

(60)

1.8	9
2.7	6
2.6	6
3.4	9
3.6	10
3.13	10

Problema 8 (Guía 1)

Calcule el grado sobre \mathbb{Q} de las siguientes extensiones

- (a) $[\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}]$ (c) $[\mathbb{Q}(\sqrt{1+2i}) : \mathbb{Q}]$
 (b) $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$ (d) $[\mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2}) : \mathbb{Q}]$

- Desarrollo -

(a) Notar que $\sqrt[4]{3}$ es raíz del polinomio $p(x) = x^4 - 3 \in \mathbb{Q}[x]$, que por criterio de Eisenstein, es irreducible. Luego

$$[\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}] = \deg(p(x)) = 4$$

(b) Afirmación $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$

Como $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$, entonces la inclusión $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ es evidente.

Ahora, como $(\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6}$, tenemos que $\sqrt{6} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Con esto último podemos verificar que $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. En efecto

$$\begin{aligned}\sqrt{2} &= (2\sqrt{3} + 3\sqrt{2}) - (2\sqrt{2} + 2\sqrt{3}) = \sqrt{6}(\sqrt{2} + \sqrt{3}) - 2(\sqrt{2} + \sqrt{3}) \\ &= \sqrt{6}(\sqrt{2} + \sqrt{3}) - 2(\sqrt{2} + \sqrt{3})\end{aligned}$$

Como $\sqrt{2} + \sqrt{3}, \sqrt{6} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$, $\sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Por otro lado

$$\sqrt{3} = (\sqrt{2} + \sqrt{3}) - \sqrt{2}$$

y así $\sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Con esto se tiene que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3})$

$$\therefore \mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

Sea ahora $a = \sqrt{2} + \sqrt{3}$. Debemos buscar un polinomio irreducible $p(x) \in \mathbb{Q}[x]$ tal que a es raíz.

$$\begin{aligned}a^2 &= 5 + 2\sqrt{6} \\ \Rightarrow a^2 - 5 &= 2\sqrt{6} \\ \Rightarrow a^4 - 10a^2 + 25 &= 24 \\ \Rightarrow a^4 - 10a^2 + 1 &= 0\end{aligned}$$

Consideraremos $p(x) \in \mathbb{Q}[x]$ por $p(x) = x^4 - 10x^2 + 1$, veremos que $p(a) = 0$.

Afirmación. $p(x) = x^4 - 10x^2 + 1$ es irreducible.

Es fácil ver que $p(x)$ no posee factores lineales ya que $p(x)$ no posee raíces en \mathbb{Q} (notar que $p(1), p(-1) \neq 0$, donde 1, -1 pueden ser las únicas raíces racionales).

Para verificar que $p(x)$ no tiene factores cuadráticos, consideramos la igualdad

$$x^4 - 10x^2 + 1 = (x^2 + ax + b)(x^2 + cx + d)$$

como $(x^2 + ax + b)(x^2 + cx + d) = x^4 + cx^3 + dx^2 + ax^3 + acx^2 + adx + bx^2 + bcx + bd$
 $= x^4 + (a+c)x^3 + (ac+b+d)x^2 + (ad+bc)x + bd$, nos queda el sistema de ec:

$$\begin{aligned} a + c &= 0 \\ ac + b + d &= -10 \\ ad + bc &= 0 \\ bd &= 1 \end{aligned}$$

De $a+c=0$, $ad+bc=0$, tenemos

$$\begin{aligned} ad + dc &= 0 & (d \neq 0) \\ ad + bc &= 0 \end{aligned}$$

luego $c(d-b)=0$.

Si $d=b$, entonces $d=b=1$, quedando

$$\begin{aligned} ac &= -12 \\ a + c &= 0 \end{aligned}$$

y de estas dos ecuaciones no queda que $c^2=12$, pero tal c no existe en \mathbb{Q} .

Si $d \neq b$, entonces $c=0$, y con ello $a=0$. Nos queda

$$\begin{aligned} b + d &= -10 \\ db &= 1 \end{aligned}$$

pero nos resulta $b^2 + 10b + 1 = 0$, lo cual no posee raíces en \mathbb{Q} . Con esto, $p(x)$ no puede factorizarse en factores cuadráticos.

∴ $p(x)$ es irreducible

$$\therefore [\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$$

$$\therefore [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$$

(c) Considerando $a = \sqrt{1+2i}$ tenemos

$$\begin{aligned}a^2 &= 1+2i \\ \Rightarrow a^2 - 1 &= 2i \\ \Rightarrow a^4 + 1 - 2a^2 &= -4 \\ \Rightarrow a^4 - 2a^2 + 5 &= 0\end{aligned}$$

a es raíz de $p(x) = x^4 - 2x^2 + 5 \in \mathbb{Q}[x]$. Recordemos que si p/q es raíz de $p(x)$, entonces $p|5$, $q|1$ (criterio usado en (b)). Luego las únicas raíces racionales pueden ser ± 5 . ($\sigma \pm 1$)

$$p(5) = p(-5) = 625 - 50 + 5 \neq 0$$

Con esto afirmamos que $p(x)$ no posee factores lineales. Para ver que $p(x)$ no tiene factores cuadráticos usamos mismo procedimiento

$$x^4 - 2x^2 + 5 = (x^2 + ax + b)(x^2 + cx + d)$$

donde

$$\begin{aligned}a+c &= 0 \\ ac+b+d &= -2 \\ ad+bc &= 0 \\ bd &= 5\end{aligned}$$

Al igual que en (b) obtenemos la igualdad $c(d-b) = 0$, pero como $bd = 5$, eso implica $b \neq d$ (en caso contrario $b^2 = d^2 = 5$, $b, d \in \mathbb{Q}$), y $c=0$. De la primera igualdad, $a=0$, y nos queda

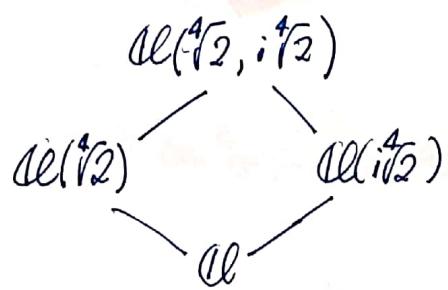
$$\begin{aligned}b+d &= -2 \\ bd &= 5\end{aligned}$$

De esto llegamos a la ecuación $d^2 + 2d + 5 = 0$, en la cual no existe $d \in \mathbb{Q}$ que la satisfaga.

$\therefore p(x)$ es irreducible

$$\therefore [\mathbb{Q}(\sqrt{1+2i}) : \mathbb{Q}] = 4$$

(d)



Como $\sqrt[4]{2}$ es raíz del polinomio irreducible $x^4 - 2$ (Eisenstein), $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$.

Como $i\sqrt[4]{2} \in \mathbb{C}\mathbb{R}$ ($\sqrt[4]{2} \in \mathbb{R}$, $i \in \mathbb{C}$), se tiene que $i \notin \mathbb{Q}(\sqrt[4]{2})$;
en otras palabras, el polinomio $x^2 + 1 \in (\mathbb{Q}(\sqrt[4]{2}))[x]$ es irreducible.

Así tenemos

$$\begin{array}{c} \mathbb{Q}(\sqrt[4]{2}, i) \\ \downarrow \\ \mathbb{Q}(\sqrt[4]{2}) \quad i \\ \downarrow \quad \downarrow \\ \mathbb{Q}(\sqrt[4]{2}) \quad i\sqrt[4]{2} \\ \downarrow \quad \downarrow \\ \mathbb{Q} \end{array}$$

Obligatoriamente $\mathbb{Q}(\sqrt[4]{2}, i) = \mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2})$, por lo tanto

$$[\mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2}) : \mathbb{Q}] = 8$$

Al ser $i\sqrt[4]{2}$ raíz de un polinomio de grado 2, el resultado es:

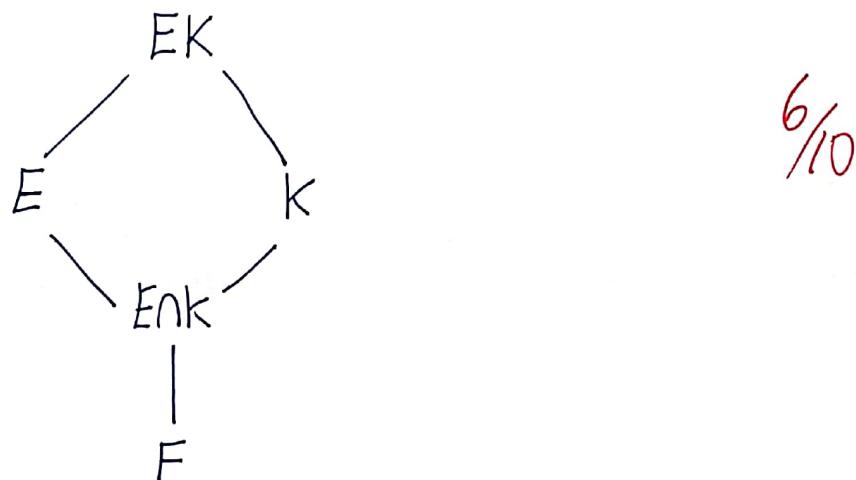
• $i\sqrt[4]{2} \in \mathbb{Q}(\sqrt[4]{2})$

Problema 7 (Guía 2)

Probar que si K/F es una extensión finita con $K \subseteq L$, entonces $[EK:EF] \leq [K:F]$ para todo campo $E \subseteq L$ que contenga a F .

- Demostración -

Primero veamos que para todo campo $E \subseteq L$ que contenga a F , $EF = E$. Haciendo un diagrama tenemos



Ahora como K/F es finita, existen $\alpha_1, \dots, \alpha_n \in K$ tales que $K = F(\alpha_1, \dots, \alpha_n)$. Recordemos que $\alpha_1, \dots, \alpha_n \notin F$, luego para E campo que contenga F , E podría contener algunos α_i . Con lo anterior:

$$\begin{aligned} EK &= E(F(\alpha_1, \dots, \alpha_n)) \\ &= E(\alpha_{i_1}, \dots, \alpha_{i_r}) \end{aligned}$$

la pregunta es el caso $K = F(\alpha)$
de modo que sólo hay un generador...

donde $|\{\alpha_{i_1}, \dots, \alpha_{i_r}\}| \leq |\{\alpha_1, \dots, \alpha_n\}|$. En particular, EK es el campo más pequeño que contiene a E, F y $\alpha_1, \dots, \alpha_n \in K$. Por otro lado, por lo visto en clases, $\text{in}_{\alpha_i, E}(x) \mid \text{in}_{\alpha_i, F}(x)$ y

$$\begin{aligned} [F(\alpha_1, \dots, \alpha_n) : F] &= \prod_{i=1}^n \deg(\text{in}_{\alpha_i, F}(x)) \\ [E(\alpha_{i_1}, \dots, \alpha_{i_r}) : E] &= \prod_{j=1}^r \deg(\text{in}_{\alpha_{i_j}, E}(x)) \end{aligned}$$

← cuidado, esto no lo cuentan
(por ej. si todas las extensiones
son iguales)

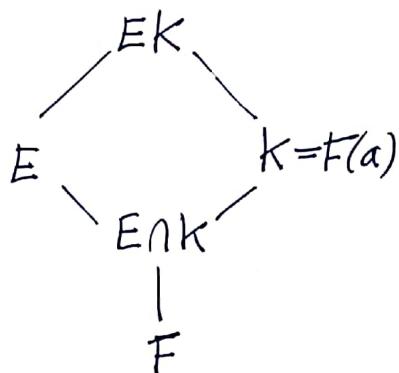
Por lo tanto, se concluye que $[EK:EF] \leq [K:F]$.

(se puede hacer una inducción para el caso general, pero el argumento de arriba no lo muestra)

Problema 6 (Guía 2)

Probar que si $K = F(\alpha) \subseteq L$, entonces $[EK : E] \leq [K : F]$ para todo cuerpo $E \subseteq L$ que contenga a F .

- Demarcación -



La desigualdad se cumple automáticamente si $[K : F] = \infty$. Si K/F es una extensión finita, entonces ocupando resultado del problema 7 (guía 2), vemos que la desigualdad se cumple.

∴ $[EK : E] \leq [K : F]$ para todo cuerpo $E \subseteq L$ que contenga a F .

¶

cuidado!

como regla general,
no se debe usar un resultado
que es una generalización
para no triviosamente el problema

(Te repito el 6/10
del problema anterior)

Problema 4 (Guía 3)

Determine si x^6+x+1 tiene o no raíces en \mathbb{F}_4 . Lo mismo para x^5+x+1

-Desarrollo-

$$\mathbb{F}_4 = \mathbb{F}_2[x] / (x^2 + x + 1) = \{a + b\alpha \mid a, b \in \mathbb{F}_2; \alpha^2 + \alpha + 1 = 0\}. \text{ No olvidemos que}$$

$x^2 + x + 1$ es el único polinomio cuadrático irreducible en $\mathbb{F}_2[x]$. Con esto, los elementos de \mathbb{F}_4 son $0, 1, \alpha, 1+\alpha$. Ahora basta reemplazar en $p(x) = x^6 + x + 1$.

$$p(0) = 0^6 + 0 + 1 = 1,$$

$$p(1) = 1^6 + 1 + 1 = 1 + 1 + 1 = 1,$$

$$p(\alpha) = \alpha^6 + \alpha + 1 \quad \text{Como } \alpha^6 = (\alpha^2)^3 = (\alpha+1)^3 = (\alpha+1)(\alpha+1)^2 = (\alpha+1)(\alpha^2 + 1)$$

$$= (\alpha+1)\alpha = \alpha^2 + \alpha = \alpha + 1 + \alpha = 1, \text{ entonces } p(\alpha) = \alpha^6 + \alpha + 1 = 1 + \alpha + 1 = \alpha$$

$$p(\alpha+1) = (\alpha+1)^6 + (\alpha+1) + 1 = (\alpha+1)^6 + \alpha. \text{ Como}$$

$$(\alpha+1)^6 = (\alpha^2 + 1)^3 = \alpha^3 = \alpha(\alpha+1) = \alpha^2 + \alpha = 1,$$

$$p(\alpha+1) = 1 + \alpha. \text{ Por lo tanto } p(x) \text{ no posee raíces en } \mathbb{F}_4.$$

Ahora para $q(x) = x^5 + x + 1$,

9/10

$$q(0) = 0^5 + 0 + 1 = 1$$

$$q(1) = 1^5 + 1 + 1 = 1,$$

$$q(\alpha) = \alpha^5 + \alpha + 1. \text{ Como } \alpha^5 = \alpha^2 \alpha^3 = (\alpha+1)^1 = \alpha + 1, \text{ entonces } q(\alpha) = \alpha + 1 + \alpha + 1 = 0$$

$$q(\alpha+1) = (\alpha+1)^5 + (\alpha+1) + 1 = (\alpha+1)^5 + \alpha.$$

$$(\alpha+1)^5 = (\alpha+1)(\alpha+1)^4 = (\alpha+1)(\alpha^4 + 1) = (\alpha+1)((\alpha+1)^2 + 1)$$

$$= (\alpha+1)(\alpha^2 + 1 + 1) = (\alpha+1)\alpha^2 = (\alpha+1)(\alpha+1) = \alpha^2 + 1 = \alpha.$$

Luego la única raíz de $q(x)$ es α .

??
q(x+1) = ?

¡imposible! si α es raíz también

$\alpha+1$ pues al grupo de Galois los intercambios.

Problema 6 (Guía 3)

• Encuentre el menor entero r tal que \mathbb{F}_7^r contiene una raíz enceava primitiva de la unidad.

- Desarrollo - Recordemos que \mathbb{F}_7^r es el cuadro de descomposición de $x^{7^r} - x$. Para $x \in (\mathbb{F}_7^r)^\times$ ($x \neq 0$) se tiene

$$x^{7^r} - x = 0 \Rightarrow x(x^{7^r-1} - 1) = 0 \rightarrow x^{7^r-1} - 1 = 0$$

Luego $(\mathbb{F}_7^r)^\times$ contiene a las $7^r - 1$ raíces de la unidad. En particular

$$(\mathbb{F}_7^r)^\times = \{x \in \mathbb{F}_7^r / x^{7^r-1} = 1\} \quad (\text{Grupo cíclico multiplicativo})$$

Ahora si $(\mathbb{F}_7^r)^\times$ contiene una raíz enceava primitiva de la unidad, digamos ξ_{11} , entonces $G = \langle x / x^{11}-1 = 0 \rangle = \langle \xi_{11} \rangle \leq (\mathbb{F}_7^r)^\times$. Ahora por Lagrange, implica que $11 \mid 7^r - 1$. La pregunta anterior ahora consiste en encontrar el menor entero r que resuelva la congruencia

$$7^r \equiv 1 \pmod{11}$$

Como 11 es primo, $\mathbb{Z}/11\mathbb{Z}$ es cuerpo, en otras palabras, los inversos módulo 11 son únicos (para empezar existen). No es difícil afirmar que

$$7^r \cdot 8^r \equiv 1 \pmod{11}$$

Luego, estudiar la congruencia $7^r \equiv 1 \pmod{11}$ es equivalente a estudiar la congruencia $8^r \equiv 1 \pmod{11}$, ya que

$$7^r \equiv 1 \pmod{11}$$

$$7^r \cdot 8^r \equiv 8^r \pmod{11}$$

$$8^r \equiv 1 \pmod{11}$$

Pero como $8 = 2^3$, entonces nos reducimos a estudiar la congruencia $2^r \equiv 1 \pmod{11}$.

Una pequeña lista para ayudar

$$2^1 = 2$$

$$2^5 \equiv 10 \pmod{11}$$

$$2^8 \equiv 14 \equiv 3 \pmod{11}$$

$$2^2 = 4$$

$$2^6 \equiv 20 \equiv 9 \pmod{11}$$

$$2^9 \equiv 6 \pmod{11}$$

$$2^3 = 8$$

$$2^7 \equiv 18 \equiv 7 \pmod{11}$$

$$2^{10} \equiv 12 \equiv 1 \pmod{11}$$

$$2^4 = 16 \equiv 5 \pmod{11}$$

Por lo tanto, $r=10$ es el menor entero que resuelve $2^r \equiv 1(11)$, en particular, $8^r \equiv 1(11)$.

∴ Para $r=10$, \mathbb{F}_{r^2} contiene una raíz octava primitiva de la unidad.

Problema 13 (Guía 3)

Sea $f(x)$ un polinomio con coeficientes en \mathbb{F}_p . Probar que $f'(x)=0$ si y sólo si $f(x)=g(x)^p$ para algún polinomio g con coeficientes en \mathbb{F}_p .

- Demostración -

$$\text{Sea } f(x) = \sum_{i=0}^n a_i x^i, \quad a_i \in \mathbb{F}_p \quad (i=0, \dots, n). \quad f'(x) = \sum_{i=1}^n i a_i x^{i-1}$$

$$f'(x)=0 \quad \text{ssi} \quad ia_i=0, \quad \text{todo } i \in \{1, \dots, n\}$$

Como p es primo y $p \mid ia_i$ ($ia_i \in \mathbb{F}_p$), entonces $p \mid i$ o $p \mid a_i$.

Recordando que $p \mid a_i$ ssi $a_i=0$ (módulo p), tenemos que

$$f'(x)=0 \quad \text{ssi} \quad f(x) = a_0 + a_p x^p + a_{2p} x^{2p} + \dots + a_{kp} x^{kp}$$

donde $kp=n$. Por otro lado, para todo $\alpha \in \mathbb{F}_p$, $\alpha^p=\alpha$; usamos este resultado de la manera siguiente

$$\begin{aligned} f(x) &= a_0 + a_p x^p + a_{2p} x^{2p} + \dots + a_{kp} x^{kp} = a_0^p + a_p^p x^p + a_{2p}^p x^{2p} + \dots + a_{kp}^p x^{kp} \\ &= (a_0 + a_p x + a_{2p} x^2 + \dots + a_{kp} x^k) \end{aligned}$$

Tomando $g(x) = a_0 + a_p x + \dots + a_{kp} x^k$, veamos que se cumple

$$f'(x)=0 \iff f(x)=g(x)^p, \quad g(x) \in \mathbb{F}_p[x].$$

Problema 1. Sea $K(t) = \left\{ \frac{f(t)}{g(t)} \mid f, g \in K(t), g \neq 0 \right\}$

K anejo, $K(t)$ anejo de funciones racionales. Sea $u = \frac{P(t)}{Q(t)} \in K(t)$, con $(P, Q) = 1$.

(a) Muestre que el polinomio $f(x) = P(x) - uQ(x)$ es irreducible en $K(u)$ y tiene a t como raíz.

Dem. Observe que $f(t) = P(t) - uQ(t) = 0$

Como $K[u]$ es un DFL y su cuerpo de fracciones es $K(u)$, por

lema de Gauss:

$P(x) - uQ(x)$ es irreducible en $(K(u))(x) \Leftrightarrow$ irreducible $(K(u))[x]$
 \Leftrightarrow es irreducible en $K(x)(u)$ lineal en este DFL \Rightarrow es irreducible.

(b) Muestre que el grado de $P(x) - uQ(x)$ como polinomio en $(K(u))[x]$ es $\max\{\deg P, \deg Q\}$

(c) Muestre que $[K(t) : K(u)] = \max\{\deg P, \deg Q\}$

Dem. t raíz del polinomio irreducible. $P(x) - uQ(x) = f(x)$

$$f = \text{irr}_{t, K(u)}(x)$$

$$\therefore [K(t) : K(u)] = \deg(\text{irr}_{t, K(u)}(x)) = \max\{\deg P, \deg Q\}$$

Problema 2. Pruebe que los automorfismos de $K(t)$ que fijan K son las transformaciones lineales fraccionarias determinadas por

$$t \mapsto \frac{at+b}{ct+d}, \text{ con } ad-bc \neq 0$$

Demarcación. Sea $\varphi: K(t) \rightarrow K(t)$. $\varphi(f(t)) = f\left(\frac{at+b}{ct+d}\right)$.

Claramente φ es un homomorfismo.

Inyección: Si $\varphi(f(t)) = \varphi(g(t)) \Rightarrow f\left(\frac{at+b}{ct+d}\right) = g\left(\frac{at+b}{ct+d}\right)$
 $\Rightarrow f = g$ en $K\left(\frac{at+b}{ct+d}\right)$. Pero

$$[K(t) : K\left(\frac{at+b}{ct+d}\right)] = \max\{1, 1\} = 1 \quad \therefore f = g \text{ en } K(t).$$

Epiyectividad: Sea $f \in k(t) \Rightarrow \exists g: g\left(\frac{at+b}{ct+d}\right) = f(t)$, pues
 $k\left(\frac{at+b}{ct+d}\right) = k(t) \quad \therefore \text{Im } \varphi = k(t)$

Conveniamente, sea $\varphi \in \text{Aut}_k(k(t))$ y $f(t) = \frac{\sum a_i t^i}{\sum b_i t^i}$; $a_i, b_i \in k$
arbitrarios en $k(t)$

$$\varphi(f(t)) = \frac{\varphi(\sum a_i t^i)}{\varphi(\sum b_i t^i)} = \frac{\sum a_i \varphi(t)^i}{\sum b_i \varphi(t)^i} = f(\varphi(t))$$

Podemos decir que $\varphi(t) = \frac{P(t)}{Q(t)}$ con $\text{mcd}(P, Q) = 1$. Ahora
 $\text{Im } \varphi = k(\varphi(t)) = k\left(\frac{P(t)}{Q(t)}\right)$. Como φ es automorfismo:

$$\text{Im } \varphi = k(t) \Rightarrow \boxed{\text{Im } \varphi = k(t)}. [k(t) : k(\varphi(t))] = 1$$

$$\therefore \varphi(t) = \frac{at+b}{ct+d}$$

Problema 3: Sea K campo y $K(t)$ cuerpo de funciones racionales.

Definimos $\sigma, \varrho: K(t) \rightarrow K(t)$,

$$\sigma(f(t)) = f\left(\frac{1}{1-t}\right)$$

$$\varrho(f(t)) = f\left(\frac{1}{t}\right)$$

Pruebe que σ, ϱ son automorfismos de $K(t)$ y que $G = \langle \sigma, \varrho \rangle \cong S_3 \cong D_6$.

Demonstración: Notar que $\sigma^3 = \varrho^2 = 1$ y que $\sigma\varrho = \varrho\sigma^{-1}$. Pues
 $\sigma(f(t)) = f\left(\frac{1}{1-t}\right) \Rightarrow \sigma^2(f(t)) = \sigma f\left(\frac{1}{1-t}\right) = f\left(\frac{1}{1-\frac{1}{1-t}}\right)$
 $= f\left(\frac{1-t}{t}\right)$

$$\sigma^3(f(t)) = f\left(\frac{1 - \frac{1}{1-t}}{-\frac{1}{1-t}}\right) = f\left(\frac{t}{1-t}\right) = f(t)$$

Problema 6. Puedes que $u = \frac{(t^2 - t + 1)^3}{t^2(t-1)^2}$ quede fijo para todo G .

Dem. Solo hay que ver que σ y τ lo fijan:

$$\sigma(u) = \frac{\left(\left(\frac{1}{1-t}\right)^2 - \frac{1}{1-t} + 1\right)^3}{\left(\frac{1}{1-t}\right)^2 \left(\frac{1}{1-t} - 1\right)^2} = u$$

$$\tau(u) = \frac{\left(\frac{1}{t^2} - \frac{1}{t} + 1\right)^3}{\frac{1}{t^2} \left(\frac{1}{t} - 1\right)^2} = u$$

Problema que $K(t)^G = K(u)$

Dem. Por lo anterior, $K(u) \subseteq K(t)^G \subseteq K(t)$, pero $[K(t) : K(u)] = 6$
 $= [K(t) : K(t)^G] = |G|$

$$\therefore K(t)^G = K(u), \text{ ya que } \underbrace{[K(t) : K(u)]}_6 = [K(t) : K(t)^G][K(t)^G : K(u)]$$

Observación: K/F Galoisiana,

$G = \text{Gal}(K/F)$, entonces:

Si $\sigma, \tau \in G$, entonces $\sigma|_E = \tau|_E$ si $\sigma \in H$

$\sigma^{-1}\tau|_E = \text{id}_E$ si $\sigma^{-1}\tau \in H$ si $\tau \in \sigma H$

\therefore Las distintas invustaciones de E están en biyección con G/H

$$\forall \sigma \in G, \sigma|_E =$$

Problema 4. E/F extensión finita y $\alpha \in E$. Sea K/F extensión de Galois que contiene a E y $H \leq \text{Gal}(K/F)$, subgrupo asociado a E .

$$N_{E/F}: E \rightarrow F$$

$$\alpha \mapsto \prod_{\sigma \in H} \sigma(\alpha)$$

(el producto se toma sobre todas las invustaciones de E en una clausura F). Sea $\mathcal{J} = \{\sigma_1, \dots, \sigma_m\}$ representantes de G/H .

Pruebe que $N_{E/F}(\alpha) \in F$

$$N_{E/F}(\alpha) = \prod_{\sigma \in \text{Gal}(E/F)} \sigma(\alpha). \text{ Sea } \sigma \in \text{Gal}(E/F) : \sigma(N_{E/F}(\alpha)) = \prod_{\sigma \in \text{Gal}(E/F)} \sigma(\alpha)$$

$\Downarrow \quad \Downarrow$

$$\prod_{\sigma \in \text{Gal}(E/F)} \sigma(\alpha) \quad N_{E/F}(\alpha)$$

Si $E=F(\sqrt{D}) \Rightarrow N(a+b\sqrt{D}) = a^2 - b^2 D$

obs: Si $\sigma(a+b\sqrt{D}) = a-b\sqrt{D}$ (solo may²)

$$\therefore N_{E/F}(a+b\sqrt{D}) = a^2 - b^2 D$$

Sea $m_\alpha(x) = x^d + a_{d-1}x^{d-1} + \dots + a_1x + a_0 \in F[x]$ - Si $n = [E:F]$,

pruebe que cuando d/n , hay d distintos conjugados de α que se repiten $\frac{n}{d}$ veces en el producto y concluir que $N_{E/F}(\alpha) = (-1)^n a_0^{n/d}$
(Si E/F Galoiana $\Rightarrow N_{E/F}(\alpha) = (-1)^n a_0$)

$$m_\alpha(x) = (x-\alpha) \dots (x-\sigma_d(\alpha))$$

$$\therefore a_0 = (-1)^d \alpha \sigma_1(\alpha) \dots \sigma_d(\alpha)$$

obs. d/n pues $n = [E:F]$, $d = [F(\alpha):F]$, $F(\alpha) \subseteq E$

Problema 1. E/F extensión finita y $\alpha \in E$. Sea k/F Galoiana con $F \subseteq E \subseteq k$ y sea $H \leq \text{Gal}(k/F)$ que corresponde a E .

$$N_{E/F} : E \rightarrow F, \quad N_{E/F}(\alpha) = \prod_{\sigma} \sigma(\alpha)$$

(σ pertenece a algún conjunto de representantes de G/H)

Sean $m_{\alpha}(x) = x^d + a_{d-1}x^{d-1} + \dots + a_0 \in F[x]$, $n = [E:F]$.

Pruebe que $d|n$, que hay d distintos conjugados de α que se repiten $\frac{n}{d}$ veces en el producto que define a la norma y concluya que: $N_{E/F}(\alpha) = (-1)^n a_0^{\frac{n}{d}}$

dem. Como $F \subset F(\alpha) \subset E$, es claro que $[F(\alpha):F] = d | n = [E:F]$.

Ahora E es separable sobre F (K separable sobre F). Las raíces del polinomio minimal son los conjugados de Galois de α .

Hay d ya que $\text{grad } m_{\alpha}(x) = d$.

Sabemos que hay n invenciones $E \rightarrow \overline{F}$. Cada una de ellas envía a α a un conjugado de α . Entonces cada conjugado se repite $\frac{n}{d}$ -veces.

$$\begin{aligned} \text{Pues si } \sigma, \tau \in G \text{ cumplen con } \sigma|_E = \tau|_E &\Leftrightarrow \sigma\tau^{-1}|_E = \text{id}_E \\ \therefore \sigma\tau^{-1} \in H &\Leftrightarrow \tau \in \sigma H \end{aligned}$$

Sean $\{\sigma_1, \dots, \sigma_d\}$ los conjugados de α . $N_{E/F}(\alpha) = \prod_{\sigma} \sigma(\alpha)$
 $= \left(\prod_{i=1}^d \alpha_i \right)^{\frac{n}{d}}$

$$\text{Dem: } m_{\alpha}(x) = (x - \alpha_1) \cdots (x - \alpha_d) = (-1)^d \prod_{i=1}^d \alpha_i = a_0$$

$$\Rightarrow N_{E/F}(\alpha) = (-1)^n a_0^{\frac{n}{d}}$$

$$\text{Ej: } \text{tr}_{E/F}(\alpha) = -\frac{n}{d} a_{d-1}$$

Problema 2. Con las notaciones precedentes muestra que :

$$N_{E/F}(\alpha) = \alpha^n N_{E/F}(\alpha) \quad , \quad \text{tr}_{E/F}(\alpha\alpha) = \alpha \text{tr}_{E/F}(\alpha) \quad \forall \alpha \in F$$

$$\text{En particular : } N_{E/F}(\alpha) = \alpha^n, \quad \text{tr}_{E/F}(\alpha) = n\alpha, \quad \alpha \in F$$

$$\underline{\text{Dem:}} \quad N_{E/F}(\alpha) = N_{E/F}(\alpha) N_{E/F}(\alpha) = \alpha^n N_{E/F}(\alpha)$$

$$\cancel{\text{tr}_{E/F}(\alpha\alpha) = \sum_{\sigma} \sigma(\alpha\alpha) = \sum_{\sigma} \alpha \sigma(\alpha) = \alpha \sum_{\sigma} \sigma(\alpha)}$$

$$= \alpha \text{tr}_{E/F}(\alpha).$$

~~$$\alpha = a + mb$$

$$\alpha^d = (a + mb)^d = a^d + \binom{d}{1} a^{d-1} mb + \binom{d}{2} a^{d-2} m^2 b^2 + \dots + m^d b^d$$~~

Problema 3. $K = \mathbb{Q}(\sqrt[n]{a})$, $a > 0$; $[K:\mathbb{Q}] = n$, $E \subseteq K$

con $[E:\mathbb{Q}] = d$. Puede que $E = \mathbb{Q}(\sqrt[n]{a})$

Dem. $x^d - a$ es irreducible sobre \mathbb{Q} , pues

$$(x^d)^k - a = x^{nk} - a$$

$$\text{Si } x^d - a = p_1(x)p_2(x) \Rightarrow (x^k)^d - a = p_1(x^k)p_2(x^k) \quad (\rightarrow \Leftarrow)$$

$\therefore [\mathbb{Q}(\sqrt[n]{a}):\mathbb{Q}] = d$, S raíz n -ésima de la unidad.

$$\text{Sea } \alpha = \sqrt[n]{a}, \text{ entonces } N_{\mathbb{Q}/\mathbb{Q}}(\alpha) = \prod_{\sigma} \sigma(\alpha) = \prod_{m=1}^k g^m \alpha$$

$$= g^m \alpha$$

$$([K:E] = k, \quad \alpha^k = a^{k/n} = a^{1/d} = \sqrt[d]{a})$$

Como $N_{K/E} : K \rightarrow E \subseteq \mathbb{R}$, $g^n = \pm 1$, como $N_{K/E}(\alpha) = \sqrt[d]{a}$

$$\Rightarrow \mathbb{Q}(\sqrt[d]{a}) \subseteq E$$

$$\therefore \mathbb{Q}(\sqrt[d]{a}) = E \quad (\text{igualdad de grado})$$

Problema 4. Sea F subcuerpo de \mathbb{R} . Sea $a \in F$ y $K = f(\bar{a})$.

Pruebe que si L es cualquier extensión de Galois de F contenida en K , entonces $[L : K] \leq 2$

dem. Supongamos que $[L : F] = d$. Entonces $F(\sqrt[d]{a}) \subseteq L$.

Como L es de Galois, también contiene a $\sqrt[d]{a}$: Como $F \subseteq \mathbb{R}$, d es a lo más raíz 2-ésima de la unidad $\therefore [L : F] = 2$.

(Pensar qué pasa con $a < 0$)

Problema 5 p primo. Prueba que un 2-ciclo y un p -ciclo generan a S_p .

Concluir que un polinomio irreducible de grado p con coeficientes racionales tienen exactamente 2 raíces no reales, y si L es el cuelpo de descomposición sobre \mathbb{Q} : $\text{Gal}(L/\mathbb{Q}) \cong S_p$.

dem. Sean $\alpha_1, \dots, \alpha_{p-2}$ raíces reales, α_{p-1}, α_p las complejas. La conjugación corresponde a $(p-1, p)$. Como $[(\mathbb{Q}(\alpha_i) : \mathbb{Q}] = p$ $\Rightarrow p \mid [L : \mathbb{Q}] = |G| \therefore$ existe elemento de orden p . Tal elemento visto en S_p es un ciclo de largo p . Salvo reordenamiento de las raíces, tal elemento es $(1, 2, \dots, p)$.

Problema. Si $n = [L : K]$ no es divisible por la característica de K , K contiene una raíz ~~de~~ n -ésima de la unidad ρ , probar que $L = K(\sqrt[n]{c})$, $c \in K$.

Demonstración. $\Phi_n(x) \in \mathbb{Z}[x]$ es mónico y su término constante es 1 a partir de $m=3$.

$$\Phi_1(x) = x-1, \Phi_2(x) = x+1, \Phi_3(x) = x^2 + x + 1$$

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x)$$

Se sigue que $N_{E/K}(p) = 1$, luego $\exists b \in E^*$: $\frac{b}{\sigma(b)} = p$
Así $\sigma(b) = p^{-1}b$
 $\sigma^2(b) = p^{-1}\sigma(b) = \cancel{p^{-1}}b = p^{-2}\sigma(b)$
 \vdots
 $\sigma^n(b) = b$

Por lo tanto, $|\sigma| \geq n = |p| \Rightarrow |\sigma| = n$

Luego: $[E : K] = n = |\text{Gal}(E/K)|$, $[L : K] = n$, $E = L$

EJERCICIO 1. (Extensiones Bicuadráticas) Sea F un cuerpo de característica $\neq 2$.

1. Si $K = F(\sqrt{D_1}, \sqrt{D_2})$ donde $D_1, D_2 \in F$ tienen la propiedad que ninguno de $D_1, D_2, D_1 D_2$ es un cuadrado en F , entonces K/F es extensión de Galois con $\text{Gal}(K/F)$ isomorfo al grupo 4 de Klein.
2. Recíprocamente, suponga que K/F es extensión de Galois con $\text{Gal}(K/F)$ isomorfo al grupo 4 de Klein. Pruebe que $K = F(\sqrt{D_1}, \sqrt{D_2})$ donde $D_1, D_2 \in F$ tienen la propiedad de que ninguno de $D_1, D_2, D_1 D_2$ es un cuadrado en F .

EJERCICIO 2. (Teorema 90 de Hilbert) Sea K/F extensión finita y sea $\alpha \in K$. Sea L extensión de Galois de F que contiene K y sea $H \leq \text{Gal}(L/F)$ el subgrupo correspondiente a K . Definir la norma de α desde K a F como:

$$N_{K/F}(\alpha) = \prod_{\substack{\sigma: K \rightarrow F \\ \text{embedding}}} \sigma(\alpha).$$

En particular, si K/F es Galois

$$N_{K/F}(\alpha) = \prod_{\sigma \in \text{Gal}(L/F)} \sigma(\alpha).$$

1. Pruebe que $N_{K/F}(\alpha) \in F$.
2. Pruebe que $N_{K/F}(\alpha\beta) = N_{K/F}(\alpha)N_{K/F}(\beta)$.
3. Teorema 90 de Hilbert:

Suponga que K/F es Galois con grupo de Galois cíclico $\text{Gal}(K/F) = \langle \sigma \rangle$. Si $\alpha \in K$ es tal que $N_{K/F}(\alpha) = 1$, entonces

$$\alpha = \frac{\beta}{\sigma(\beta)}$$

para algún $\beta \in K^$.*

EJERCICIO 3. Sea p primo. Considere el polinomio $f(x) = x^5 - 2x + p$ sobre \mathbb{Q} .

1. Demuestre que $f(x)$ es irreducible sobre \mathbb{Q} y que tiene exactamente tres raíces reales.
2. Demuestre que el grupo de Galois de $f(x)$ sobre \mathbb{Q} es isomorfo a S_5 .

EJERCICIO 4. Sea F un cuerpo y $f(x) \in F[x]$ cúbico inseparable. Demuestre que existe $g(x) \in F[x]$ de grado uno, tal que g divide a f .

EJERCICIO 5. Determine el grupo de Galois del cuerpo de descomposición de $x^4 - 14x^2 + 9$ sobre \mathbb{Q} .

EJERCICIO 6. Sea $f \in \mathbb{Q}[x]$ un polinomio mónico irreducible de grado primo p con exactamente dos raíces no reales, y sea K el cuerpo de descomposición de f sobre \mathbb{Q} . Demuestre que $\text{Gal}(K/\mathbb{Q})$ es isomorfo a un subgrupo de S_p que contiene una transposición, por lo tanto, es isomorfo a S_p (por transitividad).

EJERCICIO 7. Muestre que el grupo $\text{Gal}(\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q})$ es isomorfo al grupo Dihedral D_8 de 8 elementos.

EJERCICIO 8. Sea $p(x)$ el polinomio minimal de $\sqrt{2 + \sqrt{2}}$ sobre \mathbb{Q} . Encuentre el cuerpo de descomposición de $p(x)$ sobre \mathbb{Q} y el grupo de Galois asociado a esta extensión. Hallar todos los cuerpos intermedios de la extensión $\mathbb{Q}(\sqrt{2 + \sqrt{2}})/\mathbb{Q}$.

EJERCICIO 9. Sea $\zeta_7 = e^{\frac{2\pi i}{7}}$. Sabemos que

$$\text{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q}) \cong (\mathbb{Z}/7\mathbb{Z})^*.$$

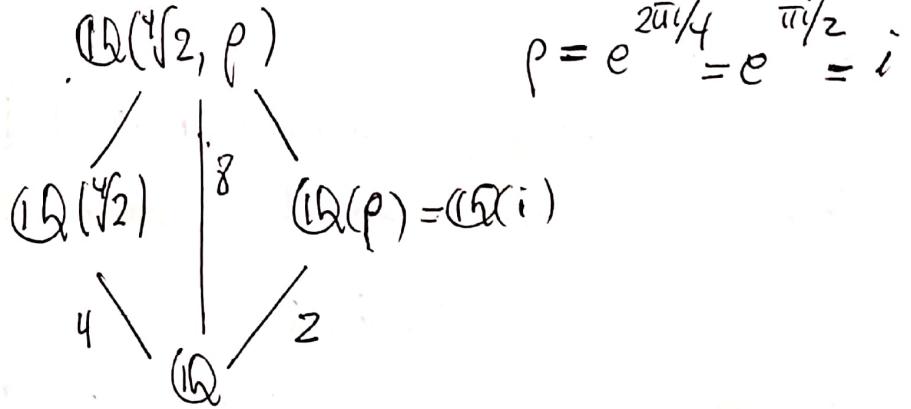
Sea $H = \langle [-1] \rangle \leq (\mathbb{Z}/7\mathbb{Z})^*$. Pruebe que el cuerpo fijo de H es $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$ y muestre que $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})/\mathbb{Q}$ es Galois con grupo de Galois isomorfo a $\mathbb{Z}/3\mathbb{Z}$.

EJERCICIO 10. Sea E/F extensión finita de Galois.

1. Sean K_1 y K_2 cuerpos intermedios de E/F con subgrupos respectivos H_1 y H_2 en $\text{Gal}(E/F) = G$.
Demuestre que si H_1 y H_2 son conjugados, entonces $\sigma(K_1) = K_2$ para algún $\sigma \in G$.
2. Pruebe que lo anterior sucede cuando $[E : F] = 750$ y $[K_1 : F] = [K_2 : F] = 6$.

EJERCICIO 11. Pruebe que si el grupo de Galois del cuerpo de descomposición de un polinomio cúbico sobre \mathbb{Q} es el grupo cíclico de orden 3, entonces todas las raíces de la cónica son reales.

$X^4 - 2$:



Sea

$$\left\{ \begin{array}{l} \sqrt[4]{2} \mapsto p^a \sqrt[4]{2} \\ i \mapsto \pm i \end{array} \right. , \quad a=0, 1, 2, 3$$

Son todos los automorfismos de K en K (non 8).

Sean

$$\sigma: \left\{ \begin{array}{l} \sqrt[4]{2} \mapsto i \sqrt[4]{2} \\ i \mapsto i \end{array} \right. , \quad \tau: \left\{ \begin{array}{l} \sqrt[4]{2} \mapsto \sqrt[4]{2} \\ i \mapsto -i \end{array} \right.$$

Queremos verificar que σ y τ generan a todos los automorfismos del párrafo anterior.

$$\sigma^2: \left\{ \begin{array}{l} \sqrt[4]{2} \mapsto -\sqrt[4]{2} \\ i \mapsto i \end{array} \right.$$

$$\sigma^3\tau: \left\{ \begin{array}{l} \sqrt[4]{2} \mapsto -i \sqrt[4]{2} \\ i \mapsto -i \end{array} \right.$$

$$\therefore \sigma^4 = \tau^2 = 1$$

$$\sigma^3: \left\{ \begin{array}{l} \sqrt[4]{2} \mapsto -i \sqrt[4]{2} \\ i \mapsto i \end{array} \right.$$

$$\text{Además } \tau \sigma \not\equiv \left\{ \begin{array}{l} \sqrt[4]{2} \mapsto -i \sqrt[4]{2} \\ i \mapsto -i \end{array} \right.$$

$$\sigma^4: \left\{ \begin{array}{l} \sqrt[4]{2} \mapsto \sqrt[4]{2} \\ i \mapsto i \end{array} \right.$$

$$\therefore \tau\sigma = \sigma^3\tau$$

$$\sigma\tau: \left\{ \begin{array}{l} \sqrt[4]{2} \mapsto i \sqrt[4]{2} \\ i \mapsto -i \end{array} \right.$$

$$\sigma^2\tau: \left\{ \begin{array}{l} \sqrt[4]{2} \mapsto -\sqrt[4]{2} \\ i \mapsto -i \end{array} \right.$$

Ejercicio 7

Muestra que el grupo $\text{Gal}(\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q})$ es isomorfo al grupo Dihedral D_8 de 8 elementos.

Dem.

(~~Definición~~)

Primero, $\mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{Q}(i, \sqrt[4]{2})$ y $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ tiene grado 4 ($\sqrt[4]{2}$ raíz de $x^4 - 2$ irreducible por Eisenstein).
Como $\mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R} \Rightarrow i \notin \mathbb{Q}(\sqrt[4]{2})$

$\therefore x^2 + 1$ irreducible sobre $\mathbb{Q}(\sqrt[4]{2})$

Así se ve fácilmente que $\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q}$ es de grado 8.

Pd: $\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q}$ es Galoisiana.

En efecto, $\mathbb{Q}(i, \sqrt[4]{2})$ es el cuerpo de descomposición de ~~$x^4 - 2 \in \mathbb{Q}[x]$~~ . Si K es el cdd de $x^4 - 2 \mid \mathbb{Q}$
 $\Rightarrow K = \mathbb{Q}(\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2})$



Evidente que $\mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2}) \subseteq \mathbb{Q}(i, \sqrt[4]{2})$. Además

$$i = \frac{i\sqrt[4]{2}}{\sqrt[4]{2}} \quad \therefore (\mathbb{Q}(i, \sqrt[4]{2})) \subseteq (\mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2}))$$

$$\therefore (\mathbb{Q}(i, \sqrt[4]{2})) = (\mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2}))$$

Ahora, como $\text{Gal}(K/\mathbb{Q})$ tiene 8 elementos, debemos encontrar 8 automorfismos de K en K .

Aquí

$$\tau\sigma = \sigma^3\tau$$

$$\tau\sigma^2 = (\tau\sigma)\sigma = (\sigma^3\tau)\sigma = \sigma^3(\tau\sigma) = \sigma^7(\sigma^3\tau) = \sigma^6\tau = \sigma^2\tau$$

$$\tau\sigma^3 = (\tau\sigma^2)\sigma = (\sigma^2\tau)\sigma = \sigma^2(\tau\sigma) = \sigma^2(\sigma^3\tau) = \sigma^5\tau = \sigma\tau$$

$$\tau\sigma^4 = (\tau\sigma^3)\sigma = (\sigma\tau)\sigma = \sigma(\tau\sigma) = \sigma(\sigma^3\tau) = \sigma^4\tau = \tau$$

Aquí, $\text{Gal}(K/\mathbb{Q}) = \langle \sigma, \tau \mid \sigma^4 = \tau^2 = 1, \sigma\tau = \tau\sigma^3 \rangle$
 $\cong D_8$ (Simetrías de un cuadrado)

Ejercicio 8. Sea $p(x)$ el polinomio minimal de $\sqrt{2+\sqrt{2}}$

sobre \mathbb{Q} . Encuentre el cuerpo de descomposición de $p(x)$

sobre \mathbb{Q} y el grupo de Galois asociado a esta extensión.

Hallar todos los cuerpos intermedios de la extensión

$$\mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q}$$

Dem. Sea $\alpha = \sqrt{2+\sqrt{2}}$

$$\begin{aligned}\alpha^2 &= 2 + \sqrt{2} \Rightarrow \alpha^2 - 2 = \sqrt{2} / (\)^2 \\ &\Rightarrow \alpha^4 - 4\alpha^2 + 4 = 2 \\ &\Rightarrow \alpha^4 - 4\alpha^2 + 2 = 0\end{aligned}$$

Si $x^4 - 4x^2 + 2$ es irreducible sobre \mathbb{Z} por Eisenstein, luego

por el lema de Gauss, $x^4 - 4x^2 + 2$ irreducible sobre \mathbb{Q} .

$$\therefore p(x) = x^4 - 4x^2 + 2 \quad ([\mathbb{Q}(\sqrt{2+\sqrt{2}}):\mathbb{Q}] = 4)$$

Como $p(\alpha) = 0 \Rightarrow p(-\alpha) = 0 \quad \therefore -\sqrt{2+\sqrt{2}}$ es raíz de
 $x^4 - 4x^2 + 2$

Luego:

$$(x - \sqrt{2+\sqrt{2}})(x + \sqrt{2+\sqrt{2}}) = x^2 - (2+\sqrt{2}) = x^2 - \alpha^2$$

$$x^4 - 4x^2 + 2 : x^2 - \alpha^2 = x^2 + (\alpha^2 - 4)$$

$$\underline{x^4 - \alpha^2 x^2}$$

$$(\alpha^2 - 4) x^2 + 2$$

$$\underline{(\alpha^2 - 4) x^2 - \alpha^2 (\alpha^2 - 4)}$$

$$2 + \alpha^2 (\alpha^2 - 4) = \alpha^4 - 4\alpha^2 + 2 = 0$$

$$x^2 + (\alpha^2 - 4) = x^2 + (2 + \sqrt{2} - 4) = x^2 + (-2 + \sqrt{2})$$

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

$$\therefore x = \pm \sqrt{2 - \sqrt{2}}$$

$$\text{Así: } p(x) = (x - \sqrt{2 + \sqrt{2}})(x + \sqrt{2 + \sqrt{2}})(x - \sqrt{2 - \sqrt{2}})(x + \sqrt{2 - \sqrt{2}})$$

Así, el cuerpo de descomposición K de $p(x) \in \mathbb{Q}[x]$

es ~~$\mathbb{Q}(x)$~~ $K = \mathbb{Q}(\sqrt{2 + \sqrt{2}}, \sqrt{2 - \sqrt{2}})$, donde

$[K : \mathbb{Q}] = 4$ (K/\mathbb{Q} Galoiana!). La cantidad

correcta de automorfismos se consiguen como

$$\begin{cases} \sqrt{2 + \sqrt{2}} \mapsto \pm \sqrt{2 + \sqrt{2}} \\ \sqrt{2 - \sqrt{2}} \mapsto \pm \sqrt{2 - \sqrt{2}} \end{cases}$$

$$\text{Sean } \sigma : \begin{cases} \sqrt{2 + \sqrt{2}} \mapsto -\sqrt{2 + \sqrt{2}} \\ \sqrt{2 - \sqrt{2}} \mapsto \sqrt{2 - \sqrt{2}} \end{cases}$$

$$\tau : \begin{cases} \sqrt{2 + \sqrt{2}} \mapsto \sqrt{2 + \sqrt{2}} \\ \sqrt{2 - \sqrt{2}} \mapsto -\sqrt{2 - \sqrt{2}} \end{cases}$$

Seguiremos con la siguiente

Afirmación. $(\mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q})$ es una extensión cíclica de grado 4.

dem. Basta ver que existe $\sigma \in \text{Gal}(\mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q})$ de orden 4.

Nuestro candidato natural es $\sigma: \sqrt{2+\sqrt{2}} \mapsto \sqrt{2-\sqrt{2}}$.

Antes de eso, se sabe que $\{\sqrt{1}, \sqrt{2}, \sqrt{2+\sqrt{2}}, \sqrt{2-\sqrt{2}}\}$ es una \mathbb{Q} -base de $\mathbb{Q}(\sqrt{2+\sqrt{2}})$. Queremos expresar $\sqrt{2-\sqrt{2}}$ como combinación lineal de estos elementos.

$$\sqrt{2-\sqrt{2}} = \frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}},$$

$$\boxed{\alpha^{-1} = 2\alpha - \frac{1}{2}\alpha^3}$$

pero $\frac{1}{\sqrt{2+\sqrt{2}}}$ se consigue de la siguiente manera,

$$\alpha = \sqrt{2+\sqrt{2}}, \quad \alpha^4 - 4\alpha^2 + 2 = 0 \Rightarrow 1 = \alpha \left(2\alpha - \frac{1}{2}\alpha^3 \right)$$

$$\begin{aligned} \therefore \sqrt{2-\sqrt{2}} &= \frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}} = 2\sqrt{2}\sqrt{2+\sqrt{2}} - \frac{1}{2}\sqrt{2}(2+\sqrt{2})\sqrt{2+\sqrt{2}} \\ &= 2\sqrt{2}\sqrt{2+\sqrt{2}} - \sqrt{2}\sqrt{2+\sqrt{2}} - \sqrt{2+\sqrt{2}} \\ &= (2\sqrt{2}-\sqrt{2}-1)\sqrt{2+\sqrt{2}} = (\sqrt{2}-1)\sqrt{2+\sqrt{2}} \end{aligned}$$

Además, si $\sigma(\sqrt{2+\sqrt{2}}) = \sqrt{2-\sqrt{2}} \Rightarrow \sigma(\sqrt{2}) = -\sqrt{2}$.

Con todo lo anterior podemos calcular el orden de σ ,

(recordar que $\sigma \in \text{Aut}(\mathbb{Q}(\sqrt{2+\sqrt{2}}))$ queda determinado por su acción en $\sqrt{2+\sqrt{2}}$)

$$\sigma(\sqrt{2+\sqrt{2}}) = \sqrt{2-\sqrt{2}} = (\sqrt{2}-1)\sqrt{2+\sqrt{2}}$$

$$\begin{aligned} \sigma^2(\sqrt{2+\sqrt{2}}) &= \sigma(\sqrt{2}-1)(\sqrt{2+\sqrt{2}}) = (-\sqrt{2}-1)(\sqrt{2+\sqrt{2}}) \\ &= (-\sqrt{2}-1)(\sqrt{2}-1)\sqrt{2+\sqrt{2}} = (-2+1)\sqrt{2+\sqrt{2}} = -\sqrt{2+\sqrt{2}} \end{aligned}$$

$$\begin{aligned} \sigma^3(\sqrt{2+\sqrt{2}}) &= -\sigma(\sqrt{2+\sqrt{2}}) = -\sqrt{2-\sqrt{2}} = -(\sqrt{2}-1)\sqrt{2+\sqrt{2}} \\ \sigma^4(\sqrt{2+\sqrt{2}}) &= -(-\sqrt{2}-1)\sqrt{2-\sqrt{2}} = -(-\sqrt{2}-1)(\sqrt{2}-1)\sqrt{2+\sqrt{2}} = \end{aligned}$$

$$= (\sqrt{2}+1)(\sqrt{2}-1) \sqrt{2+\sqrt{2}} = (2-1)\sqrt{2+\sqrt{2}} = \sqrt{2+\sqrt{2}}$$

$$\therefore \sigma^4 = 1$$

Así se tiene que $\text{Gal}(\mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q}) \cong C_4$

• Hallar las extensiones intermedias de $\mathbb{Q}(\sqrt{2+\sqrt{2}})$.

Como $C_4 \cong \mathbb{Z}/4\mathbb{Z}$

$$\begin{array}{c} \mathbb{Z}/4\mathbb{Z} \\ | \\ \langle \bar{2} \rangle \\ | \\ \langle \bar{0} \rangle \end{array}$$

Luego,

$$\mathbb{Q}(\sqrt{2+\sqrt{2}})$$

|

$$\mathbb{Q}(\sqrt{2})$$

|

$$\mathbb{Q}$$

Ejercicio 9. Sea $\zeta_7 = e^{2\pi i/7}$. Sabemos que

$$\text{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q}) \cong (\mathbb{Z}/7\mathbb{Z})^*$$

Sea $H = \langle -1 \rangle \leq (\mathbb{Z}/7\mathbb{Z})^*$. Puede que el cuerpo fijo de H es $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$ y muestre que $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})/\mathbb{Q}$ es Galois con grupo de Galois isomorfo a $\mathbb{Z}/3\mathbb{Z}$.

Dem. $H = \overline{\langle -1 \rangle} = \overline{\langle \bar{6} \rangle}$, como $\bar{6}^2 = \bar{36} = \bar{1}$, tenemos que $H \cong \langle \sigma \rangle$, $\sigma^2 = 1$, $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q})$.

Queremos encontrar $\mathbb{Q}(\zeta_7)^{\langle \sigma \rangle}$, como $1, \zeta, \zeta^2, \dots, \zeta^5$ es una base de $\mathbb{Q}(\zeta_7)$ tenemos que $(\zeta_7 = \zeta) \Leftrightarrow$

$$\lambda \in \mathbb{Q}(\zeta_7) \Leftrightarrow \lambda = a + b\zeta + c\zeta^2 + d\zeta^3 + e\zeta^4 + f\zeta^5$$

$$(\sigma(\zeta) = \zeta^6) \quad \sigma(\lambda) = a + b\zeta^6 + c\zeta^{12} + d\zeta^{18} + e\zeta^{24} + f\zeta^{30}$$

$$\sigma(\lambda) = \lambda \Leftrightarrow a + b\zeta^6 + c\zeta^{12} + d\zeta^{18} + e\zeta^{24} + f\zeta^{30}$$

$$= a + b\zeta + c\zeta^2 + d\zeta^3 + e\zeta^4 + f\zeta^5$$

$$\Leftrightarrow a + b(-1 - \zeta - \zeta^2 - \zeta^3 - \zeta^4 - \zeta^5) + c\zeta^5 + d\zeta^4 + e\zeta^3 + f\zeta^2$$

$$= a + b\zeta + c\zeta^2 + d\zeta^3 + e\zeta^4 + f\zeta^5$$

$$\Leftrightarrow (a - b) + (-b)\zeta + (-b + f)\zeta^2 + (-b + e)\zeta^3 + (-b + d)\zeta^4 + (-b + c)\zeta^5$$

$$= a + b\zeta + c\zeta^2 + d\zeta^3 + e\zeta^4 + f\zeta^5$$

$$\begin{cases} b = 0 \\ c = f \\ d = e \end{cases}$$

$$\therefore \lambda = a + c\zeta^2 + d\zeta^3 + e\zeta^4 + f\zeta^5 = a + c(\zeta^2 + \zeta^5) + d(\zeta^3 + \zeta^4)$$

$$= a + c(\zeta^2 + \zeta^{-2}) + d(\zeta^3 + \zeta^{-3})$$

$$\therefore \mathbb{Q}(\zeta)^{\langle \sigma \rangle} = \mathbb{Q}(\zeta^2 + \zeta^{-2}, \zeta^3 + \zeta^{-3}).$$

Por otro lado, $(\zeta + \zeta^{-1})^2 = \zeta^2 + \zeta^{-2} + 2\zeta\zeta^{-1} = \zeta^2 + \zeta^{-2} + 2,$

$$\begin{aligned} (\zeta + \zeta^{-1})^3 &= \zeta^3 + 3\zeta^2\zeta^{-1} + 3\zeta\zeta^{-2} + \zeta^{-3} \\ &= \zeta^3 + \zeta^{-3} + 3\zeta + 3\zeta^{-1} \\ &= \zeta^3 + \zeta^{-3} + 3(\zeta + \zeta^{-1}) \end{aligned}$$

$$\therefore \zeta^2 + \zeta^{-2} = (\zeta + \zeta^{-1})^2 - 2$$

$$\zeta^3 + \zeta^{-3} = (\zeta + \zeta^{-1})^3 - 3(\zeta + \zeta^{-1})$$

$$= (\zeta + \zeta^{-1})((\zeta + \zeta^{-1})^2 - 3)$$

$$\therefore \zeta + \zeta^{-1} \in \mathbb{Q}(\zeta^2 + \zeta^{-2}, \zeta^3 + \zeta^{-3})$$

$$\therefore \mathbb{Q}(\zeta)^{\langle \sigma \rangle} \cong \mathbb{Q}(\zeta + \zeta^{-1})$$

Por otro lado, $\mathbb{Q}(\zeta + \zeta^{-1})$ Galois $\mathbb{Q} \Leftrightarrow \langle \zeta + \zeta^{-1} \rangle$

$$\langle \zeta + \zeta^{-1} \rangle \trianglelefteq \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \Leftrightarrow \langle \bar{\zeta} \rangle \trianglelefteq (\mathbb{Z}/7\mathbb{Z})^*$$

Como $(\mathbb{Z}/7\mathbb{Z})^* \cong C_6$, C_6 abeliano $\Rightarrow \langle \bar{\zeta} \rangle \trianglelefteq (\mathbb{Z}/7\mathbb{Z})^*$

$\therefore \mathbb{Q}(\zeta + \zeta^{-1})/\mathbb{Q}$ Galosiana.

También, $\text{Gal}(\mathbb{Q}(\zeta + \zeta^{-1})/\mathbb{Q}) \cong \frac{\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})}{\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta^{\sigma}))} \cong \frac{(\mathbb{Z}/7\mathbb{Z})^*}{\langle \sigma \rangle}$

Ap. Si G abeliano $\Rightarrow VH \trianglelefteq G : G/H$ abeliano.

dem. Sean $gH, g'H \in G/H \quad \exists g, g' \in G$

$$(gh)(g'h) = (gg')H = (g'g)H = (g'H)(gh) \quad \text{G abeliano.}$$

i. Con resultado anterior, como $((\mathbb{Z}/7\mathbb{Z})^*)/\langle \sigma \rangle \cong \langle \bar{\zeta} \rangle \cong \langle \zeta + \zeta^{-1} \rangle$ abeliano:
 $\text{Gal}(\mathbb{Q}(\zeta + \zeta^{-1})/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$

Ejercicio 10

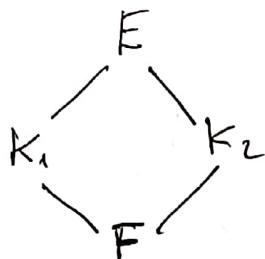
Sea E/F extensión finita de Galois.

(1) Sean K_1, K_2 cuerpos intermedios de E/F con subgrupos respectivos H_1, H_2 en $\text{Gal}(E/F) = G$. Demuestre que si H_1, H_2 son conjugados, entonces $\sigma(K_1) = K_2$, para algún $\sigma \in G$.

(2) Pruebe que lo anterior sucede cuando $[E:F] = 750$, $[K_1:F] = [K_2:F] = 6$.

Demonstración

(1)



Tenemos que $K_1 = E^{H_1}$, $K_2 = E^{H_2}$; donde $H_2 = \sigma H_1 \sigma^{-1}$, para algún $\sigma \in G$. Sea $\tau \in H_2$, $\forall \alpha \in K_2 : \tau(\alpha) = \alpha$.

Pero además existe $\tilde{\tau} \in H_1$, tal que $\tau = \sigma \tilde{\tau} \sigma^{-1}$, así

$$\begin{aligned} \forall \alpha \in K_2 : \tau(\alpha) = \alpha &\Leftrightarrow \sigma \tilde{\tau} \sigma^{-1}(\alpha) = \alpha \\ &\Leftrightarrow \tilde{\tau} \sigma^{-1}(\alpha) = \sigma^{-1}(\alpha) \\ &\Leftrightarrow \tilde{\tau}(\sigma^{-1}(\alpha)) = \sigma^{-1}(\alpha) \end{aligned}$$

Como $\tilde{\tau}$ fija a $\sigma^{-1}(\alpha)$, $\sigma^{-1}(\alpha) \in K_1$

$$\therefore \sigma^{-1}(K_2) \subseteq K_1$$

Falta demostrar que $\sigma^{-1}(K_2) \supseteq K_1$.

Sea $\alpha \in K_1$, $\forall \tau \in H_1 : \tau(\alpha) = \alpha$. Pero $\tau = \sigma^{-1} \hat{\tau} \sigma$, $\hat{\tau} \in H_2$ ya que $\sigma^{-1} H_1 \sigma = H_2$. Así

$$\begin{aligned} \tau(\alpha) = \alpha &\Leftrightarrow (\sigma^{-1} \hat{\tau} \sigma)(\alpha) = \alpha \\ &\Leftrightarrow \hat{\tau}(\sigma(\alpha)) = \sigma(\alpha) \end{aligned}$$

Como $\hat{\tau} \in H_2$ y fija a $\sigma(\alpha) \Rightarrow \sigma(\alpha) \in K_2$

$$\therefore \hat{\tau}(\sigma(\alpha)) \in K_2$$

\therefore ~~que~~ $\alpha = \sigma^{-1}(\hat{\tau}(\sigma(\alpha)))$ ~~esta~~, donde $\hat{\tau}(\sigma(\alpha)) \in K_2$

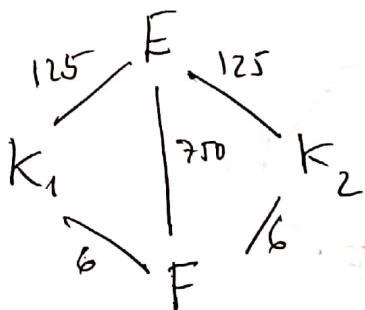
$$\therefore \alpha \in \sigma^{-1}(K_2)$$

$$\therefore \sigma^{-1}(K_2) = K_1$$

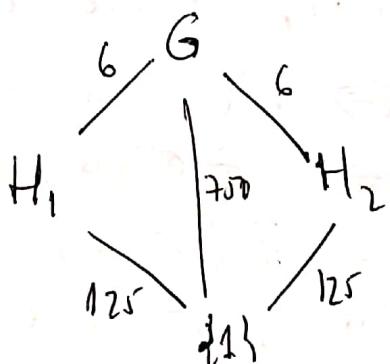
$$\therefore K_1 = \sigma(K_2)$$

$$(2) [E:F] = 750, [K_1:F] = [K_2:F] = 6.$$

Tenemos



* Sea $G = \text{Gal}(E/F)$, $H_1 = \text{Gal}(E/K_1)$, $H_2 = \text{Gal}(E/K_2)$. Así, por 2º Teorema de Galois



Por otro lado, $|G| = 750 = 5^3 \cdot 2 \cdot 3$, $|H_1| = |H_2| = 5^3$, con esto, H_1, H_2 son 5-grupos de Sylow, luego son conjugados, es decir, ~~los~~ $H_1 \cong H_2$

$$\exists \sigma \in G : \sigma H_2 \sigma^{-1} = H_1$$

Extensiones compósito.

Proposición. K/F , F'/F extensiones; K/F Galoisiana.

Entonces KF'/F' es Galoisiana, con

$$\text{Gal}(KF'/F') \cong \text{Gal}(K/F) \cap \text{Gal}(F'/F).$$

Pictóricamente:



Dem. K/F Galoisiana $\Rightarrow K$ cdd de $f(x) \in F[x]$ separable.

Como $K \subset KF'$, $F \subset F'$, KF' es el campo de descomposición de $f(x)$ visto en $F'[x]$.

$\therefore KF'/F'$ Galoisiana

K/F Galois \Rightarrow toda invariación de K que fija F es un automorfismo

$$\therefore \varphi: \text{Gal}(KF'/F') \rightarrow \text{Gal}(K/F)$$

$$\sigma \mapsto \sigma|_K$$

φ es un homomorfismo, donde

$$\ker \varphi = \{\sigma \in \text{Gal}(KF'/F') / \sigma|_K = \text{id} = 1\}$$

Afirmación: φ es inyectiva.

dem. Como $\sigma|_K = 1$, $\sigma|_{F'} = 1 \Rightarrow \sigma|_{KF'} = 1$ (evidente)

\therefore Como $\sigma \in \text{Gal}(KF'/F')$,

$$\therefore \ker \varphi = \{1\}$$

Ahora $\varphi: \text{Gal}(KF'/F') \rightarrow \text{Gal}(K/F)$.

Sea $H = \varphi(\text{Gal}(KF'/F')) \subseteq \text{Gal}(K/F)$.

Consideramos $K^H \subseteq K$. Tenemos que σ fija a F' y $\sigma|_K \in H \Rightarrow F' \cap K^H \subseteq K^H$

Falta demostrar que $K^H \subseteq F' \cap K$.

Afirmación: $K^H F'$ queda fijo por $\text{Gal}(KF'/F')$

dem: $\forall \sigma \in \text{Gal}(KF'/F')$ fija F' y $\sigma|_K$ fija a K^H por definición, ya que $\sigma|_K \in H$.

$\therefore \sigma$ fija a $K^H F'$

Por el segundo teorema fundamental de la Teoría de Galois,

$$K^H F' = F' \quad \therefore K^H \subseteq F'$$

Pero además $K^H \subseteq K \quad \therefore K^H \subseteq F' \cap K$

$$\therefore K^H = F' \cap K$$

Por segundo Teo. de Galois: $H \cong \text{Gal}(K/K^H) \cong \text{Gal}(K/K \cap F')$

$$\therefore \text{Gal}(KF'/F') \cong \text{Gal}(K/K \cap F')$$

Corolario: Si K/F Galoisiana y F'/F pura. Entonces

$$[KF':F] = \frac{[K:F][F':F]}{[K \cap F':F]}$$

dem:

$\begin{array}{c} K \\ \diagdown \quad \diagup \\ K \quad F' \\ \diagup \quad \diagdown \\ K \cap F' \end{array}$

$$[KF':F] = [KF':F'][F':F]$$
$$= [K:K \cap F'][F':F]$$
$$= \frac{[K:F][F':F]}{[K \cap F':F]}$$

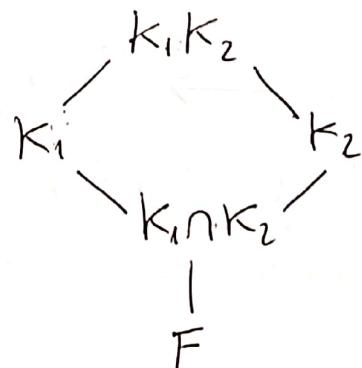
Proposición. K_1, K_2 Galoianas sobre F . Entonces

(1) $K_1 \cap K_2$ es Galoiana sobre F

(2) $K_1 K_2$ es Galoiana sobre F . Donde si $H = \text{Gal}(K_1 K_2 / F)$,

$$H = \{(\sigma, \tau) \mid \sigma|_{K_1 \cap K_2} = \tau|_{K_1 \cap K_2}\}$$

$$H \leq \text{Gal}(K_1 / F) \times \text{Gal}(K_2 / F).$$



~~dem.~~ (1) Sea $p(x) \in F[x]$ irreducible, sobre F , donde K_1 es un cuerpo de descomposición. Supongamos que $\alpha \in K_1 \cap K_2$, como $K_1 \cap K_2 \subset K_1$, todas las raíces de $p(x)$ están en K_1 . Pero como $\alpha \in K_1 \cap K_2 \Rightarrow \alpha \in K_2$ y K_2 / F Galoiana, todas las raíces de

Sea $p(x) \in F[x]$ irreducible y $\alpha \in K_1 \cap K_2$ una raíz de $p(x)$. Como $K_1 \cap K_2 \subset K_1$ y K_1 / F Galoiana, $p(x)$ se descompone completamente ~~sobre~~ en K_1 (además $p(x)$ debe ser separable). Análogamente, $p(x)$ se factoriza en K_2

$\therefore p(x)$ se factoriza ~~sobre~~ en $K_1 \cap K_2$

$\therefore K_1 \cap K_2 / F$ Galoiana!

(2) Si K_1 es el cuerpo de descomposición de $f_1(x) \in F[x]$, y K_2 cdd de $f_2(x) \in F[x]$ (ambas separables), entonces $f_1(x) f_2(x)$ se factorizan en K_1 y K_2 resp. Ahora, $K_1 K_2$ es el cdd

de la parte libre de cuadrados de $f_1(x), f_2(x)$
 $(f_1(x), f_2(x))$ podrían tener factores comunes, pero de a uno
 a la vez). Notar que $f_1(x), f_2(x)$ con su parte libre de \square 's
 sigue siendo separable.

$\therefore K_1 K_2 / F$ Galoisiana.

Consideremos la aplicación:

$$\varphi: \text{Gal}(K_1 K_2 / F) \longrightarrow \text{Gal}(K_1 / F) \times \text{Gal}(K_2 / F)$$

$$\sigma \mapsto (\sigma|_{K_1}, \sigma|_{K_2})$$

es claramente un homomorfismo (proposición anterior).

Además

$$\ker \varphi = \{\text{id}\}$$

$$= \{\sigma \in \text{Gal}(K_1 K_2 / F) \mid \sigma|_{K_1}, \sigma|_{K_2} = 1_{K_1, K_2}\}$$

$$= \{\sigma \in \text{Gal}(K_1 K_2 / F) \mid \sigma|_{K_1 \cap K_2} = 1_{K_1 \cap K_2}\}$$

$$= \{\sigma \in \text{Gal}(K_1 K_2 / F) \mid \sigma|_{K_1 K_2} = 1_{K_1 K_2}\}$$

$$= \{1\}$$

$$\therefore \ker \varphi = \{1\}$$

$\therefore \varphi$ monomorfiaco.

Como $\varphi(\text{Gal}(K_1 K_2 / F)) = H \leq \text{Gal}(K_1 / F) \times \text{Gal}(K_2 / F)$

y $\text{Gal}(K_1 K_2 / F) \cong H$, sólo debemos calcular H .

$$H = \{ \varphi(\sigma) \mid \sigma \in \text{Gal}(K_1 K_2 / F) \}$$

$$= \{ (\sigma|_{K_1}, \sigma|_{K_2}) \mid \sigma \in \text{Gal}(K_1 K_2 / F) \}$$

Como φ es un monomorfismo, $\text{Gal}(K_1 K_2 / F) \cong \varphi(\text{Gal}(K_1 K_2 / F))$
 $\leq H \leq \text{Gal}(K_1 / F) \times \text{Gal}(K_2 / F)$, así

$|\text{Gal}(K_1 K_2 / F)| \leq |H|$. Luego sólo basta comprobar que
 $|\text{Gal}(K_1 K_2 / F)| = |H|$. A notar lo siguiente:

$$(\sigma|_{K_1})|_{K_1 \cap K_2} = \sigma|_{K_1 \cap K_2} = (\sigma|_{K_2})|_{K_1 \cap K_2}$$

$|H|$ se puede calcular observando que $\forall \sigma \in \text{Gal}(K_1 / F)$, existen
 $|\text{Gal}(K_2 / K_1 \cap K_2)|$ elementos $\tau \in \text{Gal}(K_2 / F)$ tal que
 $\tau|_{K_1 \cap K_2} = \sigma|_{K_1 \cap K_2}$. Por lo tanto

$$\begin{aligned} |H| &= |\text{Gal}(K_1 / F)| \cdot |\text{Gal}(K_2 / K_1 \cap K_2)| \\ &= |\text{Gal}(K_1 / F)| \cdot \frac{|\text{Gal}(K_2 / F)|}{|\text{Gal}(K_1 \cap K_2 / F)|} \\ &= \frac{[K_1 : F][K_2 : F]}{[K_1 \cap K_2 : F]} \\ &= [K_1 K_2 : F] \\ &= |\text{Gal}(K_1 K_2 / F)| \\ \therefore |\text{Gal}(K_1 K_2 / F)| &= |H| \end{aligned}$$

Así se concluye que $H \cong \text{Gal}(K_1 K_2 / F)$.

Corolario. Sean K_1, K_2 Galoianas sobre F , con $K_1 \cap K_2 = F$.

Entonces

$$\text{Gal}(K_1 K_2 / F) \cong \text{Gal}(K_1 / F) \times \text{Gal}(K_2 / F)$$

Conversamente, si K es Galois sobre F y $G = \text{Gal}(K/F) = G_1 \times G_2$ (producto directo de G_1 y G_2), entonces

$K = K_1 K_2$, donde $K_1 / F, K_2 / F$ Galoianas y $K_1 \cap K_2 = F$.

dem. (\Rightarrow) Acabamos de demostrar que

$$[K_1 K_2 : F] = \frac{[K_1 : F][K_2 : F]}{[K_1 \cap K_2 : F]}$$

cuando $K_1 / F, K_2 / F$ Galoianas.

$$\therefore |\text{Gal}(K_1 K_2 / F)| = \frac{|\text{Gal}(K_1 : F)| |\text{Gal}(K_2 : F)|}{|\text{Gal}(K_1 \cap K_2 / F)|}$$

Pero como $K_1 \cap K_2 = F \Rightarrow \text{Gal}(K_1 \cap K_2 / F) = 1$

y $\text{Gal}(K_1 K_2 / F) \hookrightarrow \text{Gal}(K_1 / F) \times \text{Gal}(K_2 / F)$

$$\therefore \text{Gal}(K_1 K_2 / F) \cong \text{Gal}(K_1 / F) \times \text{Gal}(K_2 / F).$$

(\Leftarrow) Sea K_1 el cuerpo fijo por G_1 , K_2 cuerpo fijo por G_2 (~~porque G_1, G_2 son grupos de Galois~~). Por el segundo teorema fundamental de la teoría de Galois,

$K_1 \cap K_2$ es el cuerpo fijo por $G_1 G_2$, ~~que es todo G~~

pero $(G_1, G_2 \subset G)$, pero $G_1 G_2 \neq$ todo G , luego por

2º Teo de Galois:

$$K_1 \cap K_2 = F$$

También, $K_1 K_2$ ~~es un campo~~ están en correspondencia con $G_1 \cap G_2$, pero $G_1 \cap G_2 = 1$ $\therefore K_1 K_2 = K$

Classement K_1/F , K_2/F non Galoisianas lorsque
 $G_1, G_2 \triangleleft G$.

SEPTIEMBRE, 2014

EJERCICIO 1. Sea $p(x)$ el polinomio minimal de $\sqrt{2 + \sqrt{2}}$ sobre \mathbb{Q} . Encuentre el cuerpo de descomposición de $p(x)$ sobre \mathbb{Q} y el grupo de Galois asociado a esta extensión.

EJERCICIO 2. Calcule el grupo de Galois de $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q}$.

EJERCICIO 3. Para p primo determine los elementos del grupo de Galois de $x^p - 2$.

EJERCICIO 4. Determine todos los subcuerpos del cuerpo de descomposición de $x^8 - 2$ que son Galois sobre \mathbb{Q} .

EJERCICIO 5. Determine el grupo de Galois del cuerpo de descomposición de $x^4 - 14x^2 + 9$ sobre \mathbb{Q} .

EJERCICIO 6. Pruebe que si el grupo de Galois del cuerpo de descomposición de un polinomio cúbico sobre \mathbb{Q} es el grupo cíclico de orden 3, entonces todas las raíces de la cónica son reales.

EJERCICIO 7. (Extensiones Bicuadráticas) Sea F un cuerpo de característica $\neq 2$.

1. Si $K = F(\sqrt{D_1}, \sqrt{D_2})$ donde $D_1, D_2 \in F$ tienen la propiedad que ninguno de $D_1, D_2, D_1 D_2$ es un cuadrado en F , entonces K/F es extensión de Galois con $\text{Gal}(K/F)$ isomorfo al grupo 4 de Klein.
2. Recíprocamente, suponga que K/F es extensión de Galois con $\text{Gal}(K/F)$ isomorfo al grupo 4 de Klein. Pruebe que $K = F(\sqrt{D_1}, \sqrt{D_2})$ donde $D_1, D_2 \in F$ tienen la propiedad de que ninguno de $D_1, D_2, D_1 D_2$ es un cuadrado en F .

EJERCICIO 8. Sea K/F una extensión finita y sea $\alpha \in K$. Sea L extensión de Galois de F que contiene K y sea $H \leq \text{Gal}(L/F)$ el subgrupo correspondiente a K . Definir la traza de α desde K a F como

$$\text{Tr}_{K/F}(\alpha) = \sum_{\sigma} \sigma(\alpha),$$

donde la suma se toma sobre todas las incrustaciones de K en una clausura algebraica de F . Utilice la independencia lineal de caracteres para mostrar que para cualquier extensión K de F existe un elemento $\alpha \in K$ con $\text{Tr}_{K/F}(\alpha) \neq 0$.

EJERCICIO 9. Determine el grupo de Galois de cada polinomio sobre los cuerpos indicados:

1. $x^4 - 5$ sobre \mathbb{Q} , sobre $\mathbb{Q}(\sqrt{5})$ y sobre $\mathbb{Q}(\sqrt{-5})$.
2. $x^3 - x - 1$ sobre \mathbb{Q} .
3. $x^3 - 10$ sobre \mathbb{Q} y sobre $\mathbb{Q}(\sqrt{2})$.
4. $x^5 - 6x + 3$ sobre \mathbb{Q} .

EJERCICIO 10. Sea $f \in \mathbb{Q}[x]$ un polinomio mónico irreducible de grado primo p con exactamente dos raíces no reales, y sea K el cuerpo de descomposición de f sobre \mathbb{Q} . Demuestre que $\text{Gal}(K/\mathbb{Q})$ es isomorfo a un subgrupo de S_p que contiene una transposición, por lo tanto, es isomorfo a S_p (por transitividad).

EJERCICIO 11. Sea K/F una extensión galoisiana con grupo G y sea

$$E := \{x \in K : \sigma\tau(x) = \tau\sigma(x), \forall \sigma, \tau \in G\}.$$

Demuestre que E/F es Galois y que su grupo es abeliano.

Ejercicio 1. Sea $p(x)$ el polinomio minimal de $\sqrt{2+\sqrt{2}}$ sobre \mathbb{Q} . Encuentre el anexo de descomposición de $p(x)$ sobre \mathbb{Q} y el grupo de Galois asociado a esta extensión.

Dem. $p(x) \in \mathbb{Q}[x]$, $p(x) = m_{\alpha, \mathbb{Q}}(x)$ donde $\alpha = \sqrt{2+\sqrt{2}}$

$$\alpha = \sqrt{2+\sqrt{2}} \Rightarrow \alpha^2 = 2+\sqrt{2}$$

$$\Rightarrow \alpha^2 - 2 = \sqrt{2}$$

$$\Rightarrow \alpha^4 - 4\alpha^2 + 4 = 2 \Rightarrow \alpha^4 - 4\alpha^2 + 2 = 0$$

Como $x^4 - 4x^2 + 2 \in \mathbb{Q}[x]$ irreducible por Eisenstein (sobre \mathbb{Z}_2), se tiene que $p(x) = x^4 - 4x^2 + 2 = m_{\alpha, \mathbb{Q}}(x)$.

Por otro lado: $p(\alpha) = 0 \Rightarrow p(-\alpha) = 0$.

$\therefore (x-\alpha)(x+\alpha)$ divide $p(x)$

$$(x - \sqrt{2+\sqrt{2}})(x + \sqrt{2+\sqrt{2}})$$

~~$$(x - \sqrt{2+\sqrt{2}})(x + \sqrt{2+\sqrt{2}}) = x^2 - (2+\sqrt{2})$$~~

$$x^4 - 4x^2 + 2 : x^2 - (2+\sqrt{2}) = x^2 + (-2+\sqrt{2})$$

$$x^2 - (2+\sqrt{2})x^2$$

$$\underline{(2+\sqrt{2})x^2 - 4x^2 + 2}$$

$$\underline{(-2+\sqrt{2})x^2 + 2}$$

~~$$\underline{\underline{(-2+\sqrt{2})x^2 - (2-4)}}$$~~

$$\underline{2 + (-2)} = 0$$

$$\therefore x^4 - 4x^2 + 2 = (x^2 - (2+\sqrt{2}))(x^2 + \sqrt{2+\sqrt{2}})$$

$$\therefore \text{Si } K \text{ es cdd de } p(x) / \mathbb{Q} \Rightarrow K = \mathbb{Q}(\sqrt{2+\sqrt{2}}, -\sqrt{2+\sqrt{2}}, \sqrt{2-\sqrt{2}}, \sqrt{2-\sqrt{2}})$$

$$= \mathbb{Q}(\sqrt{2+\sqrt{2}}, \sqrt{2-\sqrt{2}})$$

Por problema 7 (Lista de ejercicios 8), $\text{Gal}(K/\mathbb{Q}) \cong V_4 \cong C_2 \times C_2$