

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

Desarrollo

Como  $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$  es el cdd de  $p(x) = (x^2 - 2)(x^2 - 3)(x^2 - 5)$ ,  $K/\mathbb{Q}$  Galoisiana ( $|Gal(K/\mathbb{Q})| = [K:\mathbb{Q}]$ ).

Se sabe que  $p(\alpha) = 0 \Rightarrow p(\sigma(\alpha)) = 0 \quad \forall \sigma \in Aut(K) = Aut_{\mathbb{Q}}(K)$   
 $= Gal(K/\mathbb{Q})$

De esta manera, contamos los elementos de  $Gal(K/\mathbb{Q})$ .

Como  $2 = \sigma(2) = \sigma(\sqrt{2})^2 \quad \therefore \sigma(\sqrt{2}) \in \{\sqrt{2}, -\sqrt{2}\}$   
 Análogamente,  $\sigma(\sqrt{3}) \in \{\sqrt{3}, -\sqrt{3}\}$ ,  $\sigma(\sqrt{5}) \in \{\sqrt{5}, -\sqrt{5}\}$ .

Cada automorfismo queda determinado por la acción en sus generadores  $(\sqrt{2}, \sqrt{3}, \sqrt{5})$ .

Luego:

$$\sigma_1 : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \\ \sqrt{5} \mapsto \sqrt{5} \end{cases}$$

$$\sigma_1 : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \\ \sqrt{5} \mapsto -\sqrt{5} \end{cases}$$

$$\sigma_2 : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \\ \sqrt{5} \mapsto \sqrt{5} \end{cases}$$

$$\sigma_3 : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \\ \sqrt{5} \mapsto -\sqrt{5} \end{cases}$$

$$\sigma_4 : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \\ \sqrt{5} \mapsto \sqrt{5} \end{cases}$$

$$\sigma_5 : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \\ \sqrt{5} \mapsto -\sqrt{5} \end{cases}$$

$$\sigma_6 : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \\ \sqrt{5} \mapsto \sqrt{5} \end{cases}$$

$$\sigma_7 : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \\ \sqrt{5} \mapsto -\sqrt{5} \end{cases}$$

$$\therefore |Gal(K/\mathbb{Q})| = 8$$

Notar que  $\sigma_i \cdot 1 = \sigma_i \quad \forall i = 1, \dots, 7$

$$\sigma_1 \sigma_2 = \sigma_2 \sigma_1 : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \\ \sqrt{5} \mapsto -\sqrt{5} \end{cases} \quad \therefore \sigma_1 \sigma_2 = \sigma_3$$

$$\sigma_1 \sigma_3 = \sigma_3 \sigma_1 : \left\{ \begin{array}{l} \sqrt{2} \longleftrightarrow \sqrt{2} \\ \sqrt{3} \longleftrightarrow -\sqrt{3} \\ \sqrt{5} \longleftrightarrow \sqrt{5} \end{array} \right. , \quad \sigma_1 \sigma_3 = \sigma_2$$

$$\sigma_1 \sigma_4 = \sigma_4 \sigma_1 : \left\{ \begin{array}{l} \sqrt{2} \longleftrightarrow -\sqrt{2} \\ \sqrt{3} \longleftrightarrow \sqrt{3} \\ \sqrt{5} \longleftrightarrow -\sqrt{5} \end{array} \right. , \quad \sigma_1 \sigma_4 = \sigma_5$$

• etc (Los demás se hacen de forma análoga)  
 Además,  $\sigma_1^2 = \sigma_2^2 = \sigma_4^2 = 1$

$$\therefore \text{Gal}(K/\mathbb{Q}) = C_2 \times C_2 \times C_2$$

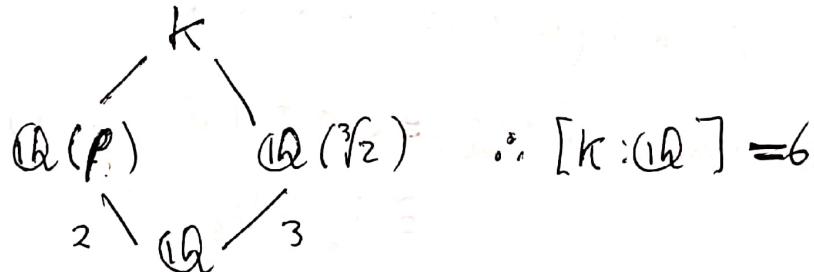
Ejercicio 3. Para  $p$  primo, determine los elementos del grupo de Galois de  $x^p - 2$

Dem. Vamos a realizar ejemplos específicos para así obtener intuición.

$$p=2 : \text{Gal}(K/\mathbb{Q}) = C_2, \text{ donde } K = \mathbb{Q}(\sqrt{2})$$

$$p=3 : \text{Tenemos } x^3 - 2 = p(x) \text{ (irred)} |_{\mathbb{Q}} \text{ por Eisenstein}$$

$$\text{Si } K \text{ cdd de } p(x) \Rightarrow K = \mathbb{Q}(\sqrt[3]{2}, \rho) (\rho = e^{2\pi i/3})$$



Como  $K$  cdd de  $p(x) \Rightarrow K/\mathbb{Q}$  Galois  $\wedge [K:\mathbb{Q}] = |\text{Gal}(K/\mathbb{Q})| = 6$ . Como cada  $\sigma \in \text{Gal}(K/\mathbb{Q})$  define una permutación sobre los raíces de  $p(x)$  (con 3),

$$G = \text{Gal}(K/\mathbb{Q}) \hookrightarrow S_3 \cong D_6$$

$$\text{pero } |G| = |S_3| = 6 \quad \therefore G \cong S_3 \cong D_6$$

Otra manera es encontrando explícitamente los automorfismos  
 ~~$K \rightarrow K$~~  (son 6).

$$\sigma: \begin{cases} {}^3\sqrt{2} \mapsto \rho {}^3\sqrt{2} \\ \rho \mapsto \rho \end{cases}, \quad \tau: \begin{cases} {}^3\sqrt{2} \mapsto {}^3\sqrt{2} \\ \rho \mapsto \rho^2 = -1 - \rho \end{cases}$$

$$\text{Notar que } \sigma^2({}^3\sqrt{2}) = \sigma(\rho {}^3\sqrt{2}) = \rho^2 {}^3\sqrt{2},$$

$$\sigma^3({}^3\sqrt{2}) = \sigma(\rho^2 {}^3\sqrt{2}) = \rho^2 \rho {}^3\sqrt{2} = \rho^3 {}^3\sqrt{2} = {}^3\sqrt{2}$$

$$\tau^2(\rho) = \tau(\rho^2) = \cancel{\rho^4} = \rho^3 \rho = \rho$$

$$\therefore \sigma^3 = \tau^2 = 1$$

$$\sigma\tau: \begin{cases} {}^3\sqrt{2} \mapsto \rho {}^3\sqrt{2} \\ \rho \mapsto \rho^2 \end{cases}, \quad \tau\sigma: \begin{cases} {}^3\sqrt{2} \mapsto \rho^2 {}^3\sqrt{2} \\ \rho \mapsto \rho^2 \end{cases}$$

$$\sigma^2\tau: \begin{cases} {}^3\sqrt{2} \mapsto \rho^2 {}^3\sqrt{2} \\ \rho \mapsto \rho^2 \end{cases}, \quad \tau\sigma^2: \begin{cases} {}^3\sqrt{2} \mapsto \rho {}^3\sqrt{2} \\ \rho \mapsto \rho^2 \end{cases}$$

$$\therefore \text{Gal}(K/\mathbb{Q}) = \{1, \sigma, \tau, \sigma^2, \sigma\tau, \tau\sigma, \sigma^2\tau, \tau\sigma^2\}$$

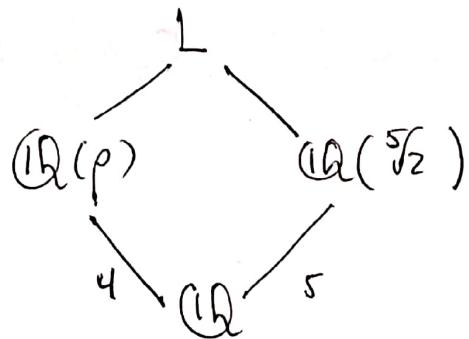
$$\text{pero } \sigma^2\tau = \tau\sigma, \quad \sigma\tau = \tau\sigma^2$$

$$\therefore \text{Gal}(K/\mathbb{Q}) = \{1, \sigma, \tau, \sigma^2, \sigma\tau, \tau\sigma\}$$

$$\text{O. tambien } \text{Gal}(K/\mathbb{Q}) = \langle \sigma, \tau \mid \sigma^3 = \tau^2 = 1, \sigma\tau = \tau\sigma^2 \rangle$$

$$\cong D_6 \cong S_3$$

$$\cdot p=5 : \quad x^5 - 2, \quad \rho = e^{2\pi i/5}$$



L cuerpo de descomposición de  $x^5 - 2 = p(x) \in \mathbb{Q}[x]$ .  
 $L/\mathbb{Q}$  Galoiana, con  $|\text{Gal}(L/\mathbb{Q})| = 20$

$$\text{Teneemos: } \sigma : \begin{cases} p \mapsto p^2 \\ \sqrt[5]{2} \mapsto \sqrt[5]{2} \end{cases}, \quad \tau : \begin{cases} p \mapsto p \\ \sqrt[5]{2} \mapsto p\sqrt[5]{2} \end{cases}$$

$$\text{Afirmación: } \sigma^4 = \tau^5 = \text{id}$$

$$\begin{aligned} \sigma^4(p) &= \sigma^3(p^2) = \sigma^2(p^4) = \sigma(p^8) = p^{16} = p^{15}p \\ &= (p^5)^3 p = 1 \cdot p = p \end{aligned}$$

~~$\tau^4(p) = \tau^3(p\sqrt[5]{2}) = \tau^2(p) \tau^2(\sqrt[5]{2}) = p \tau^2(p\sqrt[5]{2}) =$~~

$$\begin{aligned} \tau^4(\sqrt[5]{2}) &= \tau^3(p\sqrt[5]{2}) = \tau^2(p) \tau^2(\sqrt[5]{2}) = p \tau^2(p\sqrt[5]{2}) = \\ &= p \tau^2(p) \tau^2(\sqrt[5]{2}) = p^2 \tau^2(\sqrt[5]{2}) = p^2 \tau(p\sqrt[5]{2}) \\ &= p^3 \tau(\sqrt[5]{2}) = p^4 \sqrt[5]{2} \end{aligned}$$

$$\tau^5(\sqrt[5]{2}) = \tau(p^4 \sqrt[5]{2}) = p^5 \sqrt[5]{2} = \sqrt[5]{2}$$

También se cumple que

$$\sigma\tau(p) = \sigma(p) = p^2$$

$$\sigma\tau(\sqrt[5]{2}) = \sigma(p\sqrt[5]{2}) = p^2\sqrt[5]{2}$$

$$\tau^r\sigma(p) = \tau(p^2) = p^2$$

$$\tau^r\sigma(\sqrt[5]{2}) = \tau(p\sqrt[5]{2}) = p^r\sqrt[5]{2}$$

$$\begin{aligned} \sigma\tau^r(p) &= \sigma(p) = p^2 \\ \sigma\tau^r(\sqrt[5]{2}) &= \sigma(p^r\sqrt[5]{2}) = p^{2r}\sqrt[5]{2} \\ \tau^{2r}\sigma(p) &= \tau^{2r}(p^2) = p^2 \\ \tau^{2r}\sigma(\sqrt[5]{2}) &= \tau^{2r}(\sqrt[5]{2}) = p^{2r}\sqrt[5]{2} \\ \therefore \sigma\tau^r &= \tau^{2r}\sigma \end{aligned}$$

• Sea  $G$  grupo de orden 20.

Si  $G$  es abeliano :  $G \in \{C_{20}, C_4 \times C_5\}$

Anexo : (Cuerpo de descomposición de  $x^8 - 2$ )

Si  $K$  es el cdd de  $x^8 - 2 \in \mathbb{Q}[x] \Rightarrow K = \mathbb{Q}(\sqrt[8]{2}, \zeta)$  ( $\zeta = \zeta_8$ ).

Afirmación :  $\mathbb{Q}(\zeta) = \mathbb{Q}(i, \sqrt{2})$

dem.  $\zeta = e^{2\pi i/8} = e^{\pi i/4} = \cos\left(\frac{\pi}{4}\right) + i \sin\left(\frac{\pi}{4}\right)$   
 $= \frac{\sqrt{2}}{2} + i \frac{\sqrt{2}}{2}$

$$\therefore \mathbb{Q}(\zeta) = \mathbb{Q}\left(\frac{\sqrt{2}}{2} + i \frac{\sqrt{2}}{2}\right) = \mathbb{Q}(\sqrt{2} + i\sqrt{2})$$

Evidente que  $\mathbb{Q}(\sqrt{2} + i\sqrt{2}) \subseteq \mathbb{Q}(i, \sqrt{2})$ . Ahora,

$$(\sqrt{2} + i\sqrt{2})^2 = 2(i+1)^2 = 2(-1+1+2i) = 4i \quad \therefore i \in \mathbb{Q}(\sqrt{2} + i\sqrt{2})$$

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

$$\therefore i\sqrt{2} \in \mathbb{Q}(\sqrt{2} + i\sqrt{2})$$

$$\therefore \sqrt{2} \in \mathbb{Q}(\sqrt{2} + i\sqrt{2})$$

Así,  $\mathbb{Q}(\zeta) = \mathbb{Q}(i, \sqrt{2})$ .

Afirmación /  $\mathbb{Q}(\zeta) = \mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(\theta, i)$

Donde  $\theta = \sqrt[8]{2}$

~~Dem~~ Tenemos que  $\theta^4 = \sqrt{2} \in \mathbb{Q}(\theta, i)$   $\therefore \mathbb{Q}(i, \sqrt{2}) \subseteq \mathbb{Q}(\theta, i)$

~~Por otro lado~~  $\mathbb{Q}(\theta)$  tiene grado 8 y  $\not\subseteq \mathbb{Q}(i)$

~~(ya que  $\mathbb{Q}(\theta) \subseteq \mathbb{R}$ )~~

~~∴ tiene grado 2 sobre  $\mathbb{Q}(\theta)$~~

~~Así,  $\mathbb{Q}(\theta, i)$  tiene grado 16 sobre  $\mathbb{Q}$~~

~~Con todo lo anterior se tiene que~~

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

$(\mathbb{Q}(\sqrt[8]{2}, i))$  tiene grado 16 sobre  $\mathbb{Q}$ . En efecto,  
 $(\mathbb{Q}(\sqrt[8]{2}))/\mathbb{Q}$  tiene grado 8 ( $x^8 - 2$  irreducible por Eisenstein),  
y como  $(\mathbb{Q}(\sqrt[8]{2})) \subseteq \mathbb{R} \Rightarrow i \notin (\mathbb{Q}(\sqrt[8]{2}))$

$$\therefore x^2 + 1 \text{ irreducible en } \mathbb{Q}(\sqrt[8]{2})$$

$$\therefore (\mathbb{Q}(\sqrt[8]{2}, i))/\mathbb{Q} \text{ tiene grado 16.}$$

Ahora debemos encontrar  $\text{Gal}(K/\mathbb{Q})$ . Como los elementos de  $\text{Gal}(K/\mathbb{Q})$  quedan bien determinados según su acción en los generadores (y tenemos las representaciones de  $K$  como  $(\mathbb{Q}(\zeta, \sqrt[8]{2}), \mathbb{Q}(\sqrt[8]{2}, i), \mathbb{Q}(\sqrt[8]{2}, i)$ ) podemos escoger

$$\begin{cases} \theta \mapsto \zeta^\alpha \theta & , \alpha = 0, 1, 2, \dots, 7 \\ i \mapsto \pm i \end{cases}$$

lo que justo nos da 16 automorfismos! (Recordar que  $K/\mathbb{Q}$  es Galoisiana).

Definimos los automorfismos

$$\sigma: \begin{cases} \theta \mapsto \zeta \theta \\ i \mapsto i \end{cases}, \quad \tau: \begin{cases} \theta \mapsto \theta \\ i \mapsto -i \end{cases}$$

( $\tau$  es la conjugación compleja). Notemos que

$$\zeta = \frac{\sqrt{2}}{2} + i \frac{\sqrt{2}}{2} = \frac{1}{2}(1+i)\sqrt{2} = \frac{1}{2}(1+i)\theta^4 \quad (\theta = \sqrt[8]{2})$$

Por lo tanto tenemos

$$\sigma: \begin{cases} \theta \mapsto \zeta \theta \\ i \mapsto i \\ \zeta \mapsto \zeta^5 = -\zeta \end{cases}$$

$$(x^8 - 1 = (x^4 - 1)(x^4 + 1))$$

$$\begin{aligned} \sigma(\zeta) &= \frac{1}{2}(1+\sigma(i))\sigma(\theta)^4 \\ &= \frac{1}{2}(1+i)(\zeta \theta)^4 \\ &= \frac{1}{2}(1+i)\theta^4 \zeta^4 \\ &= \zeta \cdot \zeta^4 = \zeta^5 \end{aligned}$$

$$\tau\sigma : \begin{cases} \theta \mapsto \zeta^3\theta \\ i \mapsto -i \\ \zeta \mapsto \zeta^3 \end{cases}$$

$$\tau\sigma^5 : \begin{cases} \theta \mapsto \zeta^3\theta \\ i \mapsto -i \\ \zeta \mapsto \zeta^3 \end{cases}$$

$$\tau\sigma^2 : \begin{cases} \theta \mapsto \zeta^2\theta \\ i \mapsto -i \\ \zeta \mapsto \zeta^7 \end{cases}$$

$$\tau\sigma^6 : \begin{cases} \theta \mapsto \zeta^6\theta \\ i \mapsto -i \\ \zeta \mapsto \zeta^7 \end{cases}$$

$$\tau\sigma^3 : \begin{cases} \theta \mapsto \zeta\theta \\ i \mapsto -i \\ \zeta \mapsto \zeta^3 \end{cases}$$

$$\tau\sigma^7 : \begin{cases} \theta \mapsto \zeta^5\theta \\ i \mapsto -i \\ \zeta \mapsto \zeta^3 \end{cases}$$

$$\tau\sigma^4 : \begin{cases} \theta \mapsto -\theta \\ i \mapsto -i \\ \zeta \mapsto \zeta^7 \end{cases}$$

$$\therefore \sigma^8 = \tau^2 = 1$$

También debemos calcular  $\sigma\tau$

$$\sigma\tau : \begin{cases} \theta \mapsto \zeta\theta \\ i \mapsto -i \\ \zeta \mapsto \zeta^3 \end{cases}$$

$$\text{pero } \sigma\tau = \tau\sigma^3. \quad Ax$$

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

$$\sigma^3\tau = \sigma(\sigma^2\tau) = \sigma(\tau\sigma^6) = (\sigma\tau)\sigma^6 = (\tau\sigma^3)\sigma^6 = \tau\sigma^9 = \tau\sigma$$

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

$$\sigma^5\tau = \sigma(\sigma^4\tau) = \sigma(\tau\sigma^4) = (\sigma\tau)\sigma^4 = (\tau\sigma^3)\sigma^4 = \tau\sigma^7$$

$$\sigma^6\tau = \sigma(\sigma^5\tau) = \sigma(\tau\sigma^7) = (\sigma\tau)\sigma^7 = (\tau\sigma^3)\sigma^7 = \tau\sigma^{10} = \tau\sigma^2$$

$$\sigma^7\tau = \sigma(\sigma^6\tau) = \sigma(\tau\sigma^2) = (\sigma\tau)\sigma^2 = (\tau\sigma^3)\sigma^2 = \tau\sigma^5$$

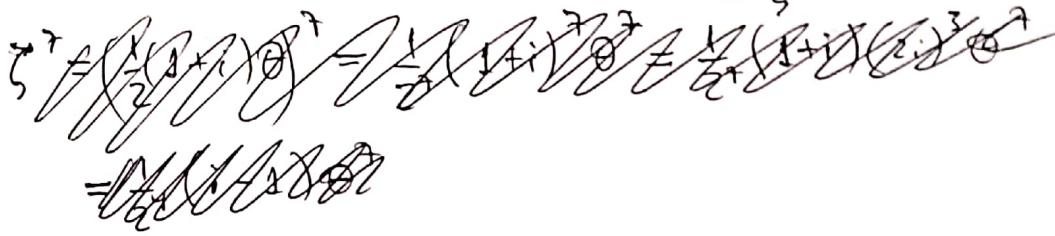
Ax' tenemos que

$$G = Gal(k/\mathbb{Q}) = \langle \sigma, \tau / \sigma^8 = \tau^2 = 1, \sigma\tau = \tau\sigma^3 \rangle$$

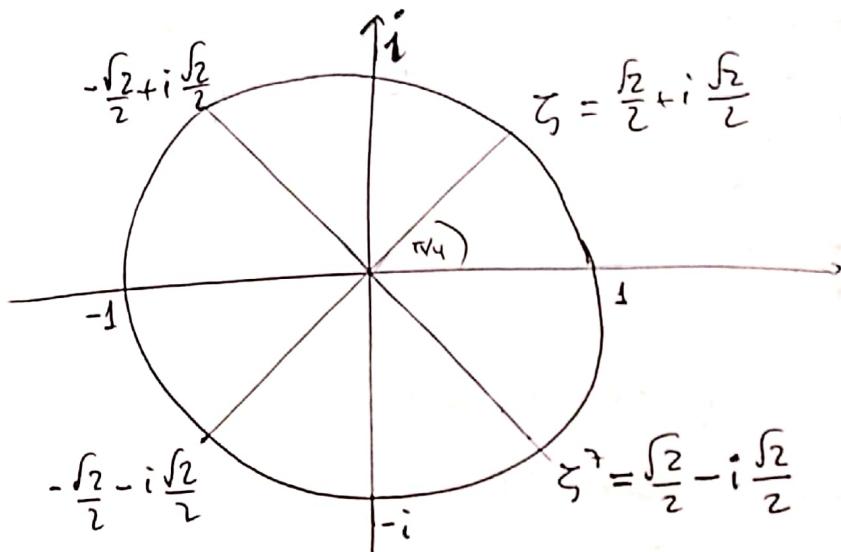
(Grupos cuadradiédrico)

$$\tau : \begin{cases} \theta \mapsto \theta \\ i \mapsto -i \\ \zeta \mapsto \zeta^7 \end{cases}$$

$$\begin{aligned}\tau(\zeta) &= \frac{1}{2}(1 + \tau(i))\tau(\theta)^4 \\ &= \frac{1}{2}(1 - i)\theta^4 = \frac{\sqrt{2}}{2} - i \cdot \frac{\sqrt{2}}{2} \\ &= \zeta^7\end{aligned}$$



Dibujo :  $\zeta = \frac{\sqrt{2}}{2} + i \frac{\sqrt{2}}{2}$



Calculemos :

$$\sigma^2(\theta) = \sigma(\zeta\theta) = \sigma(\zeta)\sigma(\theta) = -\zeta \zeta\theta = -\zeta^2\theta = -i\theta$$

$$\sigma^3 : \begin{cases} \theta \mapsto \zeta^3\theta \\ i \mapsto i \\ \zeta \mapsto \zeta^5 \end{cases}$$

$$\sigma^5 : \begin{cases} \theta \mapsto \zeta^5\theta \\ i \mapsto i \\ \zeta \mapsto -\zeta \end{cases}$$

$$\sigma^6 : \begin{cases} \theta \mapsto \zeta^6\theta \\ i \mapsto i \\ \zeta \mapsto \zeta \end{cases}$$

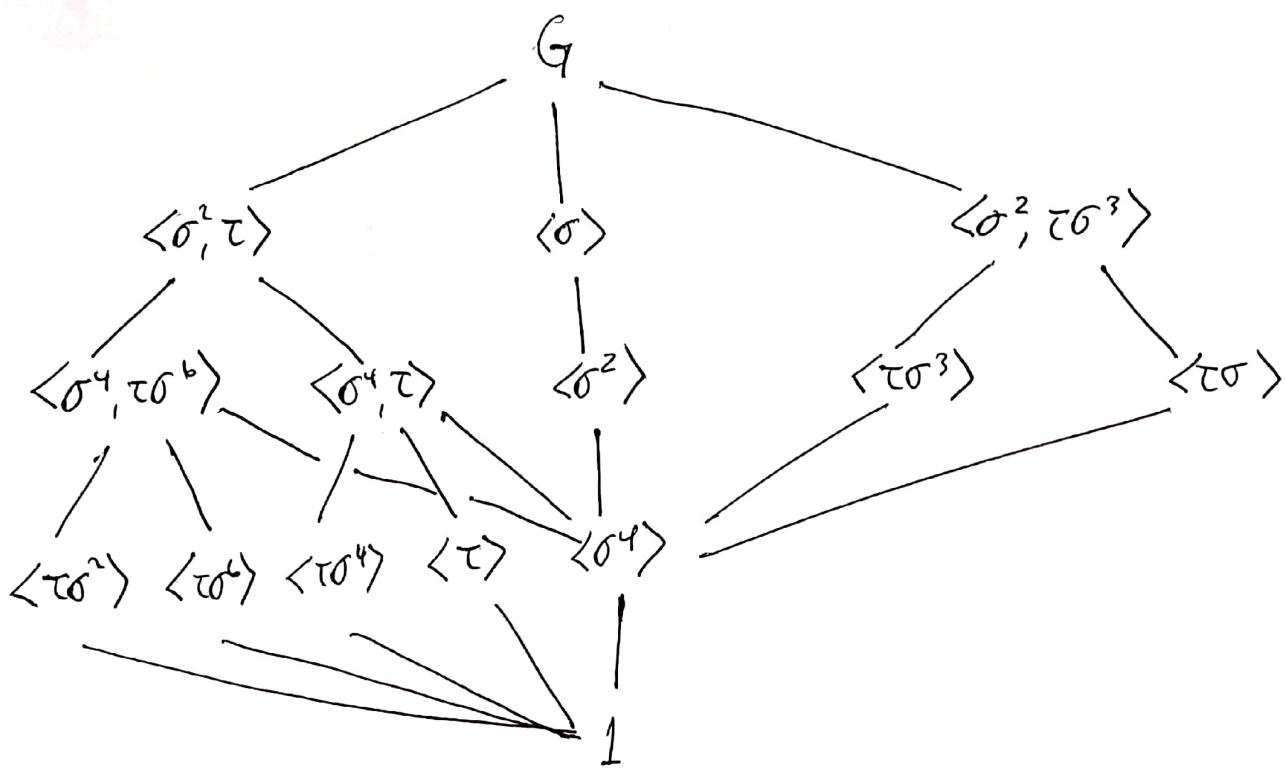
$$\sigma^7 : \begin{cases} \theta \mapsto \zeta^7\theta \\ i \mapsto i \\ \zeta \mapsto -\zeta \end{cases}$$

$$\sigma^8 : \begin{cases} \theta \mapsto -\theta \\ i \mapsto i \\ \zeta \mapsto \zeta \end{cases}$$

$$\sigma^8 : \begin{cases} \theta \mapsto \theta \\ i \mapsto i \\ \zeta \mapsto -\zeta \end{cases}$$

$$\therefore \sigma^8 = 1$$

• Tomemos el diagrama de Bruyn para  $G$ :



EJERCICIO 1. Sean  $n, m$  enteros positivos relativamente primos. Pruebe que  $\mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}(\zeta_{nm})$ . Muestre que  $\Phi_n(x)$  es irreducible sobre  $\mathbb{Q}(\zeta_m)$ .

EJERCICIO 2. Sea  $q = p^n$  con  $p$  primo. ¿Para cuál  $q$  es la extensión cuadrática  $\mathbb{F}_{q^2}$  de  $\mathbb{F}_q$  de la forma  $\mathbb{F}_q(\sqrt{x})$ ?

EJERCICIO 3. Sea  $\alpha \in \mathbb{F}_{49}$  tal que  $\alpha^2 = 3$  y  $\mathbb{F}_{49} = \mathbb{F}_7(\alpha)$ . Encuentre un generador para el grupo cíclico  $(\mathbb{F}_{49})^*$  y determine su polinomio minimal sobre  $\mathbb{F}_7$ .

EJERCICIO 4. Sea  $K = F(\alpha)$ , donde  $K$  y  $F$  son cuerpos de característica  $p > 0$ . Si  $\alpha^p - \alpha = \beta \in F$  demuestre que  $K/F$  es normal.

EJERCICIO 5. Demuestre que  $\mathbb{Q}(\cos(\pi/9))/\mathbb{Q}$  es una extensión de grado 3. ¿Es normal?

EJERCICIO 6. Sea  $K$  un cuerpo cuya única extensión algebraica y separable es  $K$ . ¿Es  $K$  algebraicamente cerrado?

EJERCICIO 7. Sea  $K/F$  extensión de cuerpos:

1. Muestre que si el cuerpo  $K$  está generado sobre  $F$  por los elementos  $a_1, \dots, a_n$  entonces un automorfismo  $\sigma$  de  $K$  que fija  $F$  está únicamente determinado por  $\sigma(a_1), \dots, \sigma(a_n)$ .
2. Sea  $G$  un subgrupo de  $\text{Gal}(K/F)$  y suponga que  $\sigma_1, \dots, \sigma_k$  son generadores para  $G$ . Muestre que el subcuerpo  $E/F$  es fijo por  $G$  si y sólo si es fijo por los generadores  $\sigma_1, \dots, \sigma_k$ .

EJERCICIO 8. Pruebe que  $\mathbb{Q}(\sqrt{2})$  y  $\mathbb{Q}(\sqrt{3})$  no son isomorfos.

EJERCICIO 9. Determine explícitamente los automorfismos de la extensión  $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ .

EJERCICIO 10. Determine  $\text{Aut}(\mathbb{R}/\mathbb{Q})$ .

EJERCICIO 11. 1. Pruebe que los automorfismos del cuerpo de funciones racionales  $k(t)$  que fijan  $k$  son precisamente las transformaciones lineales fraccionarias determinadas por

$$t \mapsto \frac{at + b}{ct + d}$$

con  $a, b, c, d \in k$  tales que  $ad - bc \neq 0$ , es decir,

$$f(t) \mapsto f\left(\frac{at + b}{ct + d}\right), \quad f(t) \in k(t).$$

2. Determine el cuerpo fijo del automorfismo  $t \mapsto t + 1$  de  $k(t)$ .

EJERCICIO 12. Calcule el grupo de Galois de  $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q}$ .

EJERCICIO 13. Sea  $K$  una extensión de  $F$ . Sea  $\phi : K \rightarrow K'$  un isomorfismo de cuerpos y sea  $F' = \phi(F)$ . Sea  $\Lambda : \text{Aut}(K/F) \rightarrow \text{Aut}(K'/F')$  dada por  $\Lambda(\sigma) = \phi\sigma\phi^{-1}$ . Demuestre que  $\Lambda$  es un isomorfismo de grupos.

EJERCICIO 14. Pruebe que el grupo  $\text{Gal}(\mathbb{C}/\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$ .

EJERCICIO 15. Sea  $E/F$  una extensión finita de Galois. Suponga que  $\text{Aut}(E/F)$  es isomorfo al grupo de Klein de 4 elementos. Demuestre que  $E = F(\alpha, \beta)$ , donde  $\alpha$  y  $\beta$  son elementos de  $E$  tales que  $\alpha^2, \beta^2 \in F$ .

Algebra II  
Lista de ejercicios VII (Desarrollo)

Ejercicio 3

Sea  $\alpha \in \mathbb{F}_{49}$  tal que  $\alpha^2 = 3$  y  $\mathbb{F}_{49} = \mathbb{F}_7(\alpha)$ . Encuentre un generador para el grupo cíclico  $(\mathbb{F}_{49})^*$  y determine su polinomio minimal sobre  $\mathbb{F}_7$ .

Desarrollo. Recordar que  $(\mathbb{F}_{49})^* \cong C_{48}$ . También

$$\begin{aligned}\alpha &= \alpha \\ \alpha^2 &= 3 \\ \alpha^3 &= 3\alpha \\ \alpha^4 &= 2 \\ \alpha^5 &= 2\alpha \\ \alpha^6 &= 6 \\ \alpha^7 &= 6\alpha \\ \alpha^8 &= 4 \\ \alpha^9 &= 4\alpha \\ \alpha^{10} &= 5 \\ \alpha^{11} &= 5\alpha \\ \alpha^{12} &= 1\end{aligned}$$

$x \in \mathbb{F}_7$	$\text{ord}(x)$ (orden)
1	1
2	3
3	6
4	3
5	6
6	2

$\mathbb{F}_{49} = \{a+b\alpha / a, b \in \mathbb{F}_7\}$ . Queremos un  $a+b\alpha \in \mathbb{F}_{49}$  tal que  $(a+b\alpha)^{48} = 1$ . Notar que

$$1 = (a+b\alpha)^{48} = ((a+b\alpha)^8)^6 \quad | \text{objetivo: } (a+b\alpha)^8 \in \{3, 5\}$$

$$\begin{aligned}(a+b\alpha)^8 &= (a+b\alpha)^7(a+b\alpha) = (a^7 + b^7\alpha^7)(a+b\alpha) \\ &= (a+b\alpha^7)(a+b\alpha) = (a+6b\alpha)(a+b\alpha) \\ &= a^2 + ab\alpha + 6ab\alpha + 6b^2\alpha^2 = a^2 + 7ab\alpha + 18b^2 \\ &= a^2 + 4b^2\end{aligned}$$

$\Rightarrow a, b \in \mathbb{F}_7 : a^2 + 4b^2 = 3$ . Con un poco de trabajo puede deducirse que  $a=1, b=2$  es una solución.

$$\therefore (\mathbb{F}_{49})^* = \langle 1+2\alpha \rangle$$

Ahora debemos encontrar  $m_{(1+2\alpha), \mathbb{F}_7}(x)$

$$\text{Sea } x = 1 + 2\alpha \iff \alpha = \frac{x-1}{2}$$

$$x^2 = (1+2\alpha)^2 = 1 + 4\alpha^2 + 4\alpha = 1 + 4 \cdot 3 + 4\alpha$$

$$= 13 + 4\alpha = 6 + 4\alpha = 6 + 4\left(\frac{x-1}{2}\right) = 6 + 2(x-1)$$

$$\therefore 6 + 2x - 2 = 4 + 2x$$

$$\therefore x^2 - 2x - 4 = 0$$

$$\iff x^2 + 5x + 3 = 0$$

$\therefore$  Tenemos que  $m_{(1+2\alpha), \mathbb{F}_7}(x) = x^2 + 5x + 3$

Ejercicio 7. Sea  $k/F$  extensión de cuerpos

(1) Demostre que si  $K = F(a_1, \dots, a_n)$ , entonces  $\sigma \in \text{Aut}_F(K)$  está determinado por  $\sigma(a_1), \dots, \sigma(a_n)$  (de manera única)

2) Sea  $G \leq \text{Gal}(K/F)$  y  $\sigma_1, \dots, \sigma_k$  generadores de  $G$ .

Demostre que  $E/F$  es fijo por  $G$  si y sólo si es fijo por los generadores  $\sigma_1, \dots, \sigma_k$ .

Demonstración

(1) Por inducción sobre  $n$ .

$n=1$ ,  $K = F(a_1)$ . Tenemos que

$$K = \{b_0 + b_1 a_1 + \dots + b_{m-1} a_1^{m-1} \mid b_j \in F\}$$

$\sigma \in \text{Aut}_F(K) : \sigma(a_1) = \sum b_j \sigma(a_1)^j ; a = \sum b_j a_1^j$ , luego  $\sigma$  queda determinado únicamente por  $\sigma(a_1)$ , ya que los  $b_j \in F$  son únicos

now Supongamos que  $K = F(a_1, \dots, a_n)$  y cada  $\sigma \in \text{Aut}_F(K)$  queda únicamente determinado por  $\sigma(a_1), \dots, \sigma(a_n)$ .

Sea  $a_{n+1}$  algebraico sobre  $\hat{K}$  de grado  $m_{n+1}$ ,  
entonces  $\{1, a_{n+1}, \dots, a_{n+1}^{m_{n+1}-1}\}$  es una base de  
 $\hat{K}(a_{n+1})/\hat{K}$ . Así que  $\forall a \in \hat{K}$ , existen únicos  
 $b_0, \dots, b_{m_{n+1}-1} \in \hat{K}$  tales que  $a = \sum_{j=0}^{m_{n+1}-1} b_j a_{n+1}^j$ . Luego  
 $\forall \sigma \in \text{Aut}_F(\hat{K}(a_{n+1}))$ :

$$\sigma(a) = \sum_{j=0}^{m_{n+1}-1} \sigma(b_j) \sigma(a_{n+1})^j$$

$\sigma$  queda determinado únicamente por  $\sigma(b_0), \dots, \sigma(b_{m_{n+1}-1})$   
y  $\sigma(a_{n+1})$ ; pero  $\sigma|_{F(a_1, \dots, a_n) = \hat{K}} \in \text{Aut}_F(\hat{K})$  es  
bien conocido por  $\sigma(a_1), \dots, \sigma(a_n)$  y  $\forall j \in \{0, \dots, m_n-1\}$   
 $\sigma(b_j) = \sigma|_{\hat{K}}(b_j)$

$\therefore \sigma$  queda únicamente determinado por  
 $\sigma(a_1), \dots, \sigma(a_n), \sigma(a_{n+1})$

□

(2) Pd:  $E$  fijo por  $G = \langle \sigma_1, \dots, \sigma_k \rangle \iff E$  fijo por  
 $\sigma_1, \dots, \sigma_k$

( $\Rightarrow$ ) Como  $\{\sigma_1, \dots, \sigma_k\} \subset G$ , entonces si  $E$  es fijo  
por  $G$ , automáticamente es fijo por  $\{\sigma_1, \dots, \sigma_k\}$

( $\Leftarrow$ ) Si  $E$  es fijo por  $\sigma_1, \dots, \sigma_k$ , entonces  $\forall m \in \mathbb{N}$ ,  
 $E$  es fijo por  $\sigma_j^m$   $\forall j$ . Ahora como  $G = \langle \sigma_1, \dots, \sigma_k \rangle$ ,  
dado  $\sigma \in G$ :  $\sigma = \sigma_1^{m_1} \cdots \sigma_k^{m_k}$ ,  $m_j \in \mathbb{N} \cup \{0\}$  ( $\sigma_j^0 = \text{id}$ )

Sea  $\alpha \in E$ :  $\sigma(\alpha) = \sigma_1^{m_1} \cdots \sigma_k^{m_k}(\alpha)$   
 $= \sigma_1^{m_1}(\sigma_2^{m_2}(\cdots (\sigma_k^{m_k}(\alpha)) \cdots))$   
 $= \sigma_1^{m_1}(\sigma_2^{m_2}(\cdots \sigma_{k-1}^{m_{k-1}}(\alpha)) \cdots)$   
 $\vdash \sigma_1^{m_1}(\alpha) = \alpha \quad \therefore E$  fijo por  $G$  □

Ejercicio 8. Demostrar que  $\mathbb{Q}(\sqrt{2})$  y  $\mathbb{Q}(\sqrt{3})$  no son isomorfos.

Dem. Un isomorfismo  $\delta: \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{3})$  debe cumplir que  $\delta(q) = q \quad \forall q \in \mathbb{Q}$  y además  $2 = \delta(\sqrt{2})^2$   
 $\therefore 2$  es cuadrado en  $\mathbb{Q}(\sqrt{3})$

Para ver que esto no es cierto, tomemos  $a, b \in \mathbb{Q}$  tales que  $2 = (a + b\sqrt{3})^2 \Leftrightarrow 2 = a^2 + 3b^2 + 2ab\sqrt{3}$

$$\therefore \begin{cases} ab = 0 \\ a^2 + 3b^2 = 2 \end{cases}$$

$$\text{Si } a=0 \Rightarrow 3b^2 = 2 \Rightarrow b^2 = \frac{2}{3} \quad (\Leftrightarrow)$$

$$\text{Si } b=0 \Rightarrow a^2 = 2 \quad (\Leftrightarrow)$$

$\therefore \mathbb{Q}(\sqrt{2})$  y  $\mathbb{Q}(\sqrt{3})$  no pueden ser isomorfos.

Ejercicio 9. Determine explícitamente los automorfismos de la extensión  $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$

Desarrollo.

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

$$2 |$$

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

$$2 |$$

$$\mathbb{Q}$$

Como  $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})] = 2$ , entonces es una extensión Galoiana. En decir,

$$[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})] = 2 = |\text{Gal}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2}))|$$

~~$\therefore \text{Si } \alpha = \sqrt[4]{2} \Rightarrow \alpha^2 - \sqrt{2} = 0$~~

$$\Rightarrow \alpha \text{ raíz de } m_{\alpha, \mathbb{Q}(\sqrt{2})}(x) = x^2 - \sqrt{2}$$

$$\text{Sea } \sigma \in \text{Gal}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2}))$$

$$0 = \sigma(0) = \sigma(\alpha)^2 - \sigma(\sqrt{2}) = \sigma(\alpha)^2 - \sqrt{2} = \sigma(\alpha)^2 - \alpha^2$$

~~$\Rightarrow \sigma(\alpha) - \alpha \quad (\sigma(\alpha) + \alpha) = 0$~~

$$a + b\sqrt[4]{2} \mapsto a + b\sqrt{2}$$

$$\therefore \sigma(\alpha) = \alpha \quad \& \quad \sigma(\alpha) = -\alpha \quad . \quad \text{Así los automorfismos son } a + b\sqrt[4]{2} \mapsto a - b\sqrt[4]{2},$$

donde  $a, b \in \mathbb{Q}(\sqrt{2})$

## Ejercicio 11

(1) Prueba que los automorfismos del cuerpo de funciones racionales  $k(t)$  que fijan  $k$  son precisamente las transformaciones lineales fraccionarias determinadas por

$$t \mapsto \frac{at+b}{ct+d}$$

con  $a, b, c, d \in k$  tales que  $ad - bc \neq 0$ , es decir,

$$f(t) \mapsto f\left(\frac{at+b}{ct+d}\right), \quad f(t) \in k(t).$$

(2) Determina el cuerpo fijo del automorfismo  $t \mapsto t+1$  de  $k(t)$ .

Dem. (1)  $\varphi \in \text{Aut}_k(k(t)) \Rightarrow \varphi(f(t)) = f(\varphi(t))$  (trivial)

Antes de demostrar los pedidos, demostraremos la siguiente:

Afirmación: Si  $u(t) = \frac{g(t)}{h(t)} \in k(t)$ , entonces  $[k(t) : k(u(t))]$  es una extensión algebraica y  $[k(t) : k(u(t))] = \max \{ \deg g(t), \deg h(t) \}$ .

dem. Supongamos que  $g, h$  relativamente primos.

$$u(t) = \frac{g(t)}{h(t)} \Leftrightarrow g(t) - u(t)h(t) = 0. \text{ Luego } t \text{ es}$$

raíz del polinomio  ~~$F(x) = g(x) - uh(x)$~~ , donde  $\deg F(x) = \max \{ \deg g(x), \deg h(x) \}$ .

$$F(x) \in k(u)[x].$$

$$\therefore [k(t) : k(u)] < \infty \text{ (extensión algebraica)}$$

$$\text{Noten que } k(u)(t) = k(t)$$

$$\text{Pd: } [k(t) : k(u)] = \max \{ \deg g, \deg h \}$$

dem. Basta probar que  $F(x) \in (k(u))[x]$  es irreducible.

Como  $(k[u])[x] \cong (k[x])[u]$ , entonces  $g(x) - u h(x)$  es irreducible en  $(k[x])[u]$  porque es de grado 1

$\therefore F(x)$  irreducible en  $k[u][x]$

Por lema de Gauss ( $k[u]$  D.F.U),  ~~$k[u][x]$  es UFD~~

( $\text{Quot } k[u] = k(u)$ ), entonces  $F(x)$  es irreducible en  $(k(u))[x]$ .

$$\therefore [k(t):k(u)] = \max \{\deg g, \deg h\}$$

Ahora, si  $t \mapsto \frac{at+b}{ct+d}$ . De otra manera

$$\varphi(f(t)) = \frac{\varphi(g(t))}{\varphi(h(t))}. \text{ Como } \varphi(k(t)) = k(\varphi(t)),$$

$\varphi$  automorfismo implica que  $[k(t):k(\varphi(t))] = 1$ .

Dejgo por el resultado anterior  $\varphi(g(t))$  y  $\varphi(h(t))$  deben ser de grado 1, es decir,  $\varphi(g(t)) = at+b$ ,

$\varphi(h(t)) = ct+d$  (La condición  $ad-bc \neq 0$  es necesaria para que no tengan factores comunes). Además

$$\varphi(g(t)) = g(\varphi(t)), \quad \varphi(h(t)) = h(\varphi(t))$$

$$\therefore \varphi(f(t)) = f(\varphi(t))$$

Por el resultado anterior, necesariamente  $\varphi(t) = \frac{at+b}{ct+d}$

(La condición  $ad-bc \neq 0$  se requiere para que no tengan factores comunes)

(2) Determinar el anillo fijo por el automorfismo  $t \mapsto t+1$  de  $k(t)$ .

Sea  $k(t)^{\varphi} = \{ f(t) \in k(t) \mid \varphi(f(t)) = f(t) \}$ , donde  
 $\varphi: k(t) \rightarrow k(t)$ ,  $\varphi|_k = \text{id}_k$ ,  $\varphi(t) = t+1$

$$\begin{aligned}\varphi(f(t)) = f(t) &\iff f(\varphi(t)) = f(t) \\ &\iff f(t+1) = f(t)\end{aligned}$$

### Ejercicio 13.

Sea  $K$  una extensión de  $F$ . Sea  $\phi: K \rightarrow K'$  un isomorfismo de cuerpos y sea  $F' = \phi(F)$ . Sea  $\Lambda: \text{Aut}(K/F) \rightarrow \text{Aut}(K'/F')$  dada por  $\Lambda(\sigma) = \phi\sigma\phi^{-1}$ . Demuestre que  $\Lambda$  es un isomorfismo de grupos.

Dem.

(1)  $\Lambda$  homomorfismo de grupos:

Sean  $\sigma, \tau \in \text{Aut}(K/F)$ :

$$\begin{aligned}\Lambda(\sigma\tau) &= \phi(\sigma\tau)\phi^{-1} = \phi\sigma(\phi^{-1}\phi)\tau\phi^{-1} \\ &= (\phi\sigma\phi^{-1})(\phi\tau\phi^{-1}) = \Lambda(\sigma)\Lambda(\tau)\end{aligned}$$

$$\Lambda(1) = \phi(1)\phi^{-1} = \phi\phi^{-1} = 1$$

$\therefore \Lambda$  es homomorfismo de grupos.

(2)  $\Lambda$  es isomorfismo de grupos:

El candidato a inversa es  $\Lambda^{-1}: \text{Aut}(K'/F') \rightarrow \text{Aut}(K/F)$ ,

$$\Lambda^{-1}(\tau) = \phi^{-1}\tau\phi. \text{ Luego}$$

$$\begin{aligned}(\Lambda \circ \Lambda^{-1})(\tau) &= \Lambda(\Lambda^{-1}(\tau)) = \Lambda(\phi^{-1}\tau\phi) \\ &= \phi(\phi^{-1}\tau\phi)\phi^{-1} = (\phi\phi^{-1})\tau(\phi\phi^{-1}) \\ &= 1\tau 1 = \tau\end{aligned}$$

$$\begin{aligned}(\Lambda^{-1} \circ \Lambda)(\sigma) &= \Lambda^{-1}(\Lambda(\sigma)) = \Lambda^{-1}(\phi\sigma\phi^{-1}) \\ &= \phi^{-1}(\phi\sigma\phi^{-1})\phi = (\phi^{-1}\phi)\sigma(\phi^{-1}\phi) \\ &= 1\sigma 1 = \sigma\end{aligned}$$

$\therefore \Lambda$  invertible

$\therefore \Lambda$  isomorfismo de grupos.

Ejercicio 14. Puede que  $\text{Gal}(\mathbb{C}/\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$ .

Dem. Sea sabido que  $[\mathbb{C}:\mathbb{R}] = 2$ . En particular  $\mathbb{C}/\mathbb{R}$  es Galoisiana, porque  $\mathbb{C}$  es cuerpo de descomposición de  $x^2 + 1 \in \mathbb{R}[x]$ . Ahora basta notar que

$$\begin{aligned}\sigma: \mathbb{C} &\longrightarrow \mathbb{C} \\ a+bi &\longmapsto a-bi\end{aligned}$$

es un automorfismo, y  $\sigma^2 = 1$

$$\therefore \text{Gal}(\mathbb{C}/\mathbb{R}) \cong \langle \sigma \rangle \cong \mathbb{Z}/2\mathbb{Z}.$$

---

Ejercicio 15.

Sea  $E/F$  una extensión finita de Galois. Suponga que  $\text{Aut}(E/F)$  es isomorfo al grupo de Klein de 4 elementos.

Demuestre que  $E=F(\alpha, \beta)$ , donde  $\alpha, \beta$  son elementos de  $E$  tales que  $\alpha^2, \beta^2 \in F$ .

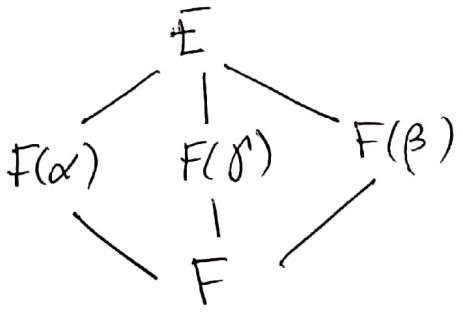
Dem.  $E/F$  finita Galoisiana,  $\text{Gal}(E/F) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .

\* Tenemos que  $\text{Gal}(E/F) = \langle \sigma, \tau \rangle$ , donde

$\sigma^2 = \tau^2 = (\sigma\tau)^2 = 1$ . Como  $\text{Gal}(E/F)$  es abeliano (todos sus subgrupos son normales)  $E^{\langle \sigma \rangle}/F$ ,  $E^{\langle \tau \rangle}/F$ ,  $E^{\langle \sigma\tau \rangle}/F$  son extensiones cuadráticas Galoisianas

$$\therefore E^{\langle \sigma \rangle} = F(\alpha), E^{\langle \tau \rangle} = F(\beta), E^{\langle \sigma\tau \rangle} = F(\gamma)$$

tales que  ~~$\alpha^2, \beta^2, \gamma^2 \in F$~~   $\alpha^2, \beta^2, \gamma^2 \in F$ .



Como no puede darse que  $\beta \in F(\alpha)$  (En caso contrario  $F(\alpha) = F(\beta)$  y eso contradice el segundo teorema fundamental de la teoría de Galois), entonces  $x^2 - \beta^2$  es irreducible sobre  $F(\alpha)$ . Así  $[F(\alpha, \beta) : F] = 4$  y  $F(\alpha, \beta) \subset E$ .  $\therefore E = F(\alpha, \beta)$ .

**EJERCICIO 1. Propiedades de los polinomios ciclotómicos.**

1. Dado  $n$ , sea  $m = \prod_{p|n} p$ . Pruebe que  $\Phi_n(x) = \Phi_m(x^{n/m})$ . Esto muestra que para calcular  $\Phi_n(x)$  podemos reducirnos al caso  $n$  libre de cuadrados. Calcule  $\Phi_{p^2}(x)$  para  $p$  primo.
2. Sea  $n > 1$  entero impar. Pruebe que  $\Phi_{2n}(x) = \Phi_n(-x)$ .
3. Sea  $p$  primo que no divide al entero  $n > 1$ . Pruebe que

$$\Phi_{pn}(x) = \frac{\Phi_n(x^p)}{\Phi_n(x)}.$$

**EJERCICIO 2.** Sean  $n, m$  enteros positivos relativamente primos. Pruebe que  $\mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}(\zeta_{nm})$ . Muestre que  $\Phi_n(x)$  es irreducible sobre  $\mathbb{Q}(\zeta_m)$ .

**EJERCICIO 3.** Calcule el número de factores irreducibles de  $x^{255} - 1 \in \mathbb{Q}[x]$  y sus grados. (Ayuda: calcule  $\Phi_{255}(x)$ )

**EJERCICIO 4.** Pruebe que  $d$  divide a  $n$  si y sólo si  $x^d - 1$  divide a  $x^n - 1$ . (*Hint: Si  $n = qd + r$  entonces  $x^n - 1 = (x^{qd+r} - x^r) + (x^r - 1)$ .*) Concluir que  $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$  si y sólo si  $d$  divide a  $n$ .

**EJERCICIO 5.** Pruebe que

$$x^{p^n-1} - 1 = \prod_{\alpha \in \mathbb{F}_{p^n}^\times} (x - \alpha).$$

En particular, para todo cuerpo finito

$$\prod_{\alpha \in \mathbb{F}_{p^n}^\times} \alpha = (-1)^{p^n}.$$

Para  $p$  impar y  $n = 1$  pruebe el Teorema de Wilson:

$$(p-1)! \equiv -1 \pmod{p}.$$

**EJERCICIO 6.** Sea  $q = p^n$  con  $p$  primo. ¿Para cuál  $q$  es la extensión cuadrática  $\mathbb{F}_{q^2}$  de  $\mathbb{F}_q$  de la forma  $\mathbb{F}_q(\sqrt{x})$ ?

**EJERCICIO 7.** Considerar  $f(x) = x^3 + x^2 + 1 \in \mathbb{F}_3[x]$ . Sea  $K \subseteq \overline{\mathbb{F}_3}$  el cuerpo de descomposición de  $f(x)$  sobre  $\mathbb{F}_3$ . Determinar el tamaño  $|K|$  de  $K$ . Demostrar que  $x^2 + 1 \in K[x]$  se descompone sobre  $K$ .

**EJERCICIO 8.** Sea  $F \subseteq K$  extensión algebraica de cuerpos. Sea  $\alpha \in K$  tal que  $\alpha^n = 1$  para algún  $n \in \mathbb{N}$ . Demuestre que  $F(\alpha)/F$  es normal.

**EJERCICIO 9.** Sea  $K = F(\alpha)$ , donde  $K$  y  $F$  son cuerpos de característica  $p > 0$ . Si  $\alpha^p - \alpha = \beta \in F$  demuestre que  $K/F$  es normal.

**EJERCICIO 10.** Demuestre que  $\mathbb{Q}(\cos(\pi/9))/\mathbb{Q}$  es una extensión de grado 3. ¿Es normal?

**EJERCICIO 11.** Sea  $F$  un cuerpo. Muestre que el anillo de polinomios  $F[x]$  posee infinitos ideales primos. Pruebe que los cuerpos algebraicamente cerrados poseen cardinalidad infinita.

**EJERCICIO 12.** Sea  $K$  un cuerpo cuya única extensión algebraica y separable es  $K$ . ¿Es  $K$  algebraicamente cerrado?

Algebra II  
Desarrollo Guía 6

Ejercicio 1. (Propiedades de los polinomios ~~irreducibles~~ ciclotómicos)

1) Dado  $n \in \mathbb{N}$ , sea  $m = \prod_{p|n} p$ . Puede que  $\Phi_n(x) = \Phi_m(x^{n/m})$ .

Esto muestra que para calcular  $\Phi_n(x)$  podemos reducirnos al caso  $n$  libre de cuadrados. Calcula  $\Phi_p^2(x)$  para  $p$  primo.

2) Sea  $n > 1$  entero impar. Puede que  $\Phi_{2n}(x) = \Phi_n(-x)$

3) Sea  $p$  primo que no divide al entero  $n > 1$ . Puede que

$$\Phi_{pn}(x) = \frac{\Phi_n(x^p)}{\Phi_n(x)}$$

Ejercicio 2. Sean  $n, m$  enteros relativamente primos. Pruebe que  $\mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}(\zeta_{nm})$ . Muestre que  $\Phi_n(x)$  es irreducible sobre  $\mathbb{Q}(\zeta_m)$ .

Demonstración.

$\mathbb{Q}(\zeta_{nm})$  cuerpo de descomposición de  $x^{nm} - 1 \in \mathbb{Z}[x]$

$$(\zeta_n)^{nm} - 1 = 0, (\zeta_m)^{nm} - 1 = 0$$

$\therefore$  Raíces  $n, m$ -ésimas de la unidad son raíces  $nm$ -ésimas de la unidad.

$$\therefore \mathbb{Q}(\zeta_n, \zeta_m) \subseteq \mathbb{Q}(\zeta_{nm})$$

Por otro lado, afirmamos que  $\zeta_n \zeta_m$  raíz  $nm$ -ésima de la unidad

En efecto,  $(\zeta_n \zeta_m)^{nm} = (\zeta_n)^{nm} (\zeta_m)^{nm} = (\zeta_n^n)^m (\zeta_m^m)^n = 1 \cdot 1 = 1$

$$\therefore (\zeta_n \zeta_m)^{nm} - 1 = 0.$$

Af.  $(n, m) = 1 \Rightarrow \zeta_n \zeta_m$  raíz primitiva  $nm$ -ésima.

dem.  $\zeta_n = e^{2\pi i k/n}, \zeta_m = e^{2\pi i l/m} \quad (\text{mcd}(k, n) = 1 \quad \text{mcd}(l, m) = 1)$

$$\zeta_n \zeta_m = e^{2\pi i k/n} e^{2\pi i l/m} = e^{2\pi i (km + ln)/nm}$$

$$\mathbb{Q}(\zeta_n, \zeta_m) \supseteq \zeta_n \zeta_m = e^{2\pi i (km + ln)/nm}$$

Por demostrar:  $\text{mcd}(nm, km + ln) = 1$

Sia  $d = \text{mcd}(nm, km + ln)$ ; sea  $p \in \mathbb{Z}$  primo:  $p \nmid d$

$$p \nmid d \Rightarrow p \nmid nm \Rightarrow p \nmid m \wedge p \nmid n$$

$$\begin{aligned} \text{Sup } p \nmid m &\Rightarrow p \nmid n \wedge p \nmid (km + ln) \\ &\Rightarrow p \nmid k \end{aligned}$$

$$\therefore p \nmid n \wedge p \nmid k$$

$$\therefore p = 1$$

$$\therefore d = 1$$

Así,  $\mathbb{Q}(\zeta_n, \zeta_m)$  contiene a todas las raíces  $nm$ -ésimas de la unidad

$$\therefore \mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}(\zeta_{nm}).$$

$$\begin{aligned} \text{• } \mathbb{Q}(\zeta_{nm}) &= \mathbb{Q}(\zeta_n, \zeta_m) \\ \downarrow & \quad \downarrow \\ \mathbb{Q}(\zeta_n) & \quad \mathbb{Q}(\zeta_m) \\ \varphi(n) \swarrow & \searrow \varphi(m) \end{aligned}$$

Como  $[\mathbb{Q}(\zeta_{nm}): \mathbb{Q}] = \varphi(nm)$   
 $= \varphi(n)\varphi(m)$   
 $(\text{mcd}(n,m)=1)$

$$\Rightarrow [\mathbb{Q}(\zeta_{nm}): \mathbb{Q}(\zeta_m)] = \varphi(n).$$

$\zeta_n \in \mathbb{Q}(\zeta_{nm})$  es raíz del polinomio  
 $\Phi_n(x)$  de grado  $\varphi(n)$ , junto con  
 $\zeta_n \notin \mathbb{Q}(\zeta_m) \Rightarrow \therefore \Phi_n(x)$  irred |  $\mathbb{Q}(\zeta_m)$

Ejercicio 3. Calcula el número de factores irreducibles de  $x^{255}-1 \in \mathbb{Q}[x]$  y sus grados. (Hint: Calcula  $\Phi_{255}(x)$ ).

Desarrollo.

$$x^{255}-1 = \prod_{d|255} \Phi_d(x)$$

$255 = 3 \cdot 5 \cdot 17 \Rightarrow$  divisores de 255 os gto:  $\{1, 3, 5, 15, 17, 51, 85, 255\}$

$$\therefore x^{255}-1 = \Phi_1(x) \Phi_3(x) \Phi_5(x) \Phi_{15}(x) \Phi_{17}(x) \Phi_{51}(x) \Phi_{85}(x) \Phi_{255}(x)$$

$\Phi_j(x)$  j-ésimo polinomio ciclotómico (ined  $\mathbb{Z}_4$ ) ( $\Phi_j(x) \in \mathbb{Z}[x]$ )

$\therefore x^{255}-1$  tiene 8 factores irreducibles.

Grados:

$$\text{gr}(\Phi_1) = \varphi(1) = 1$$

$$\text{gr}(\Phi_3) = \varphi(3) = 2$$

$$\text{gr}(\Phi_5) = \varphi(5) = 4$$

$$\text{gr}(\Phi_{15}) = \varphi(15) = \varphi(3)\varphi(5) = 2 \cdot 4 = 8$$

$$\text{gr}(\Phi_{17}) = \varphi(17) = 16$$

$$\text{gr}(\Phi_{51}) = \varphi(51) = \varphi(3)\varphi(17) = 2 \cdot 16 = 32$$

$$\text{gr}(\Phi_{85}) = \varphi(85) = \varphi(17)\varphi(5) = 16 \cdot 4 = 64$$

$$\text{gr}(\Phi_{255}) = \varphi(255) = \varphi(3)\varphi(5)\varphi(17) = 2 \cdot 4 \cdot 16 = 128$$

Ejercicio 4. Prueba que  $d$  divide a  $n$  si  $x^d - 1$  divide a  $x^n - 1$   
 (Hint: Si  $n = qd + r$ , entonces  $x^n - 1 = (x^{qd+r} - x^r) + (x^r - 1)$ ).

Concluir que  $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$  si  $d$  divide a  $n$ .

Dem.  $\forall m \in \mathbb{N}: x^m - 1 = (x-1)(x^{m-1} + x^{m-2} + \dots + x + 1)$

$(\Rightarrow) \sup d | n:$

$$\begin{aligned} x^n - 1 &= x^{dq} - 1, \quad q \in \mathbb{N} \\ &= (x^d)^q - 1 = (x^d - 1)(x^{d(q-1)} + x^{d(q-2)} + \dots + x^d + 1) \end{aligned}$$

$$\therefore x^d - 1 \mid x^n - 1.$$

$$\begin{aligned} (\Leftarrow) \quad x^n - 1 &= (x^{qd+r} - x^r) + (x^r - 1) = x^r(x^{qd} - 1) + (x^r - 1) \\ &= x^r(x^d - 1)(x^{d(q-1)} + \dots + x^d + 1) + (x^r - 1) \end{aligned}$$

$$x^d - 1 \mid x^n - 1 \Rightarrow x^r - 1 = 0 \quad \therefore r = 0$$

$$\therefore n = qd + r, \quad r = 0$$

$$\therefore n = qd$$

$$\therefore d | n.$$

Pd:  $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n} \Leftrightarrow d | n$

$\forall m \in \mathbb{N}: \mathbb{F}_{p^m}$  cuerpo de descomposición de  $x^{p^m} - x \in \mathbb{F}_p[x]$

$$x^{p^m} - x = x(x^{p^m-1} - 1)$$

Alf.  $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n} \Leftrightarrow \cancel{x^{pd} - 1} \mid x^{p^d-1} - 1 \mid x^{p^n-1} - 1$

$$(\Leftarrow) \quad x^{p^d-1} - 1 \mid x^{p^n-1} - 1 \Rightarrow x^{p^n-1} - 1 = (x^{p^d-1} - 1)q(x),$$

$$\nexists \alpha \in (\mathbb{F}_p^d)^* \Rightarrow \alpha^{p^d-1} - 1 = 0 \Rightarrow \alpha^{p^n-1} - 1 = 0 \Rightarrow \alpha \in (\mathbb{F}_p^n)^*$$

$$\therefore \mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$$

$(\Rightarrow) \quad \forall \alpha \in \mathbb{F}_{p^d}: (x-\alpha)$  factor de  $x^{p^d-1} - 1$

$\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n} \Rightarrow (x-\alpha)$  factor de  $x^{p^n-1} - 1$

Como  $x^{p^d-1} - 1$  tiene  $\#(\mathbb{F}_{p^d})^* = p^d - 1 \Rightarrow x^{p^d-1} - 1 \mid x^{p^n-1} - 1$

$$\begin{aligned}
 \text{Así } \mathbb{F}_{p^d} \subset \mathbb{F}_{p^n} &\iff x^{p^d-1} - 1 \mid x^{p^n-1} - 1 \\
 &\iff p^d - 1 \mid p^n - 1 \\
 &\cancel{\text{Cálculo de } \gcd(p^d-1, p^n-1)} \\
 &\iff d \mid n \quad (p^d-1 \mid p^n-1 \iff x^{d-1} \mid x^n - 1) \\
 \therefore \mathbb{F}_{p^d} \subset \mathbb{F}_{p^n} &\iff d \mid n.
 \end{aligned}$$

Ejercicio 5. Pruebe que  $x^{p^n-1} - 1 = \prod_{\alpha \in \mathbb{F}_{p^n}^*} (x - \alpha)$

En particular, para todo cuerpo finito:  $\prod_{\alpha \in \mathbb{F}_{p^n}^*} \alpha = (-1)^{p^n}$

Para  $p$  impar y  $n=1$ , pruebe el teorema de Wilson:

$$(p-1)! \equiv -1 \pmod{p}$$

Demonstración.

$\mathbb{F}_{p^n}$  cuerpo de descomposición de  $x^{p^n} - x \in \mathbb{F}_p[x]$ .

$x^{p^n} - x$  separable, ya que  $\text{mcd}(x^{p^n} - x, D(x^{p^n} - x)) = 1$

∴  $x^{p^n} - x$  tiene  $p^n$  raíces distintas, todas en  $\mathbb{F}_{p^n}$ .

Así,  $x^{p^n} - x = \prod_{\alpha \in \mathbb{F}_{p^n}^*} (x - \alpha)$ . Como  $x^{p^n} - x = x(x^{p^n-1} - 1)$

$$\therefore x^{p^n-1} - 1 = \prod_{\alpha \in \mathbb{F}_{p^n}^*} (x - \alpha)$$

Si  $x^{p^n-1} - 1 = \prod_{\alpha \in \mathbb{F}_{p^n}^*} (x - \alpha)$  podemos reemplazar  $x = 0$ ,

así

$$-1 = \prod_{\alpha \in \mathbb{F}_{p^n}^*} (-\alpha) \iff -1 = (-1)^{p^n-1} \prod_{\alpha \in \mathbb{F}_{p^n}^*} \alpha$$

$$\therefore \prod_{\alpha \in \mathbb{F}_{p^n}^*} \alpha = (-1)^{p^n}$$

Cuando  $n=1$ ,  $p$  impar, tenemos  $\mathbb{F}_p = \{1, \dots, p-1\}$

$$\therefore \prod_{\alpha \in \mathbb{F}_p^*} \alpha \equiv 1 \cdot 2 \cdot \dots \cdot (p-1) \equiv -1 \pmod{p}$$

$$\therefore (p-1)! \equiv -1 \pmod{p}.$$

Ejercicio 6. Sea  $q = p^n$  con  $p$  primo. ¿Para cuál  $q$  la extensión cuadrática  $\mathbb{F}_{q^2}$  de  $\mathbb{F}_q$  es de la forma  $\mathbb{F}_q(\sqrt{x})$ ?

Respuesta.

$$[\mathbb{F}_{q^2} : \mathbb{F}_q] = 2 \Rightarrow \mathbb{F}_{q^2} = \mathbb{F}_q(\alpha), \text{ donde } \alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q.$$

$$\text{m}_{\alpha, \mathbb{F}_q}(x) = x^2 + ax + b \Rightarrow \alpha^2 + a\alpha + b = 0$$

Si char  $\mathbb{F}_q \neq 2$  ( $p \neq 2$ ) :

$$\begin{aligned} \alpha^2 + a\alpha + b = 0 &\iff \alpha^2 + a\alpha + \frac{a^2}{4} = \frac{a^2}{4} - b \\ &\iff \left(\alpha + \frac{a}{2}\right)^2 = \frac{a^2 - 4b}{4} \in \mathbb{F}_q \end{aligned}$$

$$\text{Tomando } \sqrt{x} = \alpha + \frac{a}{2} \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$$

$$\mathbb{F}_{q^2} = \mathbb{F}_q(\alpha) = \mathbb{F}_q\left(\alpha + \frac{a}{2}\right) = \mathbb{F}_q(\sqrt{x})$$

∴ Cuando  $q$  no es potencia par,  $\mathbb{F}_{q^2} = \mathbb{F}_q(\sqrt{x})$ .

Ejercicio 7. Considerar  $f(x) = x^3 + x^2 + 1 \in \mathbb{F}_3[x]$ . Sea  $K \subset \overline{\mathbb{F}_3}$  el cuerpo de descomposición de  $f(x) \in \mathbb{F}_3[x]$ . Determinar el tamaño ~~de~~  $|K|$  de  $K$ , Demotstrar que  $x^2 + 1 \in K[x]$  se descompone sobre  $K$ .

Ejercicio 8. Sea  $F \subseteq K$  extensión algebraica de cuerpos.

Sea  $\alpha \in K$  tal que  $\alpha^n = 1$  para algún  $n \in \mathbb{N}$ . Demuestre que  $F(\alpha)/F$  es normal.

Dem. Vamos a suponer que  $\alpha \in K \setminus F$  (caso que importa)

$$\alpha^n = 1 \Rightarrow (\alpha^m)^n = 1 \quad \forall m \in \mathbb{N}$$

$\therefore \alpha, \alpha^2, \alpha^3, \alpha^4, \dots$ , raíces de  $x^n - 1 \in F[x]$

Como  $m_{\alpha, F}(x) \mid x^n - 1$ , entonces las raíces de  $m_{\alpha, F}(x)$  son  $\alpha^m$ ,  $m \in I$  (finito  $\subset \mathbb{N}$ ) ( $1 \in I$ )

$\therefore$  todas las raíces de  $m_{\alpha, F}(x)$  están en  $F(\alpha)$

$\therefore F(\alpha)/F$  normal.

Ejercicio 9. Sea  $K = F(\alpha)$ , donde  $K, F$  son cuerpos de característica  $p > 0$ . Si  $\alpha^p - \alpha = \beta \in F$ , demuestre que  $K/F$  es normal.

Dem.  $\alpha^p - \alpha = \beta \Rightarrow (\alpha + 1)^p - (\alpha + 1) = \beta$

$\therefore \alpha, \alpha + 1, \alpha + 2, \dots, \alpha + p - 1$  raíces de  $x^p - x - \beta$   
 $\in \overline{F[x]}$

Como  $m_{\alpha, F(x)} \mid x^p - x - \beta$ ,  $m_{\alpha, F(x)}$  comparte algunas (o todas) de estas raíces, que además están todas en  $K$ .

$\therefore m_{\alpha, F(x)}$  tiene todas sus raíces en  $K$

$\therefore K/F$  es normal.

Ejercicio 10. Demuestre que  $(\mathbb{Q}(\cos(\pi/9))) / \mathbb{Q}$  es una extensión de grado 3. Es normal?

Demonstración. Recordamos:  $\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta)$

$$\cos(\pi/3) = 4\cos^3(\pi/9) - 3\cos(\pi/9)$$

$$\frac{1}{2} = 4\cos^3(\pi/9) - 3\cos(\pi/9)$$

$$\frac{1}{2} = 8\cos^3(\pi/9) - 6\cos(\pi/9)$$

$$0 = 8\cos^3(\pi/9) - 6\cos(\pi/9) - \frac{1}{2}$$

$\therefore \delta = \cos(\pi/9)$  es raíz de  $8x^3 - 6x - \frac{1}{2} \in \mathbb{Q}[x]$

Afirmación:  $8x^3 - 6x - \frac{1}{2}$  irred  $\mathbb{Q}$ . ( $f(x) = 8x^3 - 6x - \frac{1}{2}$ )

dem. Raíces racionales  $= \{ \pm 1, \pm \frac{1}{2}, \pm \frac{1}{4}, \pm \frac{1}{8} \}$

$$f(1) = 8 - 6 - \frac{1}{2} \neq 0$$

$$f(-1) = -8 + 6 - \frac{1}{2} \neq 0$$

$$f(\frac{1}{2}) = 1 - 3 - \frac{1}{2} \neq 0$$

$$f(-\frac{1}{2}) = -1 + 3 - \frac{1}{2} \neq 0$$

$$f(\frac{1}{4}) = 8 \cdot \frac{1}{64} - 6 \cdot \frac{1}{4} - \frac{1}{2} = \frac{1-20}{8} \neq 0$$

$$f(-\frac{1}{4}) = -\frac{1}{8} + \frac{3}{2} - \frac{1}{2} = \frac{-1+12-8}{8} \neq 0$$

$$f(\frac{1}{8}) = 8 \cdot \frac{1}{512} - 6 \cdot \frac{1}{8} - \frac{1}{2} = \frac{1}{64} - \frac{3}{4} - \frac{1}{2} \neq 0$$

$$f(-\frac{1}{8}) = -\frac{1}{64} + \frac{3}{4} - \frac{1}{2} \neq 0$$

$\therefore f$  irreducible  $\mathbb{Q}$

$$\therefore [\mathbb{Q}(\delta) : \mathbb{Q}] = 3$$

•  $(\mathbb{Q}(\cos(\pi/9))) / \mathbb{Q}$  es normal?

Como  $\delta = \cos(\pi/q)$  es raíz de  $8x^3 - 6x - 1$ , podemos dividir:

$$8x^3 - 6x - 1 \text{ en } x - \delta$$

$$8x^3 - 6x - 1 : x - \delta = 8x^2 + 8\delta x + 8\delta^2 - 6$$

$$\underline{8x^2 - 8\delta x}$$

$$\underline{8\delta x^2 - 6x - 1}$$

$$\underline{8\delta x^2 - 8\delta^2 x}$$

$$\underline{8\delta^2 x - 6x - 1}$$

$$\underline{8\delta^2 x - 8\delta^3}$$

$$\begin{array}{r} 8\delta^3 - 6x - 1 = -6x + 6\delta \\ -6x + 6\delta \\ \hline 0 \end{array}$$

	$0$	$\pi/6$	$\pi/4$	$\pi/3$	$\pi/2$
$s$	0	1	2	3	4
$c$	$\sqrt{4}$	$\sqrt{3}$	2	1	2

Tenemos  $1Q(x) = 8x^2 + 8\delta x + 8\delta^2 - 6$ , cuyo discriminante es

$$\Delta = 64\delta^2 - 4 \cdot 8(8\delta^2 - 6) = 64\delta^2 - 48\delta^2 + 48 \cdot 6$$

$$= -3 \cdot 8^2 \delta^2 + 3 \cdot 8^2 = 3 \cdot 8^2 (1 - \delta^2)$$

$$\Delta = 3 \cdot 8^2 (1 - \delta^2), \text{ donde } 1 - \delta^2 = \operatorname{sen}(\pi/q)$$

$$\text{Raíces: } \bar{x} = \frac{-8\delta \pm \sqrt{3} \operatorname{sen}(\pi/q)}{8 \cdot 2} = \frac{-\cos(\pi/q) \pm \operatorname{sen}(\pi/q)\sqrt{3}}{2}$$

$$\text{Supongamos que } \bar{x}_1 = \frac{-\cos(\pi/q) + \operatorname{sen}(\pi/q)\sqrt{3}}{2} \in \mathbb{Q}(\cos(\pi/q))$$

$$\therefore \operatorname{sen}(\pi/q)\sqrt{3} \in \mathbb{Q}(\cos(\pi/q))$$

$$\begin{aligned} \frac{\sqrt{3}}{2} &= \operatorname{sen}(\pi/3) = \operatorname{sen}(3\delta) = \operatorname{sen}(2\delta)\cos(\delta) + \operatorname{sen}(\delta)\cos(2\delta) \\ &= 2\operatorname{sen}(\delta)\cos^2(\delta) + \operatorname{sen}(\delta)(-1 + 2\cos^2(\delta)) \end{aligned}$$

$$\frac{\sqrt{3}}{2} = \operatorname{sen}(\delta)(4\cos^2(\delta) - 1)$$

$$\therefore \operatorname{sen}(\pi/q)\sqrt{3} = 2\operatorname{sen}^2(\delta)(4\cos^2(\delta) - 1)$$

$$\therefore \operatorname{sen}^2(\delta) \in \mathbb{Q}(\cos(\pi/q))$$

$$1 - \cos^2(\delta) \quad \text{Certo siempre!}$$

Derivándose, a partir que  $1 - \cos^2(\delta) \in \mathbb{Q}(\cos(\delta))$ , podemos demostrar que  $\bar{x} \in \mathbb{Q}(\cos(\delta))$

$$\therefore (\mathbb{Q}(\cos(\delta)) / \mathbb{Q}) \text{ es normal!}$$

Ejercicio 11. Sea  $F$  cuerpo. Muestra que el anillo de polinomios  $F[x]$  posee infinitos ideales primos. Pueba que los cuerpos algebraicamente cerrados poseen cardinalidad infinita.

Dem.  $F$  cuerpo  $\Rightarrow F[x]$  dominio Euclídeo.

$$(p(x)) \text{ primo} \Leftrightarrow p(x) \text{ primo.}$$

Supongamos que  $\{p_1(x), \dots, p_r(x)\}$  son todos los primos en  $F[x]$ , entonces  $q(x) = p_1(x)p_2(x) \dots p_r(x) + 1 \in F[x]$  no es primo ( $q(x) \neq p_j(x) \quad \forall j \in \{1, \dots, r\}$ ).

Como  $F[x]$  D.F.U :  $\exists j_0 : p_{j_0}(x) \mid q(x)$

$$\therefore p_{j_0}(x) \mid 1 \quad (\Rightarrow \Leftarrow)$$

$\therefore F[x]$  posee infinitos primos.

$\therefore F[x]$  posee infinitos ideales primos.

Por demostrar :  $\overline{F} = F \Rightarrow \# F = \infty$ .

Supongamos que  $F = \{a_1, \dots, a_n\}$  ( $\# F = n < \infty$ ).

$p_{a_i}(x) = (x - a_i) \in F[x]$  es primo (irreducible)  $\forall i$ ,

$$\therefore \tilde{p}(x) = \left( \prod_{i=1}^n p_{a_i}(x) \right) + 1$$

debe tener todas sus raíces en  $F$ , pero  $\tilde{p}(a_i) \neq 0 \quad \forall i$  ~~(irreducible)~~

$$\therefore \# F = \infty.$$

Ejercicio 12. Sea  $K$  un cuerpo cuya única extensión algebraica  
y separable es  $\bar{K}$ . ¿Es  $K$  algebraicamente cerrado?

Resp.  $p(x) \in K[x]$ . Sea  $D_0 = \bar{K}$ , entonces

$$p(x) = a(x - \alpha_1) \dots (x - \alpha_r), \text{ donde } a \in K, \alpha_i \in D_0.$$

$$\frac{\mathbb{K}(\alpha_j)}{\mathbb{K}} \text{ algebraica } \Leftrightarrow \mathbb{K}(\alpha_j) = \bar{K} \therefore \alpha_j \in \bar{K}$$

PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE  
FACULTAD DE MATEMÁTICAS  
DEPARTAMENTO DE MATEMÁTICA

MAT2218 (Álgebra II)

Interrogación N° 3 Martes, 19 de Noviembre, 2013

Importante: Motive su respuesta, mencione el teorema, proposición, lema , etc. que usted utiliza.

1. a) Sea  $\zeta = e^{2\pi i/37}$  y  $\alpha := \zeta + \zeta^{10} + \zeta^{26}$ . Demuestre que  $\mathbb{Q}(\alpha)/\mathbb{Q}$  es Galois y calcule su grupo de Galois.  
b) Calcule el grupo de Galois de  $(x^2 + 1)(x^2 + 2)(x^2 + 4)$  sobre  $\mathbb{F}_7$ .

2. a) Sea  $K/F$  finita y Galois y tal que  $\text{Gal}(K/F) \simeq S_4$ . Considere

$$\mathcal{L} = \{L \mid L \text{ cuerpo intermedio } F \subset L \subset K \text{ tal que } [L : F] = 12\}$$

Calcular  $|\mathcal{L}|$  y determine todo  $L \in \mathcal{L}$  tal que  $L/F$  es Galois.

- b) Calcule el orden del grupo de Galois de  $x^{16} + 1$  sobre  $\mathbb{Q}$ .

3. Sean  $K_1$  y  $K_2$  finita y Galois sobre  $F$ .

- a) Demuestre que  $K_1 K_2/F$  es Galois y que la aplicación

$$\Psi : \text{Gal}(K_1 K_2/F) \rightarrow \text{Gal}(K_1/F) \times \text{Gal}(K_2/F)$$

dada por  $\Psi(\sigma) = (\sigma|_{K_1}, \sigma|_{K_2})$  define un monomorfismo de grupos.

- b) Demuestre que:  $\Psi$  es un isomorfismo  $\Leftrightarrow K_1 \cap K_2 = F$ .  $\text{TA LOKO}$

Duración: 2 horas

$$\begin{array}{ccccccccc} & 1 & 2 & 4 & 8 & 16 \\ & 3 & 5 & 6 & 7 & 9 & 11 & 13 & 15 \\ 37 & & 74 & & & & & & \end{array}$$

100

$$\begin{array}{r} 260 \\ \underline{-37} \\ 223 \end{array}$$

$$370 : 2 = 18$$

$$\begin{aligned} & (34)(12)(34) = (12) \\ & (12)(17)(13) = (23) \end{aligned}$$

Problema 1

(a) Sea  $\zeta = e^{\frac{2\pi i}{37}}$ ,  $\alpha := \zeta + \zeta^{10} + \zeta^{26}$ . Demuestre que  $\mathbb{Q}(\alpha)/\mathbb{Q}$  es Galois y calcule su grupo de Galois.

(b) Calcule el grupo de Galois de  $(x^2+1)(x^2+2)(x^4+4)$  sobre  $\mathbb{F}_7$ .

Dem. Sabemos que  $\mathbb{Q}(\zeta)/\mathbb{Q}$  es Galoiana con  $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/37\mathbb{Z})^* \cong C_{36}$  (37 primo).

$\therefore \mathbb{Q}(\zeta)/\mathbb{Q}$  extensión abeliana

$\therefore \forall H \leq \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$  ~~es abeliana~~  
 $H$  normal en  $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$

Por segundo teorema de la teoría de Galois,  $\exists H \triangleleft \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$  tal que  $\mathbb{Q}(\alpha) = \mathbb{Q}(\zeta)^H$ . Como  $H$  es normal

$\mathbb{Q}(\alpha)/\mathbb{Q}$  Galoiana.

También,  $\text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) \cong \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})/H$ . Luego debemos calcular  $H$ . ~~obviamente~~

$\forall \sigma \in \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) : \sigma(\zeta) = \zeta^m$ ,  $m=0, \dots, 36$

$\sigma \in H \iff \sigma(\alpha) = \alpha$

$$\begin{aligned} \text{Ahora, } \sigma(\alpha) &= \sigma(\zeta) + \sigma(\zeta)^{10} + \sigma(\zeta)^{26} \\ &= \zeta^m + \zeta^{10m} + \zeta^{26m} \\ &= \zeta + \zeta^{10} + \zeta^{26} \end{aligned}$$

Deben distinguir 3 casos:

i)  $\zeta^m = \zeta$

ii)  $\zeta^m \neq \zeta^{10}$

iii)  $\zeta^m = \zeta^{26}$

ii)  $\zeta^m = \zeta \Rightarrow m = 1 + 37n, n \in \mathbb{Z} \setminus \{0\}, \mathbb{N}$

$\therefore m \equiv 1 \pmod{37}$

$\begin{cases} m \equiv 1 \pmod{37} \\ 10m \equiv 10 \pmod{37} \\ 26m \equiv 26 \pmod{37} \end{cases}$

$\begin{cases} m \equiv 1 \pmod{37} \\ 10m \equiv 26 \pmod{37} \\ 26m \equiv 10 \pmod{37} \end{cases}$

El primer sistema tiene solución  $m \equiv 1 \pmod{37}$ . El segundo no tiene solución!

(ii)  $\begin{cases} m \equiv 10 \pmod{37} \\ 10m \equiv 1 \pmod{37} \\ 26m \equiv 26 \pmod{37} \end{cases}$

$\begin{cases} m \equiv 10 \pmod{37} \\ 10m \equiv 26 \pmod{37} \\ 26m \equiv 1 \pmod{37} \end{cases}$

$\begin{cases} m \equiv 10 \pmod{37} \\ m \equiv 1 \pmod{37} \end{cases}$

$\begin{cases} m \equiv 19 \cdot 26 \cdot 15 \pmod{37} \\ m \equiv 11 \cdot 19 \pmod{37} \\ m \equiv 14 \pmod{37} \end{cases}$

S.S

S.S

(iii)  $\begin{cases} m \equiv 26 \pmod{37} \\ 10m \equiv 1 \pmod{37} \\ 26m \equiv 10 \pmod{37} \end{cases}$

$\begin{cases} m \equiv 26 \pmod{37} \\ 10m \equiv 10 \pmod{37} \\ 26m \equiv 1 \pmod{37} \end{cases}$

S.S.