MATEMÁTICAS

Universidad Nacional Autónoma de México
Facultad de Ciencias

Algebra Moderna II

4ta lista de ejercicios

Por: Lorenzo Antonio Alvarado Cabrera

Problema 1. –

Sea E un campo y $f(x) = \sum_{i=0}^{n} a_i x^i \in E[x]$, definimos la derivada formal de $Df(x) = \sum_{i=0}^{n} i a_i x^{i-1}$.

1. Sea E un campo y $f(x), g(x) \in E[x]$. Demuestra que

   a)
   $$D(fg) = (Df)g + f(Dg).$$

   b)
   $$D(f+g) = Df + Dg.$$

   Supongamos ahora que E es de característica 0 y F/E es el campo de descomposición de $f(x)$.

   c) Si $\alpha \in F$ es una raíz múltiple de $f(x)$ entonces $min(\alpha, E) \mid f(x)$ y $min(\alpha, E) \mid D(f)(x)$ ambas divisibilidades en $E[x]$.

   d) $f(x)$ es separable si, y solo si, $(f, D(f)) = 1$ en $E[x]$.

   e) Si $f(x)$ es irreducible en $E[x]$, entonces $f(x)$ es separable.

   f) $f(x)$ es separable si, y solo si, la factorización de $f(x)$ en irreducibles (en $E[x]$) no tiene polinomios repetidos.

Demostración: Notemos que si $(f)_{(k)} = a_k \ \Rightarrow \ (Df)_{(k)} = ka_k$

(a) Tenemos que demostrar que $D(fg)_{(k)} = [(Df)g + f(Dg)]_{(k)}$. Tomemos $f(x) = \sum_{i=0}^{n} a_i x^i$ y $g(x) = \sum_{i=0}^{n} b_i x^i$, entonces, por un lado

$$(fg)_{(k)} = \sum_{i=0}^{k} a_i b_{k-i} \ \Rightarrow \ D(fg)_{(k)} = k\sum_{i=0}^{k} a_i b_{k-i}$$

y por otro lado

$$[(Df)g + f(Dg)]_{(k)} = [(Df)g]_{(k)} + [f(Dg)]_{(k)} = \sum_{i=0}^{k} (ia_i)b_{k-i} + \sum_{i=0}^{k} a_i([k-i]b_{k-i})$$
$$= \sum_{i=0}^{k} ia_i b_{k-i} + \sum_{i=0}^{k} ka_i b_{k-i} - ia_i b_{k-i} = \sum_{i=0}^{k} ia_i b_{k-i} + k\sum_{i=0}^{k} a_i b_{k-i} - \sum_{i=0}^{k} ia_i b_{k-i} = k\sum_{i=0}^{k} a_i b_{k-i}$$

por lo tanto $D(fg)_{(k)} = [(Df)g + f(Dg)]_{(k)}$, con lo que los polinomios coinciden coeficiente por coeficiente, por lo tanto $D(fg) = (Df)g + f(Dg)$.

■

(b) De forma sencilla

$$(f+g)(x) = \sum_{i=0}^{n} [a_i + b_i]x^i \Rightarrow D(f+g)(x) = \sum_{i=0}^{n} i[a_i + b_i]x^{i-1} = \sum_{i=0}^{n} ia_i x^{i-1} + \sum_{i=0}^{n} ib_i x^{i-1} = Df(x) + Dg(x)$$

■

(c) Sea $p(x) = \min(\alpha, E)$, por el teorema 3.2.9 tenemos que $p(x) \mid f(x)$. Ahora como por hipótesis α es raíz múltiple de $f(x)$ entonces $f(x) = q(x)(x-\alpha)^2$ para algún $q(x) \in E[x]$ entonces por el inciso (a)

$$Df(x) = [Dq(x)](x-a)^2 + [D(x-a)^m]q(x)$$

y tenemos que $D(x-a)^2 = D(x^2 - 2ax + a^2) = 2x - 2a = 2(x-a)$, entonces

$$Df(x) = [Dq(x)](x-a)^2 + 2(x-a)q(x)$$

, por lo que, $Df(\alpha) = 0$ (pues $m-1 > 0$) entonces nuevamente por el teorema 3.2.9 $p(x) \mid Df(x)$.

■

(d) Por contrapuesta.

$\Rightarrow]$ Supongamos que $f(x)$ no es separable, entonces tiene una raíz α no sencilla, por lo que, por el inciso anterior $\min(\alpha, E) \mid f(x)$ y $\min(\alpha, E) \mid Df(x)$, entonces $(f(x), Df(x)) \neq 1$.

$\Leftarrow]$ Supongamos que existe $1 \neq p(x) \in E[x]$ tal que $(f(x), Df(x)) = p(x)$ y sea $\alpha \in F$ raíz de $p(x)$, entonces como $p(x) \mid f(x)$ y $p(x) \mid Df(x)$ tendremos que α es raíz de f y Df, entonces existe $h(x) \in E[x]$ tal que $f(x) = h(x)(x-\alpha)$ por lo que $Df(x) = Dh(x)(x-\alpha) + h(x) \Rightarrow 0 = Df(\alpha)$ $= Dh(\alpha)(\alpha - \alpha) + h(\alpha) \Rightarrow h(\alpha) = 0$, por lo que nuevamente existe $H(x) \in E[x]$ tal que $h(x) =$ $H(x)(x-\alpha) \Rightarrow f(x) = H(x)(x-\alpha)^2$ por lo que $f(x)$ tiene una raíz múltiple, entonces, no es separable.

■

(e) Sea $f(x) \in E[x]$ irreducible con $\text{grad}(f(x)) = n$ entonces sabemos que $Df(x) \in E[x]$ y tal que $\text{grad}(Df(x)) = n-1$, veamos que $(f(x), Df(x)) = 1$. Sea $p(x) = (f(x), Df(x)) \Rightarrow p(x) \mid f(x) \Rightarrow$ $f(x) = q(x)p(x)$ pero $f(x)$ es irreducible, entonces $q(x) = q \in E$ o $p(x) = p \in E$.
Si $q(x) = q$ entonces $f(x) = qp(x) \Rightarrow p(x) = q^{-1}f(x)$ por lo que $p(x) \mid Df(x) \Rightarrow q^{-1}f(x) \mid Df(x)$ pero esto no es posible, pues $\text{grad}(q^{-1}f(x)) = n$ y $\text{grad}(Df(x)) = n-1$, entonces necesariamente $p(x) = p$, por lo que $(f(x), Df(x)) = p$ por lo que salvo constantes $(f(x), Df(x)) = 1$, entonces por el inciso anterior tendremos que $f(x)$ es separable.

■

(f) Si $f(x)$ es separable entonces $f(x) = \prod x - \alpha_i$ siendo polinomios irreducibles y distintos.
Por otro lado supongamos que $f(x) = \prod p_i(x)$ con $p_i(x) \in E[x]$ irreducibles y distintos, entonces tendremos que no puede haber raíces repetidas. Supongamos que existe $\alpha \in F$ tal que $p_i(\alpha) = p_j(\alpha)$ para algunas i, j, entonces tendremos que existen $q_i(x), q_j(x) \in E[x]$ tal que

$p_i(x) = q_i(x)(x-\alpha)$ y $p_j(x) = q_j(x)(x-\alpha)$, pero son irreducibles y $x-\alpha$ no es unidad, entonces $q_j(x) = q_j \in E[x]$ y $q_i(x) = q_i \in E[x]$, por lo que $p_i(x) = p_i(x-\alpha)$ y $p_j(x) = p_j(x-\alpha)$ y simplemente reordenando las constantes tendremos en esencia que $p_i(x) = p_j(x)$!!! lo cual contradice la hipótesis, por lo que los p_i´s no tienen raíces repetidas.

Para terminar, como cada p_i es irreducible tendremos por el inciso anterior que es separable y además como no hay raíces repetidas entre todos ellos concluimos que $f(x)$ es un producto de factores lineales distintos por lo que es separable.

■

Problema 2. –

Considera $K = \mathbb{Q}(\sqrt{2}, \sqrt{5})$ y la extensión $K/\mathbb{Q}$.

a) Encuentra $G = \mathrm{Gal}(K/\mathbb{Q})$.

b) Encuentra $\mathrm{Sub}(G)$.

c) Encuentra $\mathrm{Ret}(K/\mathbb{Q})$.

d) Realiza un esquema de las retículas $\mathrm{Sub}(G)$ y $\mathrm{Ret}(K/\mathbb{Q})$. ¿Podías ahorrarte alguno de estos pasos?

Demostración:

(*a*) Notemos que $K = \mathbb{Q}(\sqrt{2}, \sqrt{5})$ es el campo de descomposición de $f(x) = (x^2-2)(x^2-5)$ (pues las 4 raices están ahi). Sabemos que $[K:\mathbb{Q}] = 4$ ya que el $\mathrm{grad}(f(x)) = 4$. Además como $K = \{a + b\sqrt{2} + c\sqrt{5} + d\sqrt{5}\sqrt{2} : a,b,c,d \in \mathbb{Q}\}$ tendremos que $\beta = \{1, \sqrt{2}, \sqrt{3}, \sqrt{10}\}$ es una $\mathbb{Q}-$base de K.

Por otro lado sabemos que los $\mathbb{Q}-$automorfismos están determinados por la acción en las raíces: $\sqrt{2}, -\sqrt{2}, \sqrt{5}, -\sqrt{5}$ del polinomio $f(x)$. Por ello tenemos que los $\mathbb{Q}-$automorfismos son: I, σ, τ y $\sigma\tau$ donde

$$\sigma := \begin{cases} \sqrt{2} \to -\sqrt{2} \\ \sqrt{5} \to \sqrt{5} \end{cases}, \quad \tau := \begin{cases} \sqrt{2} \to \sqrt{2} \\ \sqrt{5} \to -\sqrt{5} \end{cases}$$

(esto pues por el corolario 4.1.3 los automorfismos permutan las raíces) es decir, $\mathrm{Gal}(K, \mathbb{Q}) = \{I, \sigma, \tau \text{ y } \sigma\tau\}$. Mas explícitamente (lo necesitaremos adelante) se tiene

$$\begin{aligned}
I(a + b\sqrt{2} + c\sqrt{5} + d\sqrt{10}) &= a + b\sqrt{2} + c\sqrt{5} + d\sqrt{10} \\
\sigma(a + b\sqrt{2} + c\sqrt{5} + d\sqrt{10}) &= a - b\sqrt{2} + c\sqrt{5} - d\sqrt{10} \\
\tau(a + b\sqrt{2} + c\sqrt{5} + d\sqrt{10}) &= a + b\sqrt{2} - c\sqrt{5} - d\sqrt{10} \\
\sigma\tau(a + b\sqrt{2} + c\sqrt{5} + d\sqrt{10}) &= a - b\sqrt{2} - c\sqrt{5} + d\sqrt{10}
\end{aligned}$$

■

(*b*) Con esto tenemos los subgrupos de G son $G_1 = \{I\}, G_2 = \{I, \sigma\}, G_3 = \{I, \tau\}, G_4 = \{I, \sigma\tau\}$ y $G_5 = G$, es decir, $\mathrm{Sub}(G) = \{G_1, G_2, G_3, G_4, G_5\}$.

■

(*c*) Ahora, sabemos que los campos intermedios son los campos fijos de cada subgrupo de G, entonces

- $K^{G_1} = \{k \in K : I(k) = k\} = K = \mathbb{Q}(\sqrt{2}, \sqrt{5})$

- $$\begin{aligned} K^{G_2} &= \{k \in K : \sigma(k) = k\} \\ &= \{k \in K : a - b\sqrt{2} + c\sqrt{5} - d\sqrt{10} = a + b\sqrt{2} + c\sqrt{5} + d\sqrt{10}\} \\ &= \{k \in K : -b\sqrt{2} - d\sqrt{10} = b\sqrt{2} + d\sqrt{10}\} \quad (\Rightarrow \ b = d = 0) \\ &= \{a + c\sqrt{5} : a, c \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{5}) \end{aligned}$$

- $$\begin{aligned} K^{G_3} &= \{k \in K : \tau(k) = k\} \\ &= \{k \in K : a + b\sqrt{2} - c\sqrt{5} - d\sqrt{10} = a + b\sqrt{2} + c\sqrt{5} + d\sqrt{10}\} \\ &= \{k \in K : -c\sqrt{5} - d\sqrt{10} = c\sqrt{5} + d\sqrt{10}\} \quad (\Rightarrow \ c = d = 0) \\ &= \{a + b\sqrt{2} : a, b \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{2}) \end{aligned}$$

- $$\begin{aligned} K^{G_4} &= \{k \in K : \sigma\tau(k) = k\} \\ &= \{k \in K : a - b\sqrt{2} - c\sqrt{5} + d\sqrt{10} = a + b\sqrt{2} + c\sqrt{5} + d\sqrt{10}\} \\ &= \{k \in K : -b\sqrt{2} - c\sqrt{5} = b\sqrt{2} + c\sqrt{5}\} \quad (\Rightarrow \ b = c = 0) \\ &= \{a + d\sqrt{10} : a, d \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{10}) \end{aligned}$$

- $K^{G_5} = \{k \in K : (I, \sigma\tau, \sigma, \tau)(k) = k\} = K^{G_1} \cap K^{G_2} \cap K^{G_3} \cap K^{G_4} = \{a : a \in \mathbb{Q}\} = \mathbb{Q}$

Por tanto $\mathrm{Ret}(K/\mathbb{Q}) = \{\mathbb{Q},\ \mathbb{Q}(\sqrt{2}),\ \mathbb{Q}(\sqrt{5}), \mathbb{Q}(\sqrt{10}),\ \mathbb{Q}(\sqrt{2}, \sqrt{5})\}$.

∎

(*d*) Tendremos

Subgrupos de $\mathrm{Gal}(K/\mathbb{Q})$

$$\begin{tikzcd}
& \{I\} & \\
\{I,\tau\} \arrow[ur] & \{I,\sigma\tau\} \arrow[u] & \{I,\sigma\} \arrow[ul] \\
& \{I,\sigma,\tau,\sigma\tau\} \arrow[ul] \arrow[u] \arrow[ur] &
\end{tikzcd}$$

Subcampos intermedios

$$\begin{tikzcd}
& \mathbb{Q}(\sqrt{2},\sqrt{5}) & \\
\mathbb{Q}(\sqrt{2}) \arrow[ur] & \mathbb{Q}(\sqrt{10}) \arrow[u] & \mathbb{Q}(\sqrt{5}) \arrow[ul] \\
& \mathbb{Q} \arrow[ul] \arrow[u] \arrow[ur] &
\end{tikzcd}$$

∎

Problema 3. –

Considera $\alpha = e^{2\pi/3}$, $K = \mathbb{Q}(\alpha)$ y la extensión $K/\mathbb{Q}$.

a) Encuentra $G = \mathrm{Gal}(K/\mathbb{Q})$.

b) Encuentra $\mathrm{Sub}(G)$.

c) Encuentra $\mathrm{Ret}(K/\mathbb{Q})$.

d) Realiza un esquema de las retículas $\mathrm{Sub}(G)$ y $\mathrm{Ret}(K/\mathbb{Q})$. ¿Podías ahorrarte alguno de estos pasos?

Demostración:

(*a*) Notemos que $K = \mathbb{Q}(e^{(2\pi/3)i})$ es el campo de descomposición de $f(x) = x^2 + x + 1$ (pues tiene como raíces $e^{(2\pi/3)i}$ y $[e^{(2\pi/3)i}]^2 = e^{(4\pi/3)i}$ que están en K). Sabemos que $[K:\mathbb{Q}] = 2$ ya que el $\mathrm{grad}(f(x)) = 2$. Además como $K = \left\{a + be^{(2\pi/3)i} : a, b \in \mathbb{Q}\right\}$ tendremos que $\beta = \left\{1, e^{(2\pi/3)i}\right\}$ es una $\mathbb{Q}-$base de K.
Por otro lado, sabemos que los $\mathbb{Q}-$automorfismos están determinados por la acción en las raíces: $e^{(2\pi/3)i}$ y $e^{(4\pi/3)i}$ del polinomio $f(x)$. Por ello tenemos que los $\mathbb{Q}-$automorfismos son: I y σ donde

$$I := id_K \ \text{ y } \ \sigma := \left\{e^{(2\pi/3)i} \to e^{(4\pi/3)i}\right.$$

(esto pues por el corolario 4.1.3 los automorfismos permutan las raíces) es decir, $\mathrm{Gal}(K, \mathbb{Q}) = \{I, \sigma\}$. Mas explícitamente (lo necesitaremos adelante) se tiene

$$I(a + be^{(2\pi/3)i}) = a + be^{(2\pi/3)i}$$
$$\sigma(a + b\sqrt{2}) = a + be^{(4\pi/3)i}$$

■

(*b*) Con esto tenemos los subgrupos de G son $G_1 = \{I\}, G_2 = \{\sigma\}, G_3 = G$, es decir, $\mathrm{Sub}(G) = \left\{G_1, G_2, G_3\right\}$.

■

(*c*) Ahora, sabemos que los campos intermedios son los campos fijos de cada subgrupo de G, entonces

- $K^{G_1} = \left\{k \in K : I(k) = k\right\} = K = \mathbb{Q}(e^{(2\pi/3)i})$

- $K^{G_2} = \left\{k \in K : \sigma(k) = k\right\}$
$= \left\{k \in K : a + be^{(4\pi/3)i} = a + be^{(2\pi/3)i}\right\}$
$= \left\{k \in K : be^{(4\pi/3)i} = be^{(2\pi/3)i}\right\}$ $(\Rightarrow \ b = 0)$
$= \left\{a : a \in \mathbb{Q}\right\} = \mathbb{Q}$

- $K^{G_5} = \left\{k \in K : (I, \sigma)(k) = k\right\} = K^{G_1} \cap K^{G_2} = \mathbb{Q}$

Por tanto $\mathrm{Ret}(K/\mathbb{Q}) = \left\{\mathbb{Q}, \ \mathbb{Q}(e^{(2\pi/3)i})\right\}$.

■

(d) Tendremos

Subgrupos de $\text{Gal}(K/\mathbb{Q})$ Subcampos intermedios

$$\begin{tikzcd} \{I\} & \mathbb{Q}(e^{(2\pi/3)i}) \\ \{I,\sigma\tau\} \arrow[u] & \mathbb{Q} \arrow[u] \end{tikzcd}$$

■

Problema 4. –

Considera K el campo de descomposición de $f(x) = x^4 - 3x^2 + 4$ sobre $\mathbb{Q}$ y la extensión $K/\mathbb{Q}$.

- $a)$ Encuentra las raíces de $p(x)$.
- $b)$ Encuentra $G = \text{Gal}(K/\mathbb{Q})$.
- $c)$ Encuentra $\text{Sub}(G)$.
- $d)$ Encuentra $\text{Ret}(K/\mathbb{Q})$.
- $e)$ Realiza un esquema de las retículas $\text{Sub}(G)$ y $\text{Ret}(K/\mathbb{Q})$. ¿Podías ahorrarte alguno de estos pasos?

Demostración:

(a) Sea $y = x^2$ entonces $y^2 - 3y + 4 = 0 \Rightarrow y = \frac{3\pm\sqrt{9-4(1)(4)}}{2} = \frac{3\pm i\sqrt{7}}{2}$, por lo que $x^2 = \frac{3\pm i\sqrt{7}}{2}$ entonces ${x_1}^2 = \frac{3+i\sqrt{7}}{2}$ o ${x_2}^2 = \frac{3-i\sqrt{7}}{2}$. Y usando sabemos un numero complejo $a+bi$ tiene exactamente dos raíces dadas por (*Curso básico de variable compleja, Antonio Lascurain Orive, pag. 11, proposición 1.1.3*)

$$\pm\left(\sqrt{\frac{a+\sqrt{a^2+b^2}}{2}} + i\sqrt{\frac{-a+\sqrt{a^2+b^2}}{2}}\right) \text{ si } b>0 \text{ ó } \pm\left(-\sqrt{\frac{a+\sqrt{a^2+b^2}}{2}} + i\sqrt{\frac{-a+\sqrt{a^2+b^2}}{2}}\right) \text{ si } b<0$$

por lo que

$$x_1 = \pm\left(\sqrt{\frac{\frac{3}{2}+\sqrt{\frac{9}{4}+\frac{7}{4}}}{2}} + i\sqrt{\frac{-\frac{3}{2}+\sqrt{\frac{9}{4}+\frac{7}{4}}}{2}}\right) = \pm\left(\sqrt{\frac{\frac{3}{2}+2}{2}} + i\sqrt{\frac{-\frac{3}{2}+2}{2}}\right) = \pm\left(\sqrt{\frac{7}{4}} + i\sqrt{\frac{1}{4}}\right) = \pm\left(\frac{\sqrt{7}}{2} + \frac{1}{2}i\right)$$

ó

$$x_2 = \pm\left(-\sqrt{\frac{\frac{3}{2}+\sqrt{\frac{9}{4}+\frac{7}{4}}}{2}} + i\sqrt{\frac{-\frac{3}{2}+\sqrt{\frac{9}{4}+\frac{7}{4}}}{2}}\right) = \pm\left(-\frac{\sqrt{7}}{2} + \frac{1}{2}i\right)$$

por lo tanto, las raíces de $x^4 - 3x^2 + 4$ son: $x_1 = \frac{\sqrt{7}}{2} + \frac{1}{2}i$, $x_2 = -\frac{\sqrt{7}}{2} - \frac{1}{2}i$, $x_3 = -\frac{\sqrt{7}}{2} + \frac{1}{2}i$ y $x_4 = \frac{\sqrt{7}}{2} - \frac{1}{2}i$. Con esto $f(x) = (x-x_1)(x-x_2)(x-x_3)(x-x_4)$.

(b) Ahora, con lo anterior notemos que todas las raíces son combinaciones lineales de $\{\sqrt{7}, i\}$ lo cual es claro, y si K es el campo de descomposición de $f(x)$ entonces $x_1 + x_2 = i \in K$ y $x_1 + x_4 = \sqrt{7} \in K$, por lo que tendremos que $K = \mathbb{Q}(i, \sqrt{7})$ y como el polinomio minimo de i e $\sqrt{7}$ es $p(x) = (x^2+1)(x^2-7)$ entonces $[K:\mathbb{Q}] = 4$ ya que el $\text{grad}(f(x)) = 4$. Además como $K = \{a + bi + c\sqrt{7} + d\sqrt{7}i : a,b,c,d \in \mathbb{Q}\}$ tendremos que $\beta = \{1, i, \sqrt{7}, \sqrt{7}i\}$ es una $\mathbb{Q}-$base de K.
Por otro lado sabemos que los $\mathbb{Q}-$automorfismos están determinados por la acción en las raíces: $\pm i$ y $\pm\sqrt{7}$ del polinomio $p(x)$. Por ello tenemos que los $\mathbb{Q}-$automorfismos son: I, σ, τ y $\sigma\tau$ donde

$$\sigma := \begin{cases} i \to -i \\ \sqrt{7} \to \sqrt{7} \end{cases}, \quad \tau := \begin{cases} i \to i \\ \sqrt{7} \to -\sqrt{7} \end{cases}$$

(esto pues por el corolario 4.1.3 los automorfismos permutan las raíces) es decir, $\text{Gal}(K,\mathbb{Q}) = \{I, \sigma, \tau \text{ y } \sigma\tau\}$. Mas explícitamente (lo necesitaremos adelante) se tiene

$$\begin{aligned}
I(a + bi + c\sqrt{7} + d\sqrt{7}i) &= a + bi + c\sqrt{7} + d\sqrt{7}i \\
\sigma(a + bi + c\sqrt{7} + d\sqrt{7}i) &= a - bi + c\sqrt{7} - d\sqrt{7}i \\
\tau(a + bi + c\sqrt{7} + d\sqrt{7}i) &= a + bi - c\sqrt{7} - d\sqrt{7}i \\
\sigma\tau(a + bi + c\sqrt{7} + d\sqrt{7}i) &= a - bi - c\sqrt{7} + d\sqrt{7}i
\end{aligned}$$

■

(c) Con esto tenemos los subgrupos de G son $G_1 = \{I\}, G_2 = \{I, \sigma\}, G_3 = \{I, \tau\}, G_4 = \{I, \sigma\tau\}$ y $G_5 = G$, es decir, $\text{Sub}(G) = \{G_1, G_2, G_3, G_4, G_5\}$.

■

(d) Ahora, sabemos que los campos intermedios son los campos fijos de cada subgrupo de G, entonces

- $K^{G_1} = \{k \in K : I(k) = k\} = K = \mathbb{Q}(i, \sqrt{7})$

- $$\begin{aligned} K^{G_2} &= \{k \in K : \sigma(k) = k\} \\ &= \{k \in K : a - bi + c\sqrt{7} - d\sqrt{7}i = a + bi + c\sqrt{7} + d\sqrt{7}i\} \\ &= \{k \in K : -bi - d\sqrt{7}i = bi + d\sqrt{7}i\} \quad (\Rightarrow \ b = d = 0) \\ &= \{a + c\sqrt{7} : a, c \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{7}) \end{aligned}$$

- $$\begin{aligned} K^{G_3} &= \{k \in K : \tau(k) = k\} \\ &= \{k \in K : a + bi - c\sqrt{7} - d\sqrt{7}i = a + bi + c\sqrt{7} + d\sqrt{7}i\} \\ &= \{k \in K : -c\sqrt{7} - d\sqrt{7}i = c\sqrt{7} + d\sqrt{7}i\} \quad (\Rightarrow \ c = d = 0) \\ &= \{a + bi : a, b \in \mathbb{Q}\} = \mathbb{Q}(i) \end{aligned}$$

- $$\begin{aligned} K^{G_4} &= \{k \in K : \sigma\tau(k) = k\} \\ &= \{k \in K : a - bi - c\sqrt{7} + d\sqrt{7}i = a + bi + c\sqrt{7} + d\sqrt{7}i\} \\ &= \{k \in K : -bi - c\sqrt{7} = bi + c\sqrt{7}\} \quad (\Rightarrow \ b = c = 0) \\ &= \{a + d\sqrt{7}i : a, d \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{7}i) \end{aligned}$$

- $K^{G_5} = \{k \in K : (I, \sigma\tau, \sigma, \tau)(k) = k\} = K^{G_1} \cap K^{G_2} \cap K^{G_3} \cap K^{G_4} = \{a : a \in \mathbb{Q}\} = \mathbb{Q}$

Por tanto $\mathrm{Ret}(K / \mathbb{Q}) = \left\{\mathbb{Q},\ \mathbb{Q}(i), \mathbb{Q}(\sqrt{7}), \mathbb{Q}(\sqrt{7}i),\ \mathbb{Q}(i, \sqrt{7})\right\}$.

■

(*e*) Tendremos

Subgrupos de $\mathrm{Gal}(K / \mathbb{Q})$

$$\begin{tikzcd}
 & \{I\} & \\
\{I,\tau\} \arrow[ur] & \{I,\sigma\tau\} \arrow[u] & \{I,\sigma\} \arrow[ul] \\
 & \{I,\sigma,\tau,\sigma\tau\} \arrow[ul] \arrow[u] \arrow[ur] &
\end{tikzcd}$$

Subcampos intermedios

$$\begin{tikzcd}
 & \mathbb{Q}(i,\sqrt{7}) & \\
\mathbb{Q}(i) \arrow[ur] & \mathbb{Q}(\sqrt{7}i) \arrow[u] & \mathbb{Q}(\sqrt{7}) \arrow[ul] \\
 & \mathbb{Q} \arrow[ul] \arrow[u] \arrow[ur] &
\end{tikzcd}$$

■