

1. Calcular $\sum_{1 \leq i, j \leq 4, i \neq j} \alpha_i^3 \alpha_j$ donde $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ son las raíces del polinomio $X^4 - X^2 + aX + 3$.

Vamos a usar $\Sigma(q)$ para denotar el simetrizado de $q \in K[X_1, X_2, X_3, X_4]$ y denotamos los polinomios simétricos en cuatro variables con s_1, s_2, s_3, s_4 . También utilizamos las funciones $\delta : K[X_1, X_2, X_3, X_4] \rightarrow \mathbb{N}^4$, que asocia a cada polinomio su grado lexicográfico, y $\Psi : \mathbb{Z}^4 \Rightarrow \mathbb{Z}^4$ dada por $\Psi(a_1, a_2, a_3, a_4) = (a_1 - a_2, a_2 - a_3, a_3 - a_4, a_4)$.

Escribimos $p = \Sigma(X_1^3 X_2)$ como polinomio en los polinomios simétricos elementales. Como $\delta(p) = (3, 1, 0, 0)$ y $\Psi(3, 1, 0, 0) = (2, 1, 0, 0)$ calculamos

$$p_1 = p - s_1^2 s_2 = -2\Sigma(X_1^2 X_2^2) - 5\Sigma(X_1^2 X_2 X_3) - 12s_4.$$

Entonces $\delta(p_1) = (2, 2, 0, 0)$ y $\Psi(2, 2, 0, 0) = (0, 2, 0, 0)$. Por tanto calculamos

$$p_2 = p_1 + 2s_2^2 = -\Sigma(x_1^2 x_2 x_3).$$

Finalmente $\delta(p_2) = (2, 1, 1, 0)$ y $\Psi(2, 1, 1, 0) = (1, 0, 1, 0)$ y calculamos

$$p_3 = p_2 + s_1 s_3 = 4s_4.$$

En conclusión

$$p = s_1^2 s_2 + p_1 = s_1^2 s_2 - 2s_2^2 + p_2 = s_1^2 s_2 - 2s_2^2 - s_1 s_3 + 4s_4.$$

Por las fórmulas de Cardano, si $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ son las raíces del polinomio dado tenemos

$$\begin{aligned} s_1(\alpha_1, \alpha_2, \alpha_3, \alpha_4) &= 0 \\ s_2(\alpha_1, \alpha_2, \alpha_3, \alpha_4) &= -1 \\ s_3(\alpha_1, \alpha_2, \alpha_3, \alpha_4) &= -a \\ s_4(\alpha_1, \alpha_2, \alpha_3, \alpha_4) &= 3 \end{aligned}$$

Por tanto

$$p(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = -2(-1)^2 + 4 \cdot 12 = 10.$$

2. Sea n un número entero libre de cuadrados (es decir, n no es divisible por el cuadrado de ningún número natural) y sea $O_n = \left\{ \frac{a+b\sqrt{n}}{2} : a, b \in \mathbb{Z}, a \equiv b \pmod{2} \right\}$. Demostrar:

(a) O_n es un subanillo del anillo de los números complejos si y sólo si $n \equiv 1 \pmod{4}$.

(b) Demostrar que si $n \equiv 1 \pmod{4}$, entonces el grupo de unidades de O_n es

$$O_n^* = \left\{ \frac{a+b\sqrt{n}}{2} : a, b \in \mathbb{Z}, |a^2 - nb^2| = 4 \right\}.$$

Poniendo $b = a + 2x$ Podemos redefinir O_n como el conjunto formado por los elementos de la forma

$$\frac{a+b\sqrt{n}}{2} = a + x \frac{1+\sqrt{n}}{2} = a + x\alpha \quad (a, x \in \mathbb{Z}),$$

Donde $\alpha = \frac{1+\sqrt{n}}{2}$. Está claro que la suma de dos elementos de O_n está también en O_n y que $1 \in O_n$. Por tanto O_n es subanillo de \mathbb{C} si y sólo si el producto de dos elementos de O_n está en O_n .

Multiplicando dos elementos de O_n y teniendo en cuenta que

$$\alpha^2 = \frac{(1+n) + 2\sqrt{n}}{4} = \frac{n-1}{4} + \alpha$$

tenemos

$$(a_1 + x_1\alpha)(a_2 + x_2\alpha) = a_1 a_2 + (a_1 x_1 + a_2 x_2)\alpha + x_1 x_2 \alpha^2 = \left(a_1 a_2 + x_1 x_2 \frac{n-1}{4} \right) + (a_1 x_1 + a_2 x_2 + x_1 x_2)\alpha.$$

El resultado obtenido está en O_n si y sólo si $x_1 x_2 \frac{n-1}{4}$ es un entero para todo $x_1, x_2 \in \mathbb{Z}$ lo cual se verifica si y sólo si $n \equiv 1 \pmod{4}$.

Utilizamos la función $N : O_n \rightarrow \mathbb{Z}$ dada por

$$N\left(\frac{a+b\sqrt{n}}{2}\right) = \frac{a+b\sqrt{n}}{2} \cdot \frac{a-b\sqrt{n}}{2} = \frac{a^2 - nb^2}{4}$$

y observamos que $N(xy) = N(x)N(y)$ para todo $x, y \in O_n$. Por tanto, si $x = \frac{a+b\sqrt{n}}{2} \in O_n$ tenemos

$$1 = N(1) = N(xx^{-1}) = N(x)N(x^{-1})$$

con lo que

$$\frac{a^2 - nb^2}{4} = N(x) = \pm 1.$$

Esto muestra que si $x = \frac{a+b\sqrt{n}}{2} \in O_n^*$ entonces $a^2 - nb^2 = \pm 4$. Recíprocamente, si $a^2 - nb^2 = \pm 4$, entonces $x = \frac{a+b\sqrt{n}}{2} = N(x) = 1$ y, por tanto $x \in O_n^*$, siendo $x^{-1} = \frac{a-b\sqrt{n}}{2}$.

3. Sean G y N dos grupos y sean $\rho : G \rightarrow \text{Aut}(N)$ un homomorfismo de grupos y $S = N \times G$. Denotamos la imagen de $g \in G$ en $\text{Aut}(N)$ como ρ_g . Demostrar que la siguiente operación define en S una estructura de grupos:

$$(n_1, g_1)(n_2, g_2) = (n_1\rho_{g_1}(n_2), g_1g_2).$$

Encontrar un homomorfismo $f : S \rightarrow G$ cuyo núcleo sea isomorfo a N .

Comprobamos los axiomas de grupo.

Asociativa.

$$\begin{aligned} (n_1, g_1)[(n_2, g_2)(n_3, g_3)] &\stackrel{(1)}{=} (n_1, g_1)(n_2\rho_{g_2}(n_3), g_2g_3) \stackrel{(1)}{=} (n_1\rho_{g_1}(n_2\rho_{g_2}(n_3)), g_1(g_2g_3)) \stackrel{(2)}{=} \\ (n_1\rho_{g_1}(n_2)\rho_{g_1}(\rho_{g_2}(n_3)), (g_1g_2)g_3) &\stackrel{(3)}{=} (n_1\rho_{g_1}(n_2)\rho_{g_1g_2}(n_3), (g_1g_2)g_3) \stackrel{(1)}{=} (n_1\rho_{g_1}(n_2), g_1g_2)(n_3, g_3) \stackrel{(1)}{=} \\ [(n_1, g_1)(n_2, g_2)](n_3, g_3) & \end{aligned}$$

Hemos utilizado las siguientes propiedades en los lugares que se indican.

- (1) Definición del producto.
- (2) Asociativa en G y ρ_{g_1} es homomorfismo.
- (3) ρ es un homomorfismo.

Neutro.

$$(n, g)(1, 1) = (n\rho_g(1), g1) \stackrel{(1)}{=} (n1, g1) = (n, g)$$

$$(1, 1)(n, g) = (1\rho_1(n), 1g) \stackrel{(2)}{=} (1n, 1g) = (n, g)$$

(1) $\rho_g(1) = 1$, pues ρ_g es un homomorfismo.

(2) $\rho_1 = I$, pues ρ es un homomorfismo.

Esto muestra que $(1, 1)$ es el neutro de S .

Inverso. Buscamos el inverso de (n, g) imponiendo las condiciones que tiene que verificar.

$$(1, 1) = (n, g)(m, h) = (n\rho_g(m), gh)$$

O equivalentemente

$$n\rho_g(m) = 1 \quad \text{y} \quad gh = 1$$

Por tanto

$$h = g^{-1} \quad \text{y} \quad \rho_{g^{-1}}(m) = n^{-1}$$

con lo que el inverso de (n, g) sólo puede ser $(\rho_{g^{-1}}(n^{-1}), g^{-1})$. En realidad todavía tenemos que comprobar que sea el inverso de (n, g) multiplicando de las dos formas posibles:

$$(n, g)(\rho_{g^{-1}}(n^{-1}), g^{-1}) = (n\rho_g(\rho_{g^{-1}}(n^{-1})), gg^{-1}) \stackrel{(1)}{=} (n\rho_g(\rho_{g^{-1}}(n^{-1})), gg^{-1}) = (nn^{-1}, gg^{-1}) = (1, 1)$$

$$(\rho_{g^{-1}}(n^{-1}), g^{-1})(n, g) = (\rho_{g^{-1}}(n^{-1})\rho_{g^{-1}}(n), g^{-1}g) \stackrel{(2)}{=} (\rho_{g^{-1}}(n)^{-1}\rho_{g^{-1}}(n), g^{-1}g) = (1, 1)$$

(1) $\rho_{g^{-1}} = \rho_g^{-1}$, pues ρ es un homomorfismo.

(2) $\rho_{g^{-1}}(n^{-1}) = \rho_{g^{-1}}(n)^{-1}$, pues $\rho_{g^{-1}}$ es un homomorfismo.

La proyección en la segunda coordenada: $f : S = N \times G \rightarrow G$, $f(n, g) = g$ es un homomorfismo:

$$f((n_1, g_1)(n_2, g_2)) = f(n_1\rho_{g_1}(n_2), g_1g_2) = g_1g_2 = f(n_1, g_1)f(n_2, g_2)$$

El núcleo de f está formado por los elementos de la forma $(n, 1)$, con $n \in N$ y está claro que la aplicación $g : N \rightarrow \text{Ker } f$, dada por $g(n) = (n, 1)$ es un isomorfismo.

4. Sean p y q dos números primos. Demostrar que todo grupo de orden pq ó p^2q es resoluble.

Consideramos los casos $p = q$ y $p \neq q$ por separado. El caso $p = q$ es fácil ya que los grupos de orden p^2 son abelianos, y por tanto resolubles, y si G tiene orden p^3 entonces $Z(G) \neq 1$. Eso implica que $Z(G)$ y $G/Z(G)$ son abelianos y por tanto G es resoluble. Por tanto suponemos a partir de ahora que $p \neq q$.

Para un grupo de orden $p^r m$, con p primo que no divide a m denotamos por n_p el número de subgrupos de orden p^r . Utilizamos el Tercer Teorema de Sylow que asegura que n_p divide a m y es congruente con 1 módulo p . Está claro que si $n_p = 1$, entonces el único subgrupo de orden p es invariante por cualquier automorfismo y por tanto es normal.

Empezamos considerando un grupo G de orden pq y, por simetría, podemos suponer que $p < q$. En particular $p \not\equiv 1 \pmod{q}$, con lo que $n_q = 1$. Es decir, G tiene un subgrupo normal N de orden q . Entonces N y G/N son abelianos y por tanto G es resoluble.

Consideremos ahora un grupo G de orden p^2q . Si $n_p = 1$ entonces G tiene un subgrupo normal N de orden p^2 . Entonces N y G/N son abelianos (pues los grupos de orden primo o cuadrado de un primo son abelianos) y por tanto G es resoluble. El mismo argumento muestra que G es resoluble si $n_q = 1$.

Por tanto a partir de ahora suponemos que $n_p \neq 1$ y $n_q \neq 1$. Eso implica que $n_q = p$ ó p^2 y $n_p = q$. En particular, $q \equiv 1 \pmod{p}$ lo que implica que $p < q$ y, por tanto, $p \not\equiv 1 \pmod{q}$. Luego $n_q \neq p$ y en conclusión $n_p = q$ y $n_q = p^2$.

Es decir G tiene q subgrupos de orden p^2 y p^2 subgrupos de orden q . El único elemento que puede estar en dos subgrupos diferentes de orden q es el 1, con lo que la unión de los p^2 elementos de orden q contiene $1 + p^2(q - 1)$ elementos del grupo. Fuera de esta unión hay $p^2q - (1 + p^2(q - 1)) = p^2 - 1$. Estos elementos y el 1 son los únicos elementos que se pueden utilizar para formar subgrupos de orden p^2 , pues la intersección de un subgrupo de orden p^2 con uno de orden q es el grupo trivial. Esto muestra que sólo puede haber un subgrupo de orden p^2 , o sea $n_p = 1$, lo que nos lleva a una contradicción.

5. ¿Cuántos cuerpos intermedios tiene la extensión $\mathbb{Q}(\sqrt{3}, \xi_7)$, donde ξ_7 es una raíz sexta primitiva de la unidad? No es necesario identificar los cuerpos intermedios basta decir cuántos hay y justificarlo.

Ponemos $\xi = \xi_7$. Empezamos calculando los subcuerpos de $\mathbb{Q}(\xi)$ para lo que utilizamos $\text{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}) \simeq \mathbb{Z}_7^*$ que es un grupo cíclico de orden 6. Por tanto $H = \text{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}) = \langle b \rangle$, un grupo cíclico de orden 6 que, por tanto, tiene cuatro subgrupos $1, \langle b^3 \rangle = \langle \sigma_{-1} \rangle, \langle b^2 \rangle = \langle \sigma_2 \rangle, H$, donde σ_r denota el elemento de H dado por $\sigma(r)(\xi) = \xi^r$. Utilizando la Teoría de Galois deducimos que $\mathbb{Q}(\xi)$ tiene cuatro subcuerpos que corresponden a los cuerpos invariantes de los subgrupos.

Ahora observamos que $\mathbb{Q}(\xi) \cap \mathbb{Q}(\sqrt{3}) = \mathbb{Q}$. En caso contrario tendríamos que $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\xi)$, con lo que $\mathbb{Q}(\sqrt{3})$ sería el único subcuerpo E de $\mathbb{Q}(\xi)$ de grado 2 sobre \mathbb{Q} . Éste es el subcuerpo invariante del subgrupo de H orden 3 que es $\langle \sigma_2 \rangle$. Ponemos $\alpha = \xi + \xi^2 + \xi^4$ y observamos que $\sigma(\alpha) = \alpha$. Además, utilizando $1 + \xi + \xi^2 + \xi^3 + \xi^4 + \xi^5 + \xi^6 = 0$, observamos que

$$\alpha^2 = \xi^2 + \xi^4 + \xi + 2(\xi^3 + \xi^5 + \xi^6) = \alpha + 2(-1 - \alpha) = -2 - \alpha$$

con lo que α es una raíz de $X^2 + X + 2$, o sea

$$\alpha = \frac{-1 \pm \sqrt{-7}}{2}$$

y, por tanto $E = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{-7}) \neq \mathbb{Q}(\sqrt{3})$.

Una vez que sabemos que $\mathbb{Q}(\xi) \cap \mathbb{Q}(\sqrt{3}) = \mathbb{Q}$ tenemos, aplicando el Teorema de las Irracionalidades Accesorias de Lagrange, que

$$G = \text{Gal}(\mathbb{Q}(\sqrt{3}, \xi)/\mathbb{Q}) \simeq \text{Gal}(\mathbb{Q}(\sqrt{3})/\mathbb{Q}) \times \text{Gal}(\mathbb{Q}(\xi_7)/\mathbb{Q}) = \langle a \rangle \times \langle b \rangle$$

donde a tiene orden 2 y $\langle b \rangle$ tiene orden 6.

Tenemos que calcular el número de subcuerpos de $\mathbb{Q}(\sqrt{3}, \xi)$ que, por Teoría de Galois, es igual al número de subgrupos de G . Empezamos calculando los grupos cíclicos que son

De orden 1: 1

De orden 2: $\langle a \rangle, \langle b^3 \rangle, \langle ab^3 \rangle$.

De orden 3: $\langle b^2 \rangle = \langle b^4 \rangle$.

De orden 6: $\langle b \rangle = \langle b^5 \rangle, \langle ab \rangle = \langle ab^5 \rangle, \langle ab^2 \rangle = \langle ab^4 \rangle$.

Ahora calculamos grupos no cíclicos:

De orden 4: $\langle a, b^3 \rangle$

De orden 12: G.

En total hay 10 subgrupos y por tanto $\mathbb{Q}(\sqrt{3}, \xi)$ tiene 10 subcuerpos.

6. **Uno de los dos siguientes polinomios es resoluble por radicales sobre \mathbb{Q} y el otro no. Identificar el resoluble y el irresoluble y en ambos casos argumentar la respuesta.**

$$X^5 + 5X^4 + 10X^3 + 10X^2 + 5X - 1, \quad X^5 - 6x + 3.$$

Observando los coeficientes del primer polinomio nos damos cuenta de que es $(X+1)^5 - 2$. Por tanto el cuerpo de escisión de este polinomio es igual al del polinomio $X^5 - 2$ que es resoluble. Por tanto el otro es el que debe ser no resoluble.

Pongamos $f = X^5 - 6X + 3$. Entonces $f' = 5X^4 - 6$, con lo que f' tiene dos raíces reales: $\pm \sqrt[4]{6/5}$. Calculando $f(\pm \sqrt[4]{6/5})$ se observa que f tiene exactamente tres raíces reales y utilizando resultados de la teoría se deduce que $\text{Gal}(f/\mathbb{Q}) \simeq S_5$ que no es resoluble.

7. **¿Cuántos elementos tiene el cuerpo de descomposición del polinomio $X^5 + X^4 + 1$ sobre el cuerpo \mathbb{F}_2 de dos elementos?**

$X^5 + X^4 + 1 = (X^2 + X + 1)(X^3 + X^2 + 1)$. Por tanto el cuerpo de descomposición de $X^5 + X^4 + 1$ sobre \mathbb{F}_2 es EF , donde E es el cuerpo de descomposición de $f = X^2 + X + 1$ y F es el cuerpo de descomposición de $g = X^3 + X^2 + 1$. Tanto f como g son irreducibles sobre \mathbb{F}_2 , con lo que $E = \mathbb{F}_2[X]/(f)$ y $F = \mathbb{F}_2[X]/(g)$ y estos cuerpos tienen grados 2 y 3 sobre \mathbb{F}_2 . Eso implica que EF tiene grado 6 sobre \mathbb{F}_2 , con lo que EF tiene $2^6 = 64$ elementos.