $\varphi(\sigma_i) = a_i$.

-Demostración-

$$g(T) = T^n + \sum_{i=1}^n a_i (-1)^i T^{n-i} = \prod_{i=1}^n (T - b_i) \text{ en } \overline{E}.$$

Existe $\psi: F[x_1, \dots, x_n] \rightarrow \overline{E}$ con $\psi(x_i) = b_i$.

$$\psi(f(T)) = \prod_{i=1}^n (T - \psi(x_i)) = g(T)$$

Comparando coeficiente a coeficiente se tiene $\varphi(\sigma_i) = \alpha_i$.

$$h(\sigma_1, \dots, \sigma_n) = 0, \quad h \in F[y_1, \dots, y_n] \Rightarrow h = 0.$$

$$E = F(y_1, \dots, y_n), \quad \varphi(\sigma_i) = y_i, \quad \varphi(h(\sigma_1, \dots, \sigma_n)) = h(y_1, \dots, y_n).$$

$$\text{Como } h(\sigma_1, \dots, \sigma_n) = 0 \text{ y } \varphi \text{ es homomorfismo} \Rightarrow h(y_1, \dots, y_n) = 0.$$

Observación. Obtener una fórmula general para resolver $g(T) = 0$ para "casi" (podría haber un denominador que moleste) todo polinomio g de grado 5 es equivalente a resolver $f(T) = 0$ por radicales en (*).

Proposición. La ecuación general de grado 5 no es soluble por radicales.

Ejemplo. Ecación de grado 3. Supongamos $F = \mathbb{C}$

$$\begin{array}{ccc} S_3 & & L \\ | & & |^3 \\ C_3 & & C_3 \\ | & & |^2 \\ \{ \text{id} \} & & L^{S_3} \end{array}$$

Si $C_3 = \langle (123) \rangle$, in $L^{C_3, x_i}(T) = (T - x_1)(T - x_2)(T - x_3)$. $L^{C_3} = L^{S_3}[\alpha]$, α es invariante por permutaciones cíclicas, $\alpha = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1)$

$$\therefore \alpha \notin L^{S_3}$$

$$\text{Si } T = (12) \Rightarrow T(\alpha) = -\alpha, \quad \alpha = \sqrt[3]{\delta}, \quad \delta = \alpha^2$$

$$\delta = (x_1 - x_2)^2(x_2 - x_3)^2(x_3 - x_1)^2, \quad L^{C_3} = K(\sqrt[3]{\delta}).$$

Corolario. Una ecación cubica irreducible $g(T) = 0$ satisface $[L : K] = 3$ ssi el discriminante es un cuadrado.

Ejemplo. $\frac{d(\eta)}{d\ell}$, $\eta = e^{\frac{2\pi i}{7}}$, $\frac{d(\eta+\eta')}{d\ell}$ cúbica.

$$\theta(\eta+\eta') = \{\eta+\eta', \eta^2+\eta'^2, \eta^3+\eta'^3\}$$

$$\begin{aligned}\alpha &= (\eta+\eta'-\eta^2-\eta'^2)(\eta^2+\eta'^2-\eta^3-\eta'^3)(\eta^3+\eta'^3-\eta-\eta') \\ &= (2(\eta+\eta')-(\eta^3+\eta'^3)-2)(\eta^3+\eta'^3-\eta-\eta')\end{aligned}$$

Si $u_i = \eta^i + \eta'^i$, α tiene $u_i u_j = u_{i+j} + u_{i-j}$, $u_j = u_{-j}$, $u_j = u_{j+7}$, $u_j = u_{7-j}$, $u_0 = 2$.

$$\begin{aligned}(2u_1 - u_3 - 2)(u_3 - u_1) &= 2u_1 u_3 - 2u_1^2 - u_3^2 + u_3 u_1 - 2u_3 + 2u_1 \\ &= 2u_3 + 2u_2 - 2u_2 - 4 - u_1 - 2 + u_3 + u_2 - 2u_3 + 2u_1 \\ &= u_3 + u_2 + u_1 - 6 \\ &= -7\end{aligned}$$

$$\therefore \alpha = -7 \Rightarrow \delta = (-7)^2$$

$g(T)=0$ tiene raíces $\alpha_1, \alpha_2, \alpha_3$. $L = k(\alpha) \hookrightarrow \delta \in K^*$

$$x^3 + Ax^2 + Bx + C = 0. \text{ Cambiamos } y = x + \frac{A}{3}, y^3 = x^3 + Ax^2 + 3\left(\frac{A}{3}\right)^2 x + \left(\frac{A}{3}\right)^3$$

$$\therefore \text{queda } y^3 - py - q = 0$$

$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3, y = a+b, p = 3ab, q = a^3 + b^3.$$

luego $ab = p/3$ (si la característica $\neq 3$), $a^3 + b^3 = q$.

$$\Rightarrow a^3 b^3 = p^3/27, a^3 + b^3 = q$$

$$x^2 - qx + \frac{p^3}{27} = 0 = (x-a^3)(x-b^3)$$

$$x = \frac{q \pm \sqrt{q^2 - 4 \frac{p^3}{27}}}{2} = \frac{q}{2} \pm \sqrt{\frac{q^2}{4} - \frac{p^3}{27}}$$

$$\delta = \frac{q^2}{4} - \frac{p^3}{27}$$

$$y_1 = \sqrt[3]{\frac{q}{2} + \sqrt{\delta}} + \sqrt[3]{\frac{q}{2} - \sqrt{\delta}}$$

$$y_2 = \omega \sqrt[3]{\frac{q}{2} + \sqrt{\delta}} + \omega^2 \sqrt[3]{\frac{q}{2} - \sqrt{\delta}}$$

$$y_3 = \omega^2 \sqrt[3]{\frac{q}{2} + \sqrt{\delta}} + \omega \sqrt[3]{\frac{q}{2} - \sqrt{\delta}}$$

$g(T) = 0$ tiene 3 raíces reales ssi $\delta < 0$

Ejemplo. $g(T) = T^3 - a$ tiene raíz $\sqrt[3]{a}$

L : cuerpo de descomposición de $g(T)$

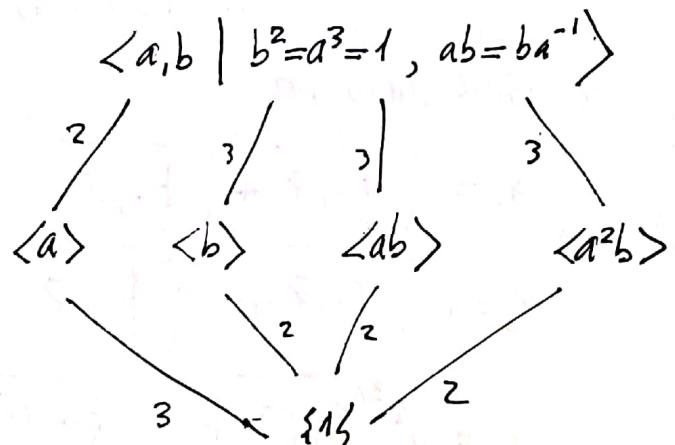
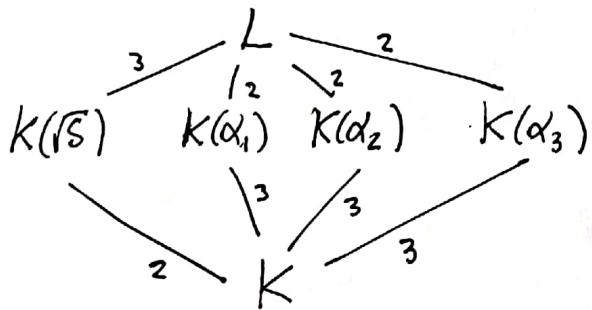


$$K(\sqrt[3]{a}) = K(\omega)$$



$$K$$

Nota. La extensión L/K es Galoiana (tiene grado 3) $\Rightarrow \delta = -3t^2$ es un cuadrado (esto ocurre $\Leftrightarrow -3$ es un cuadrado) \Rightarrow las raíces cúbicas están en K .



$$\text{Gal}(L/K) \cong S_3$$

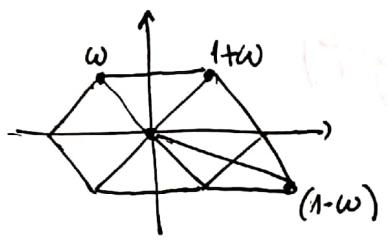
$$\sqrt[3]{\frac{q}{2} + i\alpha} = u, \sqrt[3]{\frac{q}{2} - i\alpha} = v$$

$$\alpha_1 - \alpha_2 = (1-\omega)u + (1-\omega^2)v = (1-\omega)(u + (1+\omega)v) = (1-\omega)(u - \omega^2v)$$

$$\alpha_2 - \alpha_3 = (\omega - \omega^2)u + (\omega^2 - \omega)v = (1-\omega)(\omega u - \omega v) = (1-\omega)\omega(u - v)$$

$$\alpha_3 - \alpha_1 = (\omega^2 - 1)u + (\omega - 1)v = (\omega - 1)((\omega + 1)u + v) = (\omega - 1)(\omega + 1)(u - \omega v)$$

$$(\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1) = (1-\omega)(1-\omega)\omega(\omega-1)(\omega+1)(u^3 - v^3) =$$



$$(1-\omega) = \frac{\sqrt[3]{3}}{2} e^{-\frac{\pi i}{3}}$$

$$(1-\omega)^3 = \frac{3\sqrt{3}}{8} (-i)$$

$$\therefore \sqrt[3]{8} = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1)$$

$$= -\frac{3\sqrt{3}}{4} i\sqrt{\alpha}$$

$$\delta = \frac{9}{16}(-3\alpha)$$

$$\therefore \delta > 0 \Leftrightarrow \alpha < 0$$

α viene dado por

$$\alpha_1 = \sqrt[3]{\frac{q}{2} + i\alpha} + \sqrt[3]{\frac{q}{2} - i\alpha}$$

$$\alpha_2 = \omega \sqrt[3]{\frac{q}{2} + i\alpha} + \omega^2 \sqrt[3]{\frac{q}{2} - i\alpha}$$

$$\alpha_3 = \omega^2 \sqrt[3]{\frac{q}{2} + i\alpha} + \omega \sqrt[3]{\frac{q}{2} - i\alpha}$$

Proposición. Existen ecuaciones de grado 5 sobre \mathbb{Q} que no son solubles por radicales.

Lema. S_5 está generado por una transposición y un 5-ciclo.

$$\begin{matrix} (12345) \\ (12) \end{matrix}$$

$$(12)(12345) = (2345) = \sigma$$

$$\sigma(12)\sigma^{-1} = (13)$$

$$\sigma^2(12)\sigma^{-2} = (14)$$

$$\sigma^3(12)\sigma^{-3} = (15)$$

$$(12)(13)(12) = (23)$$

$$(13)(14)(13) = (34)$$

$$(14)(15)(14) = (45)$$

$$(23)(34)(45)(52)(23) = (12345)$$

$$(12345)^2 = (13524)$$

$$(13)$$

$$(12345) = (34512)$$

$$(34)$$

□

□

Observación. Si $f(x)$ es un polinomio irreducible de grado 5, las raíces son $\alpha_1, \dots, \alpha_5$ y $G = \text{Gal}(\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)/\mathbb{Q})$ actúa transitivamente en las raíces.

$$|\sigma(\alpha_1)| = \frac{|G|}{|\text{stab}_G(\alpha_1)|} = 5$$

$5 \mid G \Rightarrow G$ tiene elemento de orden 5 (5-ciclo).

$\tau = \text{conjugación compleja}$, tiene orden 2, es una transposición si f tiene exactamente 3 raíces reales.

$$g(x) = x(x-1)(x-2)(x-5) = x^4 - 8x^3 + 17x^2 - 10x$$

$$f(x) = 3x^5 - 30x^4 + 85x^3 - 75x^2 + c$$

$$\begin{matrix} f' \\ \downarrow \\ g \end{matrix}, \quad g=0 \Leftrightarrow x=0, 1, 2, 5$$

$$f(x) = x^2(3x^3 - 30x^2 + 85x - 75)$$

$$f(0) = c$$

$$f(1) = c - 27$$

$$f(2) = 96 - 480 + 680 - 300 + c = c + 4$$

$$f(5) = c - 625$$

Poniendo $c = 30$: $f(x) = 3x^5 - 30x^4 + 85x^3 - 75x^2 + 30$

$$f(x) = 3x^5 - 30x^4 + 85x^3 - 75x^2 + 30, \text{ irreducible por Eisenstein!}$$

Extensiones trascendentales

L/K extensión, $\alpha \in L$. α trascendente

$$K[\alpha] \cong K[x]$$

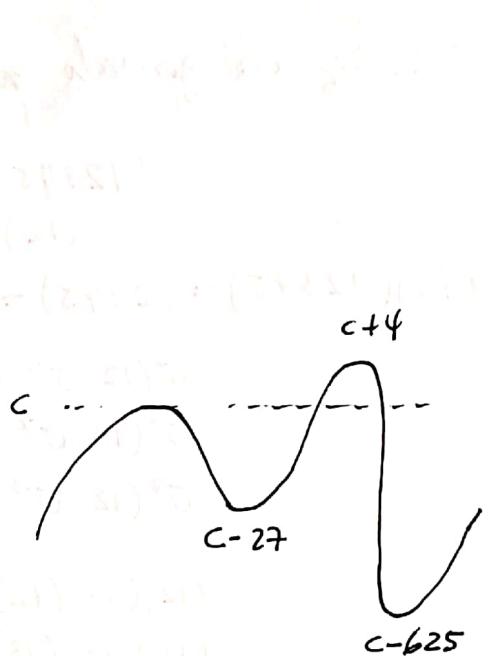
$$K(\alpha) \cong K(x)$$

Definición: $\{x_1, \dots, x_n\} \subseteq L$ se dice que genera algebraicamente L/K si $L/K(x_1, \dots, x_n)$ es algebraica.

$\{x_1, \dots, x_n\} \subseteq L$ se dice algebraicamente independiente si la evaluación

$$\varphi: K[x_1, \dots, x_n] \rightarrow K[x_1, \dots, x_n]$$

$$\varphi(x_i) = x_i$$



es inyectiva. Un conjunto $\{x_1, \dots, x_n\} \subseteq L$ se dice base de trascendencia si genera y es algebraicamente independiente.

Miscelánea

$$[1] L = F_p(x_1^{1/p}, x_2), K = F_p(\sigma_1, \sigma_2)$$

(a) L_{sep}/K Galoisiana pero L/K no es normal.

(b) L/K no tiene subextensión t.i. ni triviales pero L/K no es separable

-Demostración-

$$\text{irr}_{K, x_1^{1/p}}(T) = T^{2p} - \sigma_1 T^p + \sigma_2 = (T - x_1^{1/p})^p (T - x_2^{1/p})^p$$

$$\left. \begin{array}{c} K(x_1^{1/p}) \\ p \mid \rightarrow \text{t.i.} \\ K(x_1) \\ 2 \mid \\ K \end{array} \right\} \quad \left. \begin{array}{c} x_2^{1/p} \notin L \\ ((T - x_1)(T - x_2)) = T^2 - \sigma_1 T + \sigma_2 \end{array} \right\}$$

$$x_2^{1/p} \notin L \quad | \quad k(x_1, x_2) = k(x_1) = F$$

$$x_2^{1/p} \notin F(x_1^{1/p}), \quad x_1 \in F$$

$$F(x_1^{1/p}, x_2^{1/p}) \neq F(x_1^{1/p})$$

$$[F(x_1^{1/p}, x_2^{1/p}) : F] = p^2$$

$$\text{Base } B = \{x_1^{i/p} x_2^{j/p} / 0 \leq i, j \leq p-1\}$$

B l.i. sobre $\mathbb{F}_p[x_1, x_2]$

$$\sum_{i=0}^{p-1} \sum_{j=0}^{p-1} x_1^{\frac{i}{p}} x_2^{\frac{j}{p}} f_{i,j}(x_1, x_2) = \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} x_1^{\frac{i}{p}} x_2^{\frac{j}{p}} \sum_{\ell=0}^N \sum_{m=0}^M x_1^\ell x_2^m \alpha_{\ell m i j}$$

$$= \sum_{i, j, \ell, m} \alpha_{\ell m i j} x_1^{\frac{p\ell+i}{p}} x_2^{\frac{pm+j}{p}}$$

Como $\{x_1^{\frac{i}{p}}, x_2^{\frac{j}{p}}\}$ a.i., se tiene que $\alpha_{\ell m i j} = 0$.

① Dominio, B l.i. sobre D

$\Rightarrow B$ l.i. sobre $\text{Quot}(D)$

$$\sum \alpha_i \beta_i = 0, \alpha_i \in \text{Quot}(D)$$

$$\Rightarrow \sum \lambda_i b_i = 0, \lambda_i \in D$$

$\therefore B$ base

$$\therefore x_2^{\frac{i}{p}} \notin F(x_1^{\frac{i}{p}})$$

¿Qué es L_{sep} ?

$k(h)/k$ t.i., $h \in L \Rightarrow h = h(x_1^{\frac{i}{p}}, x_2)$

$h^p \in K$ (acuerdo de funciones simétricas)

$$h(x_1^{p^{r-1}}, x_2^{p^r}) = h(x_2^{p^{r-1}}, x_1^{p^r})$$

$$\therefore h(x_1^{p^{r-1}}, x_2^{p^r}) = g(x_1^{p^r}, x_2^{p^r})$$

$$h(x_1^{\frac{i}{p}}, x_2) = g(x_1, x_2) \in F$$

Como F/k Galoisiana, luego es separable, $g \in F$, $K(g)/K$ t.i. $\rightarrow K(g) = K$.

Afirmación: $L_{\text{sep}} = F$

F/K separable. Luego $L_{\text{sep}} \supseteq F$.

$h = h(x_1, x_2) \in L_{\text{sep}} \Rightarrow K(h)/K$ separable.

$\Rightarrow \text{irr}_{K,h}(T)$ tiene raíces distintas

$\Rightarrow \text{irr}_{F,h}(T)$ tiene raíces distintas

$\Rightarrow F(h)/F$ separable

L/F t.i. $\Rightarrow F(h)/F$ t.i.

$$\therefore F(h) = F$$

$\therefore h \in F$, luego $L_{\text{sep}} = F$

[2] Sean $a = e + \pi$, $b = e\pi$. a, b no pueden ser algebraicos simultáneamente.

-Demostración -

Sea $F = \mathbb{Q}(a, b)$, $\text{irr}_{F,e}(T) \mid (x-e)(x-\pi) \in F[T]$

$$\begin{array}{c} \mathbb{Q}(e, \pi) \\ | \qquad \qquad \qquad \text{algebraica} \\ \mathbb{Q}(e\pi, e+\pi) \\ | \qquad \qquad \qquad \text{algebraica} \\ \mathbb{Q} \end{array} \left. \begin{array}{l} \text{algebraica} \\ \text{algebraica} \end{array} \right\} \Rightarrow e, \pi \text{ algebraicos sobre } \mathbb{Q} (\Leftrightarrow).$$

$$[3] \quad L = \mathbb{F}_p(x), \quad K = \mathbb{F}_p(f)$$

L_{sep}/K galoisiana $\Rightarrow L/K$ normal.

Tenemos que $f(x) = g(x^{p^r})$, g maximal

$$x^{p^2} + x^{p^3} + 3x^{p^4} = f(x)$$

$$x + x^{p^r} + 3x^{p^{2r}} = g(x) \Rightarrow g' \neq 0.$$

$$\text{im}_{K,x}(T) = f(T) - f(x)$$

$$\begin{aligned} f(T) - f(x) &= g(T^{p^r}) - g(x^{p^r}) \\ &= (g(T) - g(x))^{p^r} \end{aligned}$$

Como $g'(T) \neq 0$, $g(T) - g(x)$ tiene raíces distintas

Afirmación: $L_{\text{sep}} = K(x^{p^r}) := F$

$$\text{Teniendo } H(T) = \text{im}_{K,x^{p^r}}(T) = g(T) - g(x^{p^r})$$

$g'(T) \neq 0$ tiene raíces distintas

ahora si $u = x^{p^r}$

$$H(T) = g(T) - g(u) \in \mathbb{F}_p(u)[T] \quad (\text{irreducible})$$

$$\therefore F \subseteq L_{\text{sep}}$$

$$\text{Como } L = F(x)/F \text{ t.i. } \Rightarrow L_{\text{sep}} = F.$$

Si $h = h(x) \in L = \mathbb{F}_p(x)$

$$h(x)^{p^r} = h(x^{p^r}) \in F = L_{\text{sep.}}$$

Definimos $G(T) = \text{irr}_{K, h}(T)$

h_1 raiz de $G(T)$. Por demostrar que $h_1 \in L$.

$$G(T) = F(T^{p^s}), F \neq 0.$$

$$F(T) = \text{irr}_{K, h^{p^s}}(T)$$

$$\begin{array}{c} K(h) \\ | \\ p^s \\ | \\ K(h^{p^s}) \quad \deg G = p^s \deg F \\ | \\ \deg F \\ | \\ K \end{array}$$

$$h^{p^s} \in F = K(x^{p^r}) \quad h_1^{p^s} \text{ raiz de } F(T) \\ (s \leq r) \quad \therefore h_1^{p^s} \in K(x^{p^r}).$$

$$h = h(x), \quad h^{p^s} = h(x^{p^s}) \in \mathbb{F}_p(x^{p^r})$$

$$h(x) = g(x^{p^t}), t \text{ maximal.}$$

$$h(x^{p^s}) = g(x^{p^{t+s}}) \in \mathbb{F}_p(x^{p^r}), t+s \geq r.$$

$$h_1^{p^s} \in \mathbb{F}_p(x^{p^r})$$

$$h_1^{p^s} = j(x^{p^r}) \quad (s \leq r)$$

$$h_1 = \sqrt[p^s]{j(x^{p^r})} = j(x^{p^{r-s}}) \quad \therefore h_1 \in \mathbb{F}_p(x) = L$$