

EJERCICIO 49. Sea  $F$  un cuerpo de descomposición de  $f = X^3 + X + 1 \in \mathbb{F}_2[X]$  y  $\alpha \in F$  una raíz de  $f$ . Razonar que  $F = \mathbb{F}_2(\alpha)$ . Resolver, en  $F$ , las siguientes ecuaciones, expresando las soluciones en función de  $\alpha$ :

$$x^3 + x + 1 = 0; \quad x^3 + x^2 + 1 = 0; \quad x^2 + x + 1 = 0.$$

Tratemos con cuerpos finitos; por tanto, puesto que  $f(x) = f(i)$  tenemos que  $f$  es irreducible de grado 3, aplicando la teoría tenemos que  $F \cong \mathbb{F}_8$ . Veamos ahora que  $F = \mathbb{F}_2(\alpha)$ , puesto que  $\mathbb{F}_2 \subseteq F$  es una extensión de cuerpos finitos, tenemos que es una extensión de gálibo, de donde es válido y por tanto, contiene a todas las raíces a la misma, como  $\alpha \in F$  y es raíz tenemos que  $\mathbb{F}_2(\alpha) \subseteq F$  y, por ese razonamiento  $\mathbb{F}_2(\alpha) \cong F$ .

Vamos a buscar, si es posible, las soluciones en  $\mathbb{F}_2(\alpha)$  de las ecuaciones impuestas; las raíces de  $f$  son  $\alpha, \alpha^2$  y  $\alpha^4$  puesto que el automorfismo de Frobenius de la extensión viene dado por

$$\gamma(\alpha) = \alpha^2$$

Para el otro caso, como también es irreducible, un razonamiento análogo nos dice que sus raíces son  $\alpha^3, \alpha^5$  y  $\alpha^6$  puesto que no comparten raíces; estas son las raíces de  $x^3+x+1 \in \mathbb{F}_2[x]$  también irreducible en  $\mathbb{F}_2[x]$ .

Para el último caso, supongamos que tiene solución en  $\mathbb{F}_8$ , en ese caso, como  $\mathbb{F}_8$  contiene todas las raíces de  $x^3-x \in \mathbb{F}_2[x]$  y este se descompone como producto de todos los irreducibles de grado divisor de 3 tendríamos que  $2|3$  lo cual es una contradicción. Este argumento es válido porque  $x^3+x+1 \in \mathbb{F}_2[x]$  es irreducible.

EJERCICIO 50. Sea  $K$  un cuerpo de descomposición de  $f = X^3 + X + 1 \in \mathbb{F}_4[X]$  y  $\alpha \in K$  una raíz de  $f$ . Razonar que  $K = \mathbb{F}_4(\alpha)$ . Resolver, en  $K$ , las siguientes ecuaciones, expresando las soluciones en función de  $\alpha$ :

$$x^3 + x + 1 = 0; \quad x^3 + x^2 + 1 = 0; \quad x^2 + x + 1 = 0.$$

Construir, si es posible, una base de  $K$  sobre  $\mathbb{F}_2$  usando  $\alpha$  y una solución de la tercera ecuación.

Primero estudiemos si  $f$  es irreducible en  $\mathbb{F}_7[x]$ ; para ello, basta ver que no tiene raíces en  $\mathbb{F}_7$  y que no tiene factores irreducibles de grado 2. Es fácil ver que no tiene raíces en  $\mathbb{F}_7$  y que los irreducibles de grado 2 en  $\mathbb{F}_7[x]$  son:

$$x^2+x+1, \quad x^2+x+3, \quad x^2+2x+2, \quad x^2+2x+3, \quad x^2+3x+3$$

Para ver si estos faltan alguno, podemos ver cuántos polinomios irreducibles de grado 2 hay en  $\mathbb{F}_7$ ; no obstante, el polinomio de partida no es divisible por ninguno de ellos, de donde  $f$  es irreducible.

Ahora bien, realizando un razonamiento análogo al ejercicio anterior obtenemos que  $\mathbb{F}_7(\alpha) \cong \mathbb{F}_{64}$  de donde  $\alpha$  tiene orden multiplicativo 63 siendo  $\mathbb{F}_{64}^*$  como  $\langle \alpha \rangle$ .

Resolvemos cada una de las ecuaciones:

- Puesto que  $\alpha$  es raíz de  $f$  tenemos que  $\alpha, \alpha^4$  y  $\alpha^16$  son las raíces de  $f$  usando el automorfismo de Frobenius de la extensión  $\mathbb{F}_7 \subseteq \mathbb{F}_{64}$

i) Puesto que es irreducible y tiene 6 raíces que admite solución; además, del ejercicio anterior, sabemos que las raíces en  $\mathbb{F}_8$  son  $\alpha^3, \alpha^5$  y  $\alpha^6$ .

ii.) Para ver esto, como  $\mathbb{F}_{64}$  contiene todas las raíces del polinomio  $x^{64}-x \in \mathbb{F}_2[X]$  y éste se descompone como producto de todos los polinomios irreducibles de grado un divisor de 6 y 216 raíces que tiene solución en  $\mathbb{F}_{64}$ . Si  $b \in \mathbb{F}_{64}$  es una raíz de ese polinomio tendríamos que  $\mathbb{F}_2(b) \leq \mathbb{F}_{64}$  es cuerpo de descomposición del polinomio y es de Galois por ser una extensión de cuerpos finitos. Además, podemos asegurar que  $\mathbb{F}_2(b) \cong \mathbb{F}_4$  de donde buscamos un elemento de  $\mathbb{F}_{64}^\times$  con orden multiplicativo 3, ese elemento puede ser  $\alpha^{21}$  y junto al automorfismo de Frobenius de  $\mathbb{F}_2 \leq \mathbb{F}_4$  obtenemos que  $\alpha^{12}$  es la otra raíz. Podemos asegurar esto gracias a que  $x^2+x+1$  es el único polinomio irreducible de grado 2 en  $\mathbb{F}_2[8]$ .

Para construir la  $\mathbb{F}_2$ -base de  $K$  basta ver que disponemos de la extensión

$$\mathbb{F}_2 \leq \mathbb{F}_2(b) \leq K$$

de donde la  $\mathbb{F}_2$ -base, gracias al tema de la tarea tenemos que, como  $\{1, b\}$  es  $\mathbb{F}_2$ -base de  $\mathbb{F}_2(b)$  y  $\{\alpha, \alpha^2\}$  es una  $\mathbb{F}_2(b)$ -base de  $K$ ,  $\{1, \alpha, \alpha^2, b, \alpha b, \alpha^2 b\}$  es una  $\mathbb{F}_2$ -base de  $K$ .

En (\*) hemos visto que  $\deg(\text{Irr}(a, \mathbb{F}_2(b))) = 3 = \deg(f)$  y que  $\mathbb{F}_2(b) \cong \mathbb{F}_4$ .

EJERCICIO 51. Calcular el número de polinomios irreducibles de grado 6 en  $\mathbb{F}_2[X]$ . (Nota: hay una fórmula general, si la encuentras en la web, no la uses, no se trata de eso).

Para ello, consideraremos el cuerpo  $\mathbb{F}_{64}$  y el polinomio  $x^{64}-x \in \mathbb{F}_2[X]$ ; sabemos que este polinomio se descompone como producto de todos los polinomios irreducibles de  $\mathbb{F}_2$  con grado un divisor de 6. Algorábiola, sabemos lo siguiente:

- i)  $\{x, x+1\}$  son los polinomios irreducibles de grado 1.
- ii)  $\{x^2+x+1\}$  es el único de grado 2
- iii)  $\{x^3+x^2+1, x^3+x+1\}$  son los polinomios irreducibles de grado 3.

Por tanto, sabemos que hay 9 polinomios irreducibles de grado 6 en  $\mathbb{F}_2[X]$ .

EJERCICIO 52. Calcular los grupos de Galois sobre  $\mathbb{Q}$  de los polinomios  $f = (X^2 + X + 1)(X^2 - 3)$  y  $g = (X^2 + X + 1)(X^2 + 3)$ .

Procedemos primero con  $f$ ; sabemos que dicho grupo es un subgrupo de  $S_4$ ; además, vamos a buscar calcular el cuerpo de descomposición de  $f$ . Para ello, consideraremos  $\omega \in \mathbb{C}$  la raíz cúbica primitiva de la unidad  $\omega = \frac{1}{2} + \frac{i\sqrt{3}}{2}$  y es claro que las raíces de  $f$  son  $\{\omega, \omega^2, \sqrt{3}, -\sqrt{3}\}$ ; por tanto,  $K = \mathbb{Q}(\omega, \sqrt{3})$ .

Observemos que  $w \in \mathbb{Q}(\sqrt[3]{\lambda})$  y que  $i\sqrt{3} \in \mathbb{Q}(w)$  luego  $K = \mathbb{Q}(i\sqrt{3}, w)$ . Además, es obvio que  $i\sqrt{3} \in \mathbb{Q}(i, \sqrt{3})$  así como que  $i \in \mathbb{Q}(i\sqrt{3}, \sqrt{3})$  pues  $i = \frac{i\sqrt{3}}{\sqrt{3}}$ ; por tanto,  $K = \mathbb{Q}(i, \sqrt{3})$ .

Es necesario recordar que  $\mathbb{Q} \subset K$  es de Galois puesto que  $f$  es separable y  $K$  es su cuerpo de descomposición; cuando ahora (sin todo lo para formalia perturbante) tenemos que

$$\text{Aut}(K) = \{ \gamma_{jk} ; j, k = 0, 1; w = 0, 1 \}$$

donde  $\gamma_{00} = (-1)^0 = 1$ ,  $\gamma_{01} = (-1)^1 = -1$ ,  $\gamma_{10} = i(-1)^0 = i$ ,  $\gamma_{11} = i(-1)^1 = -i$ . Puesto que  $f$  es irreducible en  $\mathbb{Q}[x]$  pues tiene factores de orden 2 podrá ser cualquier subgrupo de  $S_3$ . Análogamente, se trabaja con  $w$ .

EJERCICIO 53. Calcular el cardinal del grupo de Galois sobre  $\mathbb{Q}$  del polinomio  $f = (X^3 + X + 1)(X^2 + 1)$ .

Para ello, buscamos tener una idea del cuerpo de descomposición de  $f$ ; por tanto, como anteriormente debemos saber cuáles raíces reales tiene; puesto que  $h = x^3 + x + 1$  es elíptico con raíces reales tenemos que  $h' = 3x^2 + 1 > 0$  luego sólo hay una raíz real  $r \in \mathbb{R}$  y tendría  $\alpha$  y  $\bar{\alpha}$  como raíces complejas. Por tanto, es fácil deducir que  $K = \mathbb{Q}(i, r, \alpha)$ . Buscamos aplicar el lema de la Torre puesto que la conexión de Galois nos asegura que  $[K : \mathbb{Q}] = |\text{Aut}(K)|$ .

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(i)] \cdot [\mathbb{Q}(i) : \mathbb{Q}] = 2 \cdot [\mathbb{Q}(i) : \mathbb{Q}]$$

Por tanto, el problema se reduce a probar que  $[\mathbb{Q}(i) : \mathbb{Q}] = 6$ ; para ello, como  $h$  es irreducible en  $\mathbb{Q}(i)[x]$  tenemos que  $K$  es su cuerpo de descomposición, donde  $\mathbb{Q}(i)[x]$  es de Galois con  $\text{Aut}_{\mathbb{Q}(i)}(K) \leq S_3$  teniendo que ser irreducible. Como  $\text{Disc}(f) = -31$  deducido  $\Delta(h) = i\sqrt{3} \notin \mathbb{Q}(i)$  pues 31 es primo y  $x^2 - 31$  es irreducible en  $\mathbb{Q}[x]$ . Por tanto,  $\text{Aut}_{\mathbb{Q}(i)}(K) \cong S_3$  y concluimos  $[K : \mathbb{Q}] = 12$ .

(\*) Para ver esto, podemos ver que  $i \notin \mathbb{Q}(i)$  y  $\alpha \notin \mathbb{Q}(i)$ ; lo primero se debe a que, en caso contrario  $r \in \mathbb{Q}$  deducido  $h$  sería irreducible en  $\mathbb{Q}[x]$ . El segundo caso se debe a que, si no fuera así, como  $\alpha \notin \mathbb{Q}$  tenemos que  $\alpha$  tendría grado 2 sobre  $\mathbb{Q}$  deducido, como  $\alpha$  es raíz de la ecuación  $\text{Irr}(\alpha, \mathbb{Q}) \mid h$  deducido  $\alpha \mid 3$ .

EJERCICIO 54. Tomemos  $f = (X^3 - 2)(X^2 - 3) \in \mathbb{Q}[X]$  y  $K$  el cuerpo de descomposición sobre  $\mathbb{Q}$  de  $f$ .

1. Decidir razonadamente si  $i + \sqrt{3} \in K$ .
2. Calcular razonadamente  $[K : \mathbb{Q}]$ .
3. Describir los elementos del grupo  $\text{Aut}(K)$ .
4. Describir los elementos de  $\text{Aut}_{\mathbb{Q}(i+\sqrt{3})}(K)$  y decidir si es un subgrupo normal de  $\text{Aut}(K)$ .

Para trabajar en el problema, lo primero que debemos hacer es calcular el cuerpo de descomposición de  $f$ ; sus raíces son; considerando  $w \in \mathbb{C}$  la raíz cúbica primitiva de la unidad  $w = \frac{-1}{2} + i\frac{\sqrt{3}}{2}$ :

$$\{ \sqrt[3]{2}, w\sqrt[3]{2}, w^2\sqrt[3]{2}, \sqrt{3}, -\sqrt{3} \}$$

Por tanto, tenemos que  $K = \mathbb{Q}(w, \sqrt[3]{2}, \sqrt{3})$ ; veamos que  $K = \mathbb{Q}(i, \sqrt{3}, \sqrt[3]{2})$ , es decir que  $K = \mathbb{Q}(i, \sqrt{3}, \sqrt[3]{2})$ , para la inclusión contraria debemos probar que  $i \in K$ , pero  $i = \frac{w(w+1)}{\sqrt{3}}$  luego queda la igualdad

a) De la igualdad probada ya es fácil ver que  $i + \sqrt{3} \in K$ .

b) Para ello, buscamos aplicar el lema de la Torre, el cual nos asegura que

$$[K:\mathbb{Q}] = [K : \mathbb{Q}(\sqrt{3}, \sqrt{5})] \cdot [\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = 2 \cdot [\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}].$$

Donde hemos usado que  $\text{Irr}(i, \mathbb{Q}(\sqrt{3}, \sqrt{5})) = x^2 + i$  puesto que  $\mathbb{Q}(\sqrt{3}, \sqrt{5})$  no contiene ningún número complejo.

Para calcular  $[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}]$  basta ver que  $x^3 - 3 \in \mathbb{Q}[x]$  es irreducible en  $\mathbb{Q}[x]$  así como también lo es  $x^2 - 3 \in \mathbb{Q}[x]$ . Por tanto, el lema de la Torre nos dice que

$$[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = 2 \cdot [\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{3})]$$

$$[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = 3 \cdot [\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{3})]$$

Luego podemos ya deducir que  $[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = 6$  (realmente necesitamos probarlo antes, pero  $\sqrt{3}$  y  $\sqrt{5}$  son raíces de f de donde se obtiene la desigualdad). Entonces  $[K:\mathbb{Q}] = 12$ .

c) Este ejercicio consiste en usar tres veces la proposición de extensión para obtener

$$\begin{aligned} \gamma_{\text{gal}} : K &\longrightarrow K \\ i &\longmapsto \zeta_3^k i \quad k=0,1 \\ \sqrt{2} &\longmapsto \omega^k \sqrt{2} \quad k=0,1,2 \\ \sqrt{3} &\longmapsto \zeta_4^j \sqrt{3} \quad j=0,1 \end{aligned}$$

d) Por otro lado, la conexión de Galois nos dice que su subcuerpo correspondiente es  $K^{\text{Aut}(K/\mathbb{Q}(\alpha))^{(1)}}$ ; por tanto, buscamos aquellos elementos de  $\text{Aut}(K)$  que dejan fija a  $i\sqrt{3}$ ; estos son  $\gamma_{\text{gal}}$  con  $k=0,1,2$ . Por tanto,  $|\text{Aut}_{\mathbb{Q}(\sqrt{3})}(K)| = 3$ . Para que sea normal es necesario y suficiente que  $\mathbb{Q} \subseteq \mathbb{Q}(i, \sqrt{3})$  sea una extensión de Galois; pero si consideramos  $g = (x^2 + i)(x^2 - 3) \in \mathbb{Q}[x]$  tenemos que es separable y que  $\mathbb{Q}(i\sqrt{3}) = \mathbb{Q}(i, \sqrt{3})$  es su cuerpo de descomposición (luego es de Galois y por tanto  $\text{Aut}_{\mathbb{Q}(i+\sqrt{3})}(K) \trianglelefteq \text{Aut}(K)$ ).

En (\*) hemos usado que si  $\alpha = i\sqrt{3}$  entonces  $i = \frac{4-\alpha^2}{2\alpha}$  y  $\sqrt{3} = \alpha - i$  obteniendo la igualdad.

EJERCICIO 55. Sea  $f = X^3 - 3X + 1 \in \mathbb{Q}[X]$  y  $\alpha$  cualquier raíz real de  $f$ . Demostrar que el cuerpo de descomposición de  $f$  sobre  $\mathbb{Q}$  es  $\mathbb{Q}(\alpha)$ .

Para resolver este ejercicio, lo primero que nos preguntaremos sobre  $f$  es la irreducibilidad de  $f$ ; puesto que  $f \in \mathbb{Z}[x]$  las únicas raíces posibles son  $\pm 1 \pm i\sqrt{3}$  debido a  $f(1) = -1$  y  $f(-1) \neq 0$  (luego es irreducible en  $\mathbb{Q}[x]$  al ser de grado 3 y sin raíces en  $\mathbb{Q}$ ). Sea ahora  $K$  el cuerpo de descomposición de  $f$ ; puesto que este es irreducible tenemos que  $\mathbb{Q} \subseteq K$  es de Galois; de donde  $\text{Aut}(K) \leq S_3$  (análogamente, sería  $S_3$  o  $A_3$ ). Como  $\text{Disc}(f) = 81$  tenemos que  $\text{Aut}(f) \leq \mathbb{Q}$  de donde  $\text{Aut}(K) \cong A_3$  y  $[K:\mathbb{Q}] = |\text{Aut}(K)| = 3$ . Como  $\text{Irr}(\alpha, \mathbb{Q}) = f$  tenemos que  $[\mathbb{Q}(\alpha):\mathbb{Q}] = 3$  de donde se deduce que  $K = \mathbb{Q}(\alpha)$ .



EJERCICIO 56. Sea  $K$  el cuerpo de descomposición del polinomio  $f = (X^2 + 3)(X^3 - 3) \in \mathbb{Q}[X]$ . Calcular todos los subcuerpos de  $K$ . Demostrar que  $\mathbb{Q}(\sqrt[3]{3} + i\sqrt{3}) = K$ .

Comenzamos calculando el cuerpo de descomposición de  $f$ ; sea  $\omega \in \mathbb{C}$  una raíz cuarta primitiva de la unidad, considero  $\omega = \frac{1}{2} + \frac{i\sqrt{3}}{2}$ ; las raíces de  $f$  son:

$$\{\sqrt[3]{3}, -i\sqrt[3]{3}, \sqrt[3]{3}, \omega\sqrt[3]{3}, \omega^2\sqrt[3]{3}\}$$

Por tanto, deducimos ya que  $K = \mathbb{Q}(\omega, i\sqrt{3}, \sqrt[3]{3})$ ; como  $\omega \in \mathbb{Q}(i\sqrt{3})$  y  $\mathbb{Q}(i\sqrt{3}) \subseteq \mathbb{Q}(\omega)$  tenemos que  $K = \mathbb{Q}(i\sqrt{3}, \sqrt[3]{3})$  de donde el lema de la Torre nos dice que  $|\text{Aut}(K)| = 6$  puesto que  $[K : \mathbb{Q}(\sqrt[3]{3})] = 2$  ya que  $x^2 + 3 = \text{Irr}(i\sqrt{3}, \mathbb{Q}(\sqrt[3]{3}))$  puesto que  $\mathbb{Q}(\sqrt[3]{3})$  no contiene números complejos; esto se traduce que  $x^3 - 3 = \text{Irr}(\sqrt[3]{3}, \mathbb{Q})$  por Eisenstein aplicado a  $p=3$ .

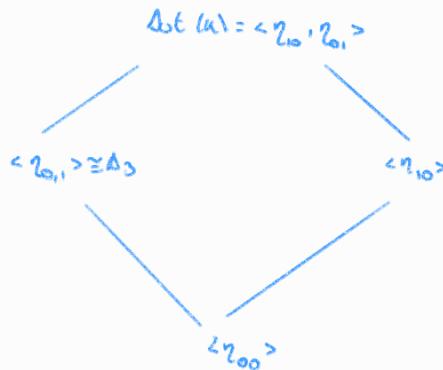
Aplicando ahora la proposición de extensión con  $p_1 = x^2 + 3$  y  $p_2 = x^3 - 3$  obtenemos que

$$\text{Aut}(K) = \{\eta_{j,0} : j=0,1 ; \ell=0,1,2\}$$

donde  $\eta_{j,0}(\sqrt[3]{3}) = (-1)^j i\sqrt{3}$  y  $\eta_{j,0}(\sqrt[3]{3}) = \omega^j \sqrt[3]{3}$ . Buscamos identificar cuáles el grupo; hay tres operaciones:  $\circ$  es un círculo de orden 6,  $\circ$  biejes  $S_3$ .

$$\begin{matrix} \eta_{0,0} & \eta_{1,0} & \eta_{0,1} & \eta_{1,1} & \eta_{0,2} & \eta_{1,2} \\ 1 & 2 & 3 & 2 & 3 & 2 \end{matrix}$$

por tanto, descartamos el círculo y por tanto,  $\text{Aut}(K) \cong S_3$ . El retículo de subgrupos es:



Al usar ahora la conexión de Galois tenemos que los subcuerpos de  $K$  son  $K^{Aut(K)} = \mathbb{Q}$ ,  $K^{<\eta_{0,0}>} = K$ ,  $K^{<\eta_{0,1}>}$  y  $K^{<\eta_{1,0}>}$ .

- i) Sabemos bie que  $\eta_{0,1}$  deja fijo  $i\sqrt{3}$  de donde  $\mathbb{Q}(i\sqrt{3}) \subseteq K^{<\eta_{0,1}>}$  además  $[K^{<\eta_{0,1}>} : \mathbb{Q}] = \frac{|\text{Aut}(K)|}{|\text{Aut}_{\mathbb{Q}(i\sqrt{3})}(K)|}$  por tanto  $[K^{<\eta_{0,1}>} : \mathbb{Q}] = 2 = [\mathbb{Q}(i\sqrt{3}) : \mathbb{Q}]$  entonces  $\mathbb{Q}(i\sqrt{3}) \cong K^{<\eta_{0,1}>}$
- ii) De la misma manera se deduce que  $K^{<\eta_{0,1}>} \cong \mathbb{Q}(\sqrt[3]{3})$ .

Para probar esto último bastaría probar que  $\eta_{0,0}$  es el único que deja fijo a  $\sqrt[3]{3} + i\sqrt{3}$  porque ya sabemos que  $\mathbb{Q}(i\sqrt{3} + \sqrt[3]{3}) \subseteq K$  de forma trivial por tanto, si vemos que  $|\text{Aut}_{\mathbb{Q}(i\sqrt{3} + \sqrt[3]{3})}(K)| = 1$  obtendremos por la conexión de Galois que  $[K : \mathbb{Q}(i\sqrt{3} + \sqrt[3]{3})] = 1$  consiguiendo la igualdad.

$$\eta_{0,0}(\alpha = i\sqrt{3} + \sqrt[3]{3}) = \alpha$$

$$\eta_{1,0}(\alpha) = -i\sqrt{3} + \sqrt[3]{3} \neq \alpha$$

$$\eta_{0,1}(\alpha) = i\sqrt{3} + \omega\sqrt[3]{3} \neq \alpha$$

$$\eta_{1,1}(\alpha) = -i\sqrt{3} + \omega^2\sqrt[3]{3} \neq \alpha$$

$$\eta_{0,2}(\alpha) = i\sqrt{3} + \omega^2\sqrt[3]{3} \neq \alpha$$

$$\eta_{1,2}(\alpha) = -i\sqrt{3} + \omega^2\sqrt[3]{3} \neq \alpha$$

Para ver las dos igualdades basta considerar parte real o imaginaria para llegar a contradicción.

EJERCICIO 57. Sea  $F$  un cuerpo de descomposición de  $f = X^6 + X + 1 \in F_2[X]$  y  $\alpha \in F$  una raíz de  $f$ .

1. Razonar que  $F = F_2(\alpha)$ .
2. Calcular el orden multiplicativo de  $\alpha$ .
3. Resolver en  $F$ , expresando las soluciones en función de  $\alpha$ , la ecuación  $x^2 + x + 1 = 0$ .

1 Caso  $F_2 \leq F$  es una extensión de cuerpos finitos y toda extensión de cuerpos finitos es de Galois tenemos que, en particular,  $F_2 \leq F$  es normal de donde, si tiene una raíz las tendrá todos. Como  $\alpha$  es una raíz de tenemos que, como  $F$  es cuerpo de descomposición de  $f$ , este será  $F_2(\alpha)$ .

2. Ahora bien; para esto, debemos ver que  $f$  es irreducible en  $F_2[X]$ , en cuyo caso,  $F_2(\alpha) \cong F_{64}$ . Como no tiene raíces en  $F_2$  y los posibles factores de grado 2 y 3 no lo son tenemos que  $f$  es irreducible. Dichos factores son  $\{x^2+x+1, x^3+x+1, x^3+x^2+1\}$ , basta hacer la división en  $F_2[X]$ .

Por tanto,  $F_2(\alpha) \cong F_{64}$ , de donde se deduce que el menor orden multiplicativo es divisor de 63. Además, sabemos que  $\{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5\}$  es una  $F_2$ -base de  $F_{64}$  en virtud del Teorema de la Torre. Los posibles órdenes son 1, 3, 7, 9, 21, 63:

i) Caso 1; como  $\{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5\}$  es una  $F_2$ -base claramente  $\alpha \neq 1$ .

ii) Caso  $\alpha(\alpha) = 3$ ; de manera análoga  $\alpha^3 \neq 1$ .

iii) Caso  $\alpha(\alpha) = 7$ ;  $\alpha^7 = \alpha \alpha^6 = \alpha(\alpha+1) = \alpha^2 + \alpha + 1$  pues  $\alpha^2, \alpha, 1$  son linealmente independientes.

iv) Caso  $\alpha(\alpha) = 9$ ,  $\alpha^9 = \alpha^6 \alpha^3 = \alpha^3(\alpha+1) = \alpha^4 + \alpha^3 + 1$  pues  $\alpha^4, \alpha^3, 1$  son linealmente independientes.

v) Caso  $\alpha(\alpha) = 21$ ,  $\alpha^{21} = (\alpha^7)^3 = (\alpha^2 + \alpha)^3 = (\alpha^4 + \alpha^2 + 2\alpha^3)(\alpha^2 + \alpha) = \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + 2\alpha^5 + 2\alpha^4 = \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3$   
 $= \alpha^5 + \alpha^4 + \alpha^3 + \alpha + 1$  pues  $\alpha^5, \alpha^4, \alpha^3, \alpha$  son linealmente independientes.

Por tanto,  $\alpha(\alpha) = 63$  y de donde se deduce que  $F_{64} \cong \langle \alpha \rangle$

3. Puesto que en  $F_{64}$  se encuentran todas las raíces de todos los polinomios irreducibles de grado un divisor de 6 y el grado de  $6 = x^2+x+1 \in F_2[X]$  divide a 6 la ecuación tiene solución. Ahora bien, por el mismo razonamiento que en el apartado 1  $F_2(b) \cong F_7$  puesto que  $b$  es irreducible. De ahí se deduce, siendo  $b \in F_7$  una raíz de 6, que  $\{1, b\}$  es una  $F_2$ -base de  $F_7$ , entonces  $b$  tiene orden multiplicativo 3 y por tanto, buscamos un elemento de  $F_{64}^X$  que tenga orden multiplicativo 3; un posible candidato es  $\alpha^{21}$ ; veámos si es así:

$$\text{Como } \alpha^{21} = (\alpha^6)^3 \alpha^3 = (\alpha+1)^3 \alpha^3 = (\alpha^2+1)(\alpha+1) \alpha^3 = (\alpha^3 + \alpha^2 + \alpha + 1) \alpha^3 = \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 = \alpha^5 + \alpha^4 + \alpha^3 + \alpha + 1$$

$$\text{Tenemos que } (\alpha^{21})^6 + \alpha^{21} + 1 = (\alpha^5 + \alpha^4 + \alpha^3 + \alpha + 1)^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha = \alpha^{30} + \alpha^{28} + \alpha^{26} + \alpha^{24} + \dots + \alpha^5 + \alpha^4 + \alpha^3 + \alpha = \\ = \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 + \dots + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = 0$$

Por tanto, las raíces son  $\alpha^{21}$  y  $\alpha^{42}$  donde se ha aplicado el autorrizamo de Frobenius de  $F_2 \leq F_7$ . Finalmente, como es el único polinomio irreducible de grado 2 en  $F_2[X]$  no es necesario comprobarlo, entre esos.

EJERCICIO 58. Sea  $\alpha = \sqrt{2} + i\sqrt{3} \in \mathbb{C}$ .

1. Demostrar que  $\sqrt{2} \in \mathbb{Q}(\alpha)$  y calcular  $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ .
2. Calcular, definiendo explícitamente todos sus elementos, el grupo de Galois de  $\text{Irr}(\alpha; \mathbb{Q})$ .
3. ¿Son las raíces de  $\text{Irr}(\alpha; \mathbb{Q})$  construibles con regla y compás?

1. Veamos que  $\sqrt{2} \in \mathbb{Q}(\alpha)$ , puesto que  $\sqrt{2} = \frac{\alpha + \alpha^2}{2\alpha}$  tenemos que  $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\alpha)$ . Para calcular dicho grado veamos primero que  $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, i\sqrt{3})$ ; pero  $\mathbb{Q}(\alpha) \leq \mathbb{Q}(\sqrt{2}, i\sqrt{3})$  es trivial; además, como  $\mathbb{Q}(\sqrt{2}) \leq \mathbb{Q}(\alpha)$  solo queda probar que  $i\sqrt{3} \in \mathbb{Q}(\alpha)$ ; pero  $i\sqrt{3} = \alpha - \sqrt{2}$  basta demostrar la igualdad. Ahora, aplicando el Teorema de la Torre tenemos que  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4$  puesto que  $\text{Irr}(\sqrt{2}, \mathbb{Q}) = x^2 - 2$  y  $\text{Irr}(i\sqrt{3}, \mathbb{Q}(\sqrt{2})) = x^2 + 3$  puesto que  $\mathbb{Q}(\sqrt{2})$  no contiene números complejos.

2. Como  $\text{Irr}(\alpha, \mathbb{Q})$  es irreducible y  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$  tenemos que  $\deg(\text{Irr}(\alpha, \mathbb{Q})) = f = 4$ . Además, si  $K$  es un cuerpo de descomposición de  $f$  tenemos que  $\mathbb{Q} \leq K$  es de Galois. Veamos qué tipo es  $f$ ; dicho polinomio es:

$$f = x^4 + 2x^2 + 25 \in \mathbb{Q}[x]$$

buscando factores  
de grado 2

Debemos ver que es irreducible, pero los posibles raíces son  $\pm 25, \pm 5, \pm 1$  y ninguna de ellas es. Además, una manera más sencilla de verlo es usar que no es necesario un irreducible si no es separable, podemos considerar  $g = (x^2 - 2)(x^2 + 3) \in \mathbb{Q}[x]$ . Como  $\mathbb{Q}(\sqrt{2}, i\sqrt{3})$  es cuerpo de descomposición de  $g$  por contener todos, y sobre todo, las raíces de  $g$ ; obtenemos que  $\mathbb{Q} \leq \mathbb{Q}(\alpha)$  es de Galois, y de hecho, como  $\mathbb{Q}(\alpha) \leq K$  anteriormente, obtenemos ya que  $\mathbb{Q}(\alpha) = K \rightarrow$  de aquí se deduce que  $\mathbb{Q}(\alpha)$  es todo de separabilidad.

Para obtener los elementos de  $\text{Aut}(K)$  debemos usar la primera proposición de extensión; consideraremos los siguientes dos diagramas y el polinomio  $x^2 - 2 \in \mathbb{Q}[x]$  irreducible; dicha proposición nos asegura

$$\begin{array}{ccc} \mathbb{Q} & \xhookrightarrow{c} & K \\ & \searrow \bar{c} & \\ & & \mathbb{Q}(\sqrt{2}) \end{array}$$

que las extensiones de la inclusión están en correspondencia biyectiva con las raíces de  $p' = x^2 - 2$  en  $K$ , estas son  $R = \{ \pm \sqrt{2} \}$

Además, dichas extensiones viene dadas por  $\gamma_j : \mathbb{Q}(\sqrt{2}) \longrightarrow K$  para  $j=0,1$   
 $\sqrt{2} \longmapsto (-1)^j \sqrt{2}$

Aplicando esto de forma análoga con el esquema siguiente para cada  $j, k, u$ , ¿obtenemos que

$$\begin{array}{ccc} \mathbb{Q}(\sqrt{2}) & \xrightarrow{c} & K \\ & \searrow \bar{c} & \\ & \uparrow \gamma_{jk} & \\ & \mathbb{Q}(\sqrt{2}, i\sqrt{3}) & \end{array} \quad \text{Aut}(K) = \{ \gamma_{ju} : j=0,1; u=0,1 \}$$

donde  $\gamma_{ju}|_{\mathbb{Q}(\sqrt{2})} = \gamma_j$   $j=0,1$  y  $\gamma_{ju}(i\sqrt{3}) = (-1)^k i\sqrt{3}$  con  $u=0,1$ .

3. Esta respuesta es afirmativa, puesto que  $\mathbb{Q}(\alpha)$  es el cuerpo de descomposición del  $\text{Irr}(\alpha, \mathbb{Q})$ ,  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^2$  y  $\mathbb{Q} \leq \mathbb{Q}(\alpha)$  es una extensión de Galois tenemos que las raíces son constructibles con regla y compás. Para acabar, deberíamos probar que  $\alpha \notin \mathbb{Q}$ , pero esto es trivial principalmente porque  $i \notin \mathbb{Q}$ .

EJERCICIO 59. Sea  $K$  el cuerpo de descomposición de  $f = X^6 - 3 \in \mathbb{Q}[X]$ .

1. Calcular  $[K : \mathbb{Q}]$ .
2. Demostrar que  $i + \sqrt{3} \in K$ .
3. Calcular, definiendo explícitamente todos sus elementos, el grupo  $G = \text{Aut}_{\mathbb{Q}(i+\sqrt{3})}(\mathbb{Q})$ .
4. ¿Es  $G$  un subgrupo normal del grupo de Galois de  $f$ ?

1. Para ello, como es el primer ejercicio de extensiones cíclicas, lo haremos de forma exhaustiva. Consideremos  $\sqrt[6]{3}$  y  $\omega \in \mathbb{C}$  una raíz sexta primitiva de la unidad; vienes en teoría que el cuerpo de descomposición de  $f$  es  $\mathbb{Q}(\sqrt[6]{3}, \omega)$ .

Ahora bien, buscamos simplificar ese cuerpo; como  $\omega = \frac{1}{2} + \frac{i\sqrt{3}}{2}$  tenemos claramente que  $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[6]{3}, i\sqrt{3})$ ; además,  $i\sqrt{3} = 2(\omega - \frac{1}{2}) \in \mathbb{Q}(\sqrt[6]{3}, \omega)$  luego  $\mathbb{Q} = \mathbb{Q}(\sqrt[6]{3}, i\sqrt{3})$ . Veamos ahora que  $\mathbb{Q}(\sqrt[6]{3}, i\sqrt{3}) = \mathbb{Q}(\sqrt[6]{3}, i)$ ; como  $i\sqrt{3} = i(\sqrt[6]{3})^3$  tenemos que  $i\sqrt{3} \in \mathbb{Q}(\sqrt[6]{3}, i)$ ; además, como  $i = \frac{i\sqrt{3}}{(\sqrt[6]{3})^3}$  tenemos la otra inclusione; por tanto,  $\mathbb{Q} = \mathbb{Q}(\sqrt[6]{3}, i)$ .

Aplicando ahora el Teorema de la Torre, como  $\text{Irr}(\sqrt[6]{3}, \mathbb{Q}) = x^6 - 3$  que es irreducible aplicando el criterio de Eisenstein para  $p=3$  y  $\text{Irr}(i, \mathbb{Q}(\sqrt[6]{3})) = x^4 + 1 \in \mathbb{Q}(\sqrt[6]{3})[x]$  pues  $\mathbb{Q}(\sqrt[6]{3})$  no contiene números complejos tenemos que

$$[\mathbb{Q} : \mathbb{Q}] = [\mathbb{Q} : \mathbb{Q}(\sqrt[6]{3})] [\mathbb{Q}(\sqrt[6]{3}) : \mathbb{Q}] = 12$$

2. Puesto que hemos realizado una simplificación exhaustiva basta ver que  $i + \sqrt{3} = i + (\sqrt[6]{3})^3 \in \mathbb{Q}(\sqrt[6]{3}, i)$   
 3. Para ello, primero vamos a calcular el grupo de Galois de la extensión  $\mathbb{Q} \subseteq K$  que vienes que era de Galois. Aplicamos la primera proposición de extensión dos veces [usar la parafrasea] obteniendo los siguientes automorfismos  $\mathbb{Q}$ -fijos:

$$\begin{aligned} \gamma_K : \mathbb{Q} &\longrightarrow K \\ \sqrt[6]{3} &\longmapsto \omega^j \sqrt[6]{3} \quad \text{para } j = 0, 1, 2, 3, 4, 5 \\ i &\longmapsto (-1)^u i \quad \text{para } u = 0, 1 \end{aligned}$$

Por tanto,  $\text{Aut}(K) = \{\gamma_{ju} : j = 0, 1, 2, 3, 4, 5; u = 0, 1\}$ . Aplicando ahora la conexión de Galois, partiendo de que vos pides aquellos índices  $j \in \{0, 1, 2, 3, 4, 5\}$ ,  $u \in \{0, 1\}$  tales que  $\gamma_{ju}(i + \sqrt{3}) = i + \sqrt{3}$ , buscamos saber cuáles son. Dicha conexión de Galois nos dice que  $|\text{Aut}_{\mathbb{Q}(i+\sqrt{3})}(K)| = [\mathbb{Q} : \mathbb{Q}(i+\sqrt{3})]$ .

Para calcular ese índice, como en 2. hemos visto que  $i + \sqrt{3} \in K$ , buscamos la siguiente torre de cuerpos

$$\mathbb{Q} \subseteq \mathbb{Q}(i + \sqrt{3}) \subseteq K$$

de donde el Teorema de la Torre, juntito a que  $\mathbb{Q}(i + \sqrt{3}) = \mathbb{Q}(i, \sqrt{3})$ , nos dice que:

$$[\mathbb{Q} : \mathbb{Q}] = [\mathbb{Q} : \mathbb{Q}(i, \sqrt{3})] [\mathbb{Q}(i, \sqrt{3}) : \mathbb{Q}]$$

Usando de nuevo el Teorema de la Torre obtenemos que

$$[\mathbb{Q}(i, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(i, \sqrt{3}) : \mathbb{Q}(\sqrt{3})] [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 6$$

y como  $\text{Irr}(\sqrt{3}, \mathbb{Q}) = x^2 - 3 \in \mathbb{Q}[x]$  por el criterio de Eisenstein para  $p=3$  así como  $x^2 + 1 = \text{Irr}(i, \mathbb{Q}(i)) \in \mathbb{Q}(i)[x]$  deducido  $[\mathbb{Q} : \mathbb{Q}(i)] = 2$ .

Volviendo al problema, buscamos dos automorfismos que dejen fijo a  $i + \sqrt{3}$  es.

$$\gamma_{ju}(i+\sqrt{3}) = \gamma_{ju}(i) + \gamma_{ju}(\sqrt{3}) = (\gamma_j)^k i + \gamma_{ju}(\sqrt{3}) \gamma_{ju}(\sqrt{3}) \gamma_{ju}(\sqrt{3})$$

$$= (-1)^ki + \omega^j\sqrt{3} + \omega^{j+1}\sqrt{3} + \omega^{j+2}\sqrt{3}$$

Observe que se deduce que una combinación posible es  $k=0, j=0$ . Si embargo, como  $\omega^6=1$ , teniendo  $j=2$  y  $k=0$  obtenemos el otro elemento.

4. Para ver esta cuestión, debemos estudiar si  $\mathbb{Q} \leq \mathbb{Q}(i+\sqrt{3})$  es una extensión de galois, pero esto es cierto como cuerpo de descomposición del polinomio separable en  $\mathbb{Q}[x]$   $h=(x^2+i)(x^2-3) \in \mathbb{Q}[x]$  ya que  $\mathbb{Q}(i+\sqrt{3})=\mathbb{Q}(i, \sqrt{3})$ .

EJERCICIO 60. Sea  $F = \mathbb{F}_3(a)$  un cuerpo con  $a$  satisfaciendo la ecuación  $a^3 + a - 1 = 0$ .

1. Calcular el cardinal de  $F$ .
2. Calcular el grado de  $\text{Irr}(a^2, \mathbb{F}_3)$ .
3. Calcular  $\text{Irr}(a^2, \mathbb{F}_3)$ .

1. Consideremos el polinomio  $x^3+x-1 \in \mathbb{F}_3[x]$ , como  $x^3+x-1=0$  tenemos que  $(x-1) \in \mathbb{F}_3[x]$  es un factor de dicho polinomio; por tanto, consideremos ahora  $f=x^2+2x+2$  ahora si irreducible en  $\mathbb{F}_3[x]$  pues no tiene raíces. Debemos distinguir casos:

i) Si  $a=2$  entonces  $a \in \mathbb{F}_3$  deducido  $\mathbb{F}_3(a) \cong \mathbb{F}_3$  y  $|\mathbb{F}_3|=3$ .

ii) Si  $a \neq 2$  en ese caso  $a \notin \mathbb{F}_3$  y  $\text{Irr}(a, \mathbb{F}_3) = x^2+2x+2$  de donde, al ser  $\mathbb{F}_3 \leq \mathbb{F}_3(a)$  una extensión de cuerpos finitos es de galois y  $\mathbb{F}_3(a)$  sería cuerpo de descomposición de  $f$ .

Entonces, usando uno de los tres teoremas de cuerpos finitos tenemos que

$$\mathbb{F}_3(a) \cong \mathbb{F}_q \text{ de donde } |\mathbb{F}_3(a)|=q.$$

2. Volvemos a distinguir casos:

i) Si  $a=2$  tenemos que  $a^2=1$  de donde  $\text{Irr}(a^2, \mathbb{F}_3) = x+2$  y  $\deg(\text{Irr}(a^2, \mathbb{F}_3))=2$ .

ii) Si  $a \neq 2$  tenemos que  $a^2+2a+2=0 \Leftrightarrow a^2+2=a$ , de donde  $a \in \mathbb{F}_3(a^2)$ . Como, finalmente,  $\mathbb{F}_3(a^2) \leq \mathbb{F}_3(a)$  tenemos  $\mathbb{F}_3(a^2) = \mathbb{F}_3(a)$  de donde  $\deg(\text{Irr}(a^2, \mathbb{F}_3))=2$ .

3. Nos centraremos en el caso  $a \neq 2$ . Una opción sería usar que  $a^2+2a+2=0$  y que  $\{1, a\}$  es una  $\mathbb{F}_3$ -base de  $\mathbb{F}_3(a)$  para probarlos todos los polinomios irreducibles de grado 2 en  $\mathbb{F}_3[x]$ , que son:

$$\{x^2+1, x^2+x+2, x^2+2x+2\}$$

Siguiendo esta estrategia tenemos que

$$i) a^4+1 = (a^2)^2+1 = a^2+2a+1+1 = a^2+2a+2=0$$

$$ii) 4+a^2+2 = a^2+2a+2+a^2+1 = a+1+1 = a+2 = a-1 = 0 \Leftrightarrow a=1 \text{ cosa que no ocurre}$$

iii) En este caso, puesto que  $a$  es raíz, el automorfo de Frobenius de  $\mathbb{F}_3 \leq \mathbb{F}_3(a)$  nos da que  $a^3=1-a$  es la otra raíz

Por tanto,  $\text{Irr}(x^2 + 1, \mathbb{F}_5) = x^2 + 1$ .

EJERCICIO 61. Calcular el número de polinomios monómicos irreducibles de grado menor o igual que 3 en  $\mathbb{F}_5[X]$ .

Consideremos el cuerpo  $\mathbb{F}_{25}$  y el polinomio  $x^{25} - x \in \mathbb{F}_5[x]$ ; sabemos de teoría que este polinomio factorial es un producto de todos los polinomios irreducibles en  $\mathbb{F}_5[x]$  cuyo grado sea un divisor de 3.

Sabemos que los polinomios irreducibles de grado 1 son  $\{x, x+1, x+2, x+3, x+4, x+5\}$  de donde el número de polinomios irreducibles de grado 3 es 40.

Considerando ahora el cuerpo  $\mathbb{F}_5$  y el polinomio  $x^5 - x \in \mathbb{F}_5[x]$  tenemos por su factorización sabemos que el número de polinomios irreducibles de grado 2 en  $\mathbb{F}_5[x]$  es 10 de donde el número pedido es 50.

EJERCICIO 62. Sean  $\sqrt[3]{2}, \sqrt[3]{2} \in \mathbb{R}$ .

1. Calcular razonadamente  $[\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}), \mathbb{Q}]$ .
2. Decidir razonadamente si  $K = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}, i\sqrt{3})$  es una extensión de Galois de  $\mathbb{Q}$ .
3. Calcular  $\text{Aut}(K)$  definiendo explícitamente todos sus elementos.
4. Calcular razonadamente el grado del polinomio  $f = \text{Irr}(\sqrt[3]{2} + i\sqrt[3]{2}, \mathbb{Q})$ .
5. Decidir razonadamente quién es el grupo de Galois de  $f$ . ¿Es  $f$  resoluble por radicales? ¿Son las raíces complejas de este polinomio construibles con regla y compás?

1. Podemos aplicar el teorema de la Torre; además, como  $(x^2 - 2)(x^3 - 2) \in \mathbb{Q}[x]$  tiene a  $\sqrt{2}, \sqrt[3]{2}$  como raíces, tenemos que  $[\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}) : \mathbb{Q}] \leq 6$ . Además, como  $\text{Irr}(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2 \in \mathbb{Q}[x]$  y  $\text{Irr}(\sqrt[3]{2}, \mathbb{Q}) = x^2 - 2 \in \mathbb{Q}[x]$  cumpliendo el criterio de Eisenstein para  $p=2$ . Por tanto, aplicando el teorema de la Torre dos veces obtenemos claramente que  $[\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}) : \mathbb{Q}] = 6$  por ser múltiplo de 2 y 3 y ser menor o igual que 6.

2. La respuesta es afirmativa puesto que  $K$  es cuerpo de descomposición de  $f = (x^2 - 2)(x^3 - 2) \in \mathbb{Q}[x]$  que es un polinomio separable. Además, como  $i \notin \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2})$  tenemos que  $|\text{Aut}(K)| = [K : \mathbb{Q}] = 12$ , en virtud del apartado anterior y del teorema de la Torre.

3. Para este apartado basta usar la primera proposición de extensión: cuantas veces sea necesario contando el razoñamiento y considerando  $\omega \in \mathbb{C}$ ,  $\omega = \frac{-1}{2} + \frac{i\sqrt{3}}{2}$  una raíz cúbica primitiva de la unidad. Los elementos son:  $\gamma_{1,0}(\sqrt[3]{2}) = \omega^0 \sqrt[3]{2}$ ,  $\gamma_{1,1}(\sqrt[3]{2}) = (-1)^n (\sqrt[3]{2})$  y  $\gamma_{1,2}(\sqrt[3]{2}) = \omega^l \sqrt[3]{2}$  para  $j=0,1,2$ ;  $n=0,1$  y  $l=0,1$ .

4. Sabemos que  $\deg(f) = [\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}) : \mathbb{Q}]$ ; puesto que  $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2})$  aplicando un razonamiento que hemos usado muchas veces tenemos que  $\deg(f) = 6$ .

5. Aunque podemos pensar que  $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2})$  es el cuerpo de descomposición de  $f$  esto no es así; sin embargo, si sabemos que  $f$  se descompone como producto de polinomios lineales en  $K$ . Sea ahora  $E$  el cuerpo de descomposición de  $f$  tenemos que  $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}) \subseteq E \subseteq K$  de donde el teorema de la torre nos dice que

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

de donde hay dos opciones; obviamente  $[E : E] = 1$  y  $[E : \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2})] = 1$  obviamente  $[K : E] = 1$  y  $[E : \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2})]$ . Puesto que  $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}) \subseteq E$  pero no es todo la igualdad obtenemos que  $[K : E] = 1$ .

de donde  $K = E$ .

Como el grupo de Galois de  $f$  es  $\text{Aut}(K)$  es resoluble y, por tanto,  $f$  es resoluble por radicales. Sin embargo, como  $[\mathbb{Q}(\zeta_6):\mathbb{Q}] = 2$  que no es una potencia de 2, tenemos que las raíces cuadráticas del polinomio no son construibles con regla y compás. Otra forma de justificar esto es diciendo que, si fuese constructible tendría grado sobre  $\mathbb{Q}$  una potencia de 2 y esto no es así.

EJERCICIO 65. Sea  $K$  el cuerpo de descomposición de  $f = X^{12}-1 \in \mathbb{Q}[X]$ .

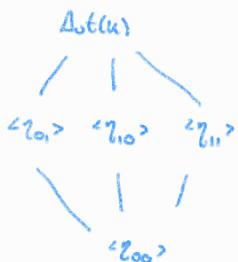
1. Calcular el grupo de Galois  $G$  de  $f$ , definiendo explícitamente todos sus elementos.
2. Calcular todos los subgrupos de  $G$ .
3. Calcular todos los subcuerpos de  $K$ , indicando a qué subgrupo de  $G$  corresponde cada uno de ellos mediante la Conexión de Galois.

Nos encontramos ante una extensión ciclotómica, sabemos que, si consideramos una raíz duodécima primitiva de la unidad el cuerpo de descomposición de  $f$  es  $\mathbb{Q}(\zeta)$  ahora bien, teniendo  $\zeta = \frac{\sqrt{3}}{2} + \frac{i}{2}$  vemos claramente que  $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta, \sqrt{3})$  de donde  $[\mathbb{Q}(\zeta, \sqrt{3}) : \mathbb{Q}] = 4$ .

1. Para ello, usando la primera proposición de extensión y asumiendo que se ha demostrado que  $\mathbb{Q} \leq \mathbb{Q}(\zeta)$  es de Galois cosa que es clara por ser cíclica (en particular) obtenemos que  $\text{Aut}(\mathbb{Q}) = \langle \gamma_{j,u} : j=0,1, u=0,1 \rangle$  donde  $\gamma_u(i) = (-1)^{ki}$  y  $\gamma_u(\sqrt{3}) = (-1)^j \sqrt{3}$ . Calcularemos los órdenes de los elementos

$$\begin{matrix} \gamma_{00} & \gamma_{01} & \gamma_{10} & \gamma_{11} \\ 1 & 2 & 2 & 2 \end{matrix}$$

De aquí deducimos que  $\text{Aut}(\mathbb{Q})$  no es cíclico sino que es isomorfo a  $C_2 \oplus C_2$  de donde los subgrupos son:



3. Para ello, usaremos la conexión de Galois; buscamos obtener, para cada subgrupo  $H \subset \text{Aut}(K)$  cuáles su subcuerpo de  $K$  fijo por la acción de  $H$ , es decir,  $K^H$ .

$\Rightarrow K^{\langle \gamma_{00} \rangle} \cong K$  puesto que  $\gamma_{00}$  deja fijo a todos los elementos; realmente, de aquí sólo deducimos que  $K^{\langle \gamma_{00} \rangle} \leq K$ ; pero, por la conexión de Galois sabemos que  $[K^{\langle \gamma_{00} \rangle} : \mathbb{Q}] = \frac{|\text{Aut}(K)|}{|\langle \gamma_{00} \rangle|} = 4$  lo que nos da la igualdad

$\Rightarrow$  Como  $\gamma_{00}(i) = i$  tenemos que  $K^{\langle \gamma_{00} \rangle} = \mathbb{Q}(i)$  y como  $[\mathbb{Q}(i) : \mathbb{Q}] = 2 = [K^{\langle \gamma_{00} \rangle} : \mathbb{Q}] = \frac{|\text{Aut}(K)|}{|\langle \gamma_{00} \rangle|}$  tenemos la igualdad

Análogamente se obtiene que  $K^{\langle \gamma_{01} \rangle} \cong \mathbb{Q}(\sqrt{3})$  y que  $K^{\langle \gamma_{10} \rangle} \cong \mathbb{Q}(\imath\sqrt{3})$ .

EJERCICIO 55. Calcular el cardinal del grupo de Galois sobre  $\mathbb{Q}$  del polinomio  $f = (X^3 + X + 1)(X^2 + 1)$ .

Consideramos  $f \circ g$  con  $g = x^3 + x + 1$  y  $h = x^2 + 1$  cumpliendo que  $g, h \in \mathbb{Q}[x]$ . Algunabien, si  $K$  es el cuerpo de descomposición de  $f$  en  $\mathbb{Q}(i)[x]$  es claro que  $\mathbb{Q}(i) \subseteq K$ ; el Teorema de la Torre nos dice que

$$[K : \mathbb{Q}] = [\mathbb{Q}(i) : \mathbb{Q}][\alpha(i) : \mathbb{Q}]$$

Solo queda por determinar  $[\mathbb{Q}(i) : \mathbb{Q}]$ ; para ello, buscamos probar que  $K$  es el cuerpo de descomposición de  $g$  sobre  $\mathbb{Q}(i)[x]$ ; necesitamos probar que  $g$  es irreducible en  $\mathbb{Q}(i)[x]$ .

Sabemos que  $g' = 3x^2 + 1 \geq 0$  por lo que solo dispone de una raíz real y dos complejas  $\alpha, \bar{\alpha} \in \mathbb{C}$ . Podemos deducir ya que  $r \notin \mathbb{Q}(i)$  siendo  $r \in \mathbb{R}$  con  $r^3 + r + 1 = 0$  puesto que en caso contrario tendríamos que  $r \in \mathbb{Q}$  de donde, necesariamente  $r = \pm 1$ , lo cual es una contradicción pues  $3 \neq 0$ !!

Supongamos ahora que  $\alpha \in \mathbb{Q}(i)$  entonces  $\bar{\alpha} \in \mathbb{Q}(i)$  de donde  $T = (x - \alpha)(x - \bar{\alpha}) \in \mathbb{Q}(i)[x]$  sería un factor de  $g$  en  $\mathbb{Q}(i)[x]$  de donde el resultado del cociente sería  $x - r \in \mathbb{Q}[x]$  de donde  $r \in \mathbb{Q}$ !!

Por tanto, tenemos que el grupo de Galois de  $g$  sobre  $\mathbb{Q}(i)$  es  $S_3 \times \mathbb{Z}_2$  puesto que  $g$  es irreducible en  $\mathbb{Q}(i)[x]$ . Estudiando ahora el discriminante de los vértices que  $\text{Disc}(g) = -4 \cdot 27 = -31$  de donde  $A(g) = i\sqrt{31} \notin \mathbb{Q}(i)$  puesto que  $x^2 + 31 \in \mathbb{Q}(i)[x]$  es irreducible por ser irreducible en  $\mathbb{Q}[x]$  y no incorporar elementos complejos. Por tanto, dicho grupo de Galois es  $S_3$  de donde  $[K : \mathbb{Q}(i)] = 6$  y podemos garantizar que  $[K : \mathbb{Q}] = 12$ .

EJERCICIO 66. Sea  $F = \mathbb{F}_3(a)$  un cuerpo con  $a$  satisfaciendo la ecuación  $a^3 + a^2 - 1 = 0$ .

1. Calcular el cardinal de  $F$ .
2. Calcular el grado de  $\text{Irr}(a^2, \mathbb{F}_3)$ .
3. Calcular  $\text{Irr}(a^2, \mathbb{F}_3)$ .

1. Puesto que  $a \notin \mathbb{F}_3$  y  $a$  es raíz de  $f = x^3 + x^2 - 1 \in \mathbb{F}_3[x]$  que es irreducible tenemos que  $\mathbb{F}_3(a)$  es una extensión de Galois por ser finita y, además, por este medio  $\mathbb{F}_3(a)$  es el cuerpo de descomposición de  $f$  por tanto  $F = \mathbb{F}_3(a)$ . De acuerdo con parámetros de la teoría de cuerpos finitos tenemos que  $|\mathbb{F}_3(a)| = |\mathbb{F}_3| = 9$ .

2. Como  $a^3 = -a$  tenemos que  $a^2 = 2 + 2a^2 = 2 + 2(-a) = 2 + 2 - 2a = 2 + 2a = 1 + a$  por tanto,  $\mathbb{F}_3(a) \leq \mathbb{F}_3(a)$  de donde se deduce que  $\deg(\text{Irr}(a^2, \mathbb{F}_3)) = 3$  puesto que  $\mathbb{F}_3(a)$  es isomorfa a  $\mathbb{F}_3(a)$  y  $[\mathbb{F}_3(a) : \mathbb{F}_3] = 3$  con  $\{1, a, a^2\}$  una  $\mathbb{F}_3$ -base de  $\mathbb{F}_3(a)$ .

3. Los polinomios irreducibles de grado 3 en  $\mathbb{F}_3$  son 3 y son muchos; sin embargo, si tenemos el polinomio  $x^3 - x^2 + 2x - 1$  obtenemos que  $a^3$  es raíz de él; por tanto, este es el polinomio pedido.

Para hacer este ejercicio hay que obtener todos los polinomios e ir probando; salvo que haya otra forma esta es seguramente larga.

EJERCICIO 68. Realizar las siguientes tareas.

1. Demostrar que existe  $a \in \mathbb{F}_{16}$  tal que  $\mathbb{F}_{16} = \mathbb{F}_2(a)$  y  $a^4 + a + 1 = 0$ .
2. Demostrar que  $a$  genera el grupo cíclico  $\mathbb{F}_{16}^\times$ .
3. Resolver en  $\mathbb{F}_{16}$ , expresando la solución en función de  $a$ , la ecuación  $x^2 + x + 1 = 0$ .
4. Calcular el número de homomorfismos de cuerpos  $\mathbb{F}_4 \rightarrow \mathbb{F}_{16}$ .

1. Consideremos el polinomio  $p = x^4 + x + 1 \in \mathbb{F}_2[x]$ ; puesto que no tiene raíces y  $(x^2 + x + 1)^2 = x^4 + x^2 + 1 \neq p$  tampoco tiene factores irreducibles de grado 2. Supongamos que se ha probado la existencia de  $a \in \mathbb{F}_{16}$  raíz de  $p$  (entendemos que  $\mathbb{F}_2 \subseteq \mathbb{F}_2(a)$ ) sería una extensión de Galois por ser una extensión de cuerpos finitos. Por ser de Galois es normal de donde  $\mathbb{F}_2(a)$  debe contener todas las raíces de  $p$  y por tanto, ser cuerpo de descomposición de  $p$ . Al contrario, usando un poco de teoría de cuerpos finitos tenemos que  $\mathbb{F}_{16}$  es cuerpo de descomposición de  $p$  por lo que el  $T^{\text{ra}}_a$  de  $\mathbb{F}_{16}$  es el cuerpo de descomposición de  $p$  que  $\mathbb{F}_2(a) = \mathbb{F}_{16}$ .

Veamos ahora la existencia de  $a$ ; consideramos el polinomio  $p$  que es irreducible. Usando ahora el lema del Grupo de Galois que  $\exists \sigma: \mathbb{F}_2 \longrightarrow F$  (automorfismo) tal que  $\exists a \in F$  con  $p^\sigma(a) = 0$ . De hecho, se tiene que  $F = \sigma(\mathbb{F}_2)(a) = \frac{\sigma(\mathbb{F}_2)[x]}{(p(x))}$ . Al contrario, puesto que  $a$  debe ser raíz de  $p$  no queda otra salida que  $\sigma = \text{id}$  de donde  $p^\sigma(a) = p(a) = 0$ ; además,  $\sigma(\mathbb{F}_2) = \mathbb{F}_2$  entonces  $F = \mathbb{F}_2(a)$  y como  $\deg p = 4$  tenemos que  $a \in \mathbb{F}_{16}$ .

2. Para ver que  $\mathbb{F}_2(a) = \mathbb{F}_{16}$  basta ver que el orden multiplicativo de  $a$  es 15; usaremos la virtud de la proposición del teorema 1, que  $1, a, a^2, a^3$  es  $\mathbb{F}_2$ -base de  $\mathbb{F}_2(a)$  pues  $[\mathbb{F}_2(a), \mathbb{F}_2] = \deg \text{In}(a, \mathbb{F}_2) = 4$ .
  - i)  $O(a) = 1 \Rightarrow a = 1$  !!  $a \neq 1$  son  $\mathbb{F}_2$ -linealmente independientes
  - ii)  $O(a) = 3 \Rightarrow a^3 = 1$  !!  $a^3 \neq 1$  son  $\mathbb{F}_2$ -linealmente independientes
  - iii)  $O(a) = 5 \Rightarrow 1 = a^5 = a^4 a = (a+1)a = a^2 + a$  !!

Por tanto, la única salida es la virtud del Teorema de Lagrange es que  $O(a) = 15$  de donde  $\mathbb{F}_{16}^\times = \langle a \rangle$ .

3. Puesto que en esta ecuación tiene solución en  $\mathbb{F}_{16}$ . Para ello, sea  $b \in \mathbb{F}_{16}$  una solución suya sabemos que  $\mathbb{F}_2(b)$  es cuerpo de descomposición de  $x^2 + x + 1 \in \mathbb{F}_2[x]$  y además  $\mathbb{F}_2(b) = \mathbb{F}_4$  pues  $\deg(x^2 + x + 1) = 2$  y es irreducible; por tanto, buscamos un elemento cuyo orden multiplicativo sea 3 (obviamente, como  $x^2 + x + 1$  es el único irreducible de grado 2 en  $\mathbb{F}_2$ , las soluciones son  $a^5$  y  $a^{10}$  gracias al automorfismo de Frobenius); por tanto,  $b = a^5$ .
4. Puesto que hemos visto que  $\mathbb{F}_4 = \mathbb{F}_2(b)$  con  $b^2 + b + 1 = 0$  y sabemos por la proposición que dicho automorfismo es biyectivo con las raíces de  $x^2 + x + 1$  en  $\mathbb{F}_{16}$  y estas son 2, tenemos que hay 2.

Otra forma de hacerlo es usar que  $\mathbb{F}_2 \subseteq \mathbb{F}_{16}$  son todos de Galois por ser de cuerpos finitos, por lo que nos piden  $|\text{Aut}_{\mathbb{F}_4}(\mathbb{F}_{16})| = [\mathbb{F}_{16} : \mathbb{F}_4] = 2$ .