5. Resolución de ecuaciones polinómicas por radicales

Sea $f \in K[x]$ un polinomio con coeficientes en un cuerpo de números $K \leq \mathbb{C}$. Nos plantemos el problema de saber si es posible determinar sus raíces mediante un uso reiterado de las operaciones algebraicas básicas de suma, resta, multiplicación, división y extracción de radicales desde números del cuerpo de coeficientes K. En caso positivo, diremos que **el polinomio f es resoluble por radicales sobre** K, o también que **la ecuación polinómica** $f(x) = 0$ **es resoluble por radicales** sobre K. Más formalmente, establecemos que

Definición 1. *Sea $f \in K[x]$, donde K es un cuerpo de números. Se dice que f* **es resoluble por radicales sobre** *K si existe una torre de cuerpos de números*

$$K = K_0 \leq K_1 \leq \cdots \leq K_r\,,$$

tal que cada extensión K_{i+1}/K_i es una extensión radical, y tal que su extremo K_r contenga a todas las raíces del polinomio f (lo que equivale a decir que $K(f) \leq K_r$). Una tal torre se llama una **torre radical** *de origen K en cuyo extremo el polinomio f descompone totalmente.*

Este concepto de resolubilidad de f es relativo al cuerpo K, y bien podría ser que un polinomio f sea resoluble sobre un cuerpo de números y no sobre otro. Aunque es fácil argumentar que si f es resoluble por radicales sobre un cuerpo K, entonces lo es sobre cualquier cuerpo E extensión de K: Si E/K es una extensión y $K = K_0 \leq K_1 \leq \cdots \leq K_r$ es una torre radical en cuyo extremo descompone f, donde $K_{i+1} = K_i(\alpha_i)$ con $\alpha_i^{n_i} \in K_i$, entonces, definiendo $E_0 = E$ y $E_{i+1} = E_i(\alpha_i)$, obtenemos una torre radical $E = E_0 \leq E_1 \leq \cdots \leq E_r$, en cuyo extremo están todas las raíces de f. Así que $f \in E[x]$ y f es resoluble por radicales sobre E.

Ilustramos la definición con algunos ejemplos:

- El polinomio $x^2+x-\frac{1}{2}$ es resoluble sobre $\mathbb{Q}$ (y entonces sobre cualquier cuerpo de números). Sus raíces son $\frac{-1\pm\sqrt{3}}{2}$, y ambas están en el extremo de la torre radical
$$\mathbb{Q} \leq \mathbb{Q}\big(\sqrt{3}\,\big)\,.$$
- Los polinomios $x^n - 1$ y Φ_n son resolubles sobre $\mathbb{Q}$. Su cuerpo de descomposición es la extensión ciclotómica $\mathbb{Q}(z_n)$, que es una extensión radical de $\mathbb{Q}$.
- Para cualquier $a \in K$, el polinomio $x^n - a$ es resoluble sobre K, pues todos sus raíces están en extremo de la torre radical: $K \leq K(z_n) \leq K(z_n, \sqrt[n]{a})$.
- El polinomio $x^3 - 6x^2 + 12x - 12 = (x-2)^3 - 4$ es resoluble sobre $\mathbb{Q}$. Sus raíces son
$$2 + \sqrt[3]{4},\ 2 - \frac{1 - i\sqrt{3}}{\sqrt[3]{2}},\ 2 - \frac{1 + i\sqrt{3}}{\sqrt[3]{2}}$$
y las cuatro están en el extremo de la torre radical
$$\mathbb{Q} \leq \mathbb{Q}\big(\sqrt[3]{2}\,\big) \leq \mathbb{Q}\big(\sqrt[3]{2}, i\sqrt{3}\,\big)\,.$$
- El polinomio $x^4 - 4x^3 + 7x^2 - 6x + 4 = (x-1)^4 + (x-1)^2 + 2$ es resoluble por radicales sobre $\mathbb{Q}$. Sus raíces son
$$\frac{2 \pm \sqrt{2(-1 \pm i\sqrt{7}\,)}}{2}\,,$$

y las cuatro están en el extremo de la torre radical

$$\mathbb{Q} \le \mathbb{Q}\big(\sqrt{2}\,\big) \le \mathbb{Q}\big(\sqrt{2}, i\sqrt{7}\,\big) \le \mathbb{Q}\Big(\sqrt{2}, \sqrt{-1+i\sqrt{7}}\Big) \le \mathbb{Q}\Big(\sqrt{2}, \sqrt{-1+i\sqrt{7}}, \sqrt{-1-i\sqrt{7}}\Big)\,.$$

El siguiente hecho nos prepara para el resultado fundamental sobre resolución de ecuaciones polinómicas.

Lema 2. *Si $K \le K_1 \le \cdots \le K_r$ es cualquier torre radical, entonces existe una otra torre radical $K \le E_1 \le \cdots \le E_s$, tal que $K_r \le E_s$ y E_s/K es normal.*

Demostración. Procedemos inductivamente en r.

Caso $r = 1$. Tenemos $K \le K_1$, donde $K_1 = K\big(\sqrt[n]{a}\, z_n^k\big)$, para algún $a \in K$, $n \ge 1$ y $1 \le k \le n$. Consideremos la torre

$$K \le K(z_n) \le K\big(z_n, \sqrt[n]{a}\,\big)\,.$$

Es evidente que $K_1 \le K\big(z_n, \sqrt[n]{a}\,\big)$, y puesto que $K\big(z_n, \sqrt[n]{a}\,\big)$ es justamente el cuerpo de descomposición sobre K del polinomio $x^n - a$, la extensión $K\big(z_n, \sqrt[n]{a}\,\big)/K$ es normal.

Caso $r > 1$. Por hipótesis de inducción, existe una torre radical $K \le F_1 \le \cdots \le F_t$, tal que $K_{r-1} \le F_t$ y F_t/K es normal. Será F_t el cuerpo de descomposición sobre K de algún polinomio $f \in K[x]$, esto es, $F_t = K(\alpha_1, \ldots, \alpha_l)$ donde $\alpha_1, \ldots, \alpha_l$ son las diferentes raíces en $\mathbb{C}$ de ese f. Supongamos que su grupo de Galois es $G(F_t/K) = \{\sigma_1 = id, \sigma_2, \ldots, \sigma_m\}$.

Puesto que K_r/K_{r-1} es radical, será $K_r = K_{r-1}(\sqrt[n]{a}\, z_n^k)$, para algún $a \in K_{r-1}$, $n \ge 1$ y $1 \le k \le n$. Construimos entonces la torre radical

$$K \le F_1 \le \cdots \le F_t \le F_t(z_n) \le F_t\big(z_n, \sqrt[n]{a}\,\big) \le F_t\big(z_n, \sqrt[n]{a}, \sqrt[n]{\sigma_2(a)}\,\big) \le \cdots$$

$$\cdots \le F_t\big(z_n, \sqrt[n]{a}, \sqrt[n]{\sigma_2(a)}, \ldots, \sqrt[n]{\sigma_m(a)}\,\big) = E_s\,.$$

Manifiestamente se trata de una torre radical y $K_r \le E_s$. Bastará por tanto argumentar que E_s/K es normal:

Consideremos el polinomio $g = \prod_{i=1}^m \big(x^n - \sigma_i(a)\big) \in F_t[x]$. Para cualquier $\sigma \in G(F_t/K)$, la lista $(\sigma\sigma_1, \ldots, \sigma\sigma_m)$ es una permutación de la lista $(\sigma_1, \ldots, \sigma_m)$, y por consiguiente

$$g^\sigma = \prod_{i=1}^m (x^n - \sigma\sigma_i(a)) = \prod_{i=1}^m (x^n - \sigma_i(a)) = g;$$

esto es, los coeficientes de g están en el cuerpo fijo $F_t^{G(F_t/K)} = K$. Así que $g \in K[x]$. El cuerpo de descomposición sobre K del polinomio producto fg es justamente

$$K\big(\alpha_1, \ldots \alpha_k, z_n, \sqrt[n]{a}, \sqrt[n]{\sigma_2(a)}, \ldots, \sqrt[n]{\sigma_m(a)}\,\big) = F_t\big(z_n, \sqrt[n]{a}, \sqrt[n]{\sigma_2(a)}, \ldots, \sqrt[n]{\sigma_m(a)}\,\big) = E_s\,,$$

y concluimos que la extensión E_s/K es efectivamente normal. □

Proposición 3. *Si $f \in K[x]$ es resoluble, existe una torre radical $K = K_0 \le K_1 \le \cdots \le K_r$ tal que K_r/K es normal y $K(f) \le K_r$.*

Recordemos ahora que, si $f \in K[x]$, donde $K \le \mathbb{C}$ es un cuerpo de números, su **grupo de Galois sobre** K, denotado por $G(f/K)$, es el grupo de Galois sobre K de su cuerpo de descomposición. Esto es, $G(f/K) = G(K(f)/K)$.

Teorema 4 (Abel-Galois)**.** * *Un polinomio sobre un cuerpo de números es resoluble si y solo si su grupo de Galois es resoluble.*

DEMOSTRACIÓN. *Necesidad*: Por hipótesis, y aplicando el anterior lema, existe una torre radical $K = K_0 \leq K_1 \leq \cdots \leq K_r$, tal que f descompone totalmente en su extremo K_r y K_r/K es una extensión normal. Supongamos que cada $K_{i+1} = K_i(\alpha_i)$, donde $\alpha_i^{n_i} \in K_i$. Si tomamos $n = \prod n_i$ tendremos que $\alpha_i^n \in K_i$, para todo $i = 0, \ldots, r-1$, de manera que cada extensión K_{i+1}/K_i es una extensión radical generada por una raíz n-ésima de un elemento de K_i. Consideremos la raíz n-ésima primitiva de la unidad, $z = z_n$, y construimos la torre

$$K = K_0 \leq K_0(z) \leq K_1(z) \leq \cdots \leq K_r(z)\,.$$

Esta es también una torre radical, ya que $K_{i+1}(z) = K_i(\alpha_i, z) = K_i(z)(\alpha_i)$ y $\alpha_i^n \in K_i(z)$, y se verifica también que $K_r(z)/K$ es normal (ya que si K_r es el cuerpo de descomposición de un polinomio $g \in K[x]$, entonces $K_r(z)$ es el cuerpo de descomposición sobre K del polinomio producto $g(x^n - 1)$) y, obviamente, todas las raíces de f están en $K_r(z)$. Probaremos ahora sucesivamente los siguientes hechos:

(1) El grupo de Galois $G\big(K_r(z)/K(z)\big)$ es resoluble.
(2) El grupo de Galois $G\big(K_r(z)/K\big)$ es resoluble.
(3) El grupo de Galois $G\big(f/K\big) = G\big(K(f)/K\big)$ es resoluble.

(1): La extensión $K_r(z)/K$ es normal y la torre de subcuerpos

$$K(z) = K_0(z) \leq K_1(z) \leq \cdots \leq K_i(z) \leq K_{i+1}(z) \leq \cdots \leq K_r(z)\,,$$

corresponde por la conexión de Galois a la torre de subgrupos de su grupo de Galois

$$G\big(K_r(z)/K_0(z)\big) \geq \cdots \geq G\big(K_r(z)/K_i(z)\big) \geq G\big(K_r(z)/K_{i+1}(z)\big) \geq \cdots \geq G\big(K_r(z)/K_r(z)\big) = \{id\}.$$

Y resulta que esta es precisamente una serie del grupo $G\big(K_r(z)/K(z)\big)$ con factores cíclicos, de donde el grupo es resoluble. En efecto, puesto que cada $K_{i+1}(z)/K_i(z)$ es una extensión radical generada por una raíz n-ésima, y $z = z_n \in K_i(z)$, por el Teorema de Lagrange la extensión $K_{i+1}(z)/K_i(z)$ es cíclica, o sea, normal y con grupo de Galois $G\big(K_{i+1}(z)/K_i(z)\big)$ cíclico. Ahora, aplicando el Teorema Fundamental de la Teoría de Galois a la torre

$$K_i(z) \leq K_{i+1}(z) \leq K_r(z),$$

podemos asegurar que

$$G\big(K_r(z)/K_{i+1}(z)\big) \trianglelefteq G\big(K_r(z)/K_i(z)\big),$$

y que

$$G\big(K_{i+1}(z)/K_i(z)\big) \cong \frac{G\big(K_r(z)/K_i(z)\big)}{G\big(K_r(z)/K_{i+1}(z)\big)}.$$

(2): En la torre $K \leq K(z) \leq K_r(z)$, la extensión $K(z)/K$ es normal (es ciclotómica). Por tanto

$$G\big(K_r(z)/K(z)\big) \trianglelefteq G\big(K_r(z)/K)\big)\,, \quad \text{y} \quad G\big(K(z)/K\big) \cong \frac{G\big(K_r(z)/K\big)}{G\big(K_r(z)/K(z)\big)}\,.$$

Conocemos que el grupo de Galois de la extensión ciclotómica $K(z)/K$ es abeliano y, por tanto resoluble; luego el grupo $G\big(K_r(z)/K\big)$ contiene un subgrupo normal y resoluble (por (1)), cuyo cociente es también resoluble y podemos concluir que él mismo es resoluble.

(3): Puesto que en $K_r(z)$ están todas las raíces de f, el cuerpo de descomposición de este polinomio sobre K está contenido en él, así que $K \leq K(f) \leq K_r(z)$. Entonces,

$$G\big(K_r(z)/K(f)\big) \trianglelefteq G\big(K_r(z)/K)\big)\,, \quad \text{y} \quad G\big(K(f)/K\big) \cong \frac{G\big(K_r(z)/K\big)}{G\big(K_r(z)/K(f)\big)}\,.$$

Como todo grupo cociente de un resoluble es resoluble, concluimos que $G(f/K) = G\big(K(f)/K\big)$ es resoluble.

Suficiencia: Denotemos por $E = K(f)$ al cuerpo de descomposición de f sobre K. Por hipótesis el grupo $G\big(E/K\big)$ es resoluble. Supongamos que $[E : K] = n$. Llamemos $z = z_n$ y consideremos la torre $K \leq K(z) \leq E(z)$. Como $E(z) = K(f(x^n - 1))$, la extensión $E(z)/K$ es normal, y también entonces lo es la extensión $E(z)/K(z)$. Si $\sigma \in G\big(E(z)/K(z)\big)$, su restricción a E es una K-inmersión compleja del cuerpo E y, por tanto, ya que E una extensión normal de K, se verificará que $\sigma\big(E\big) = E$; así que $\sigma|_E \in G\big(E/K\big)$. La correspondencia

$$G\big(E(z)/K(z)\big) \longrightarrow G\big(E/K\big)\,, \quad \sigma \mapsto \sigma|_E\,,$$

es un homomorfismo de grupos que fácilmente se reconoce como un monomorfismo (si $\sigma|_E = id$, como $\sigma(z) = z$, entonces $\sigma \in G\big(E(z)/E(z)\big) = \{id\}$). Desde que todo subgrupo de un grupo resoluble lo es así mismo, concluimos que el grupo $G\big(E(z)/K(z)\big)$ es resoluble.

Existirá entonces una serie de ese grupo

$$G\big(E(z)/K(z)\big) = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_{r-1} \trianglerighteq G_r = \{id\}\,,$$

cuyos factores G_i/G_{i+1} son cíclicos y de orden un divisor de $n = |G(E/K)|$ (el orden de cada G_i es un divisor del orden del grupo $G\big(E(z)/K(z)\big)$ que a su vez es un divisor del orden del grupo $G(E/K)$ que es $n = [E : K]$). Por la Conexión de Galois, tendremos asociada una torre de subcuerpos

$$K(z) = E(z)^{G_0} \leq E(z)^{G_1} \leq \cdots E(z)^{G_i} \leq E(z)^{G_{i+1}} \leq \cdots \leq E(z)^{G_r} = E(z)\,. \tag{1}$$

Como cada $G_i = G\big(E(z)/E(z)^{G_i}\big)$ y es $G_{i+1} \trianglelefteq G_i$, el Teorema Fundamental de la Teoría de Galois, aplicado a cada torre $E(z)^{G_i} \leq E(z)^{G_{i+1}} \leq E(z)$, nos garantiza que cada eslabón $E(z)^{G_{i+1}}/E(z)^{G_i}$ de la torre (1) es una extensión normal con grupo de Galois

$$G\Big(E(z)^{G_{i+1}}/E(z)^{G_i}\Big) \cong G_i/G_{i+1}\,,$$

que es cíclico de orden un divisor de n. Como $z = z_n \in E(z)^{G_i}$, por el Teorema de Lagrange podemos concluir que cada extensión $E(z)^{G_{i+1}}/E(z)^{G_i}$ de la torre (1) es una extensión radical. Así que (1) es una torre de extensiones radicales, de manera que también lo es la torre

$$K \leq K(z) = E(z)^{G_0} \leq E(z)^{G_1} \leq \cdots E(z)^{G_i} \leq E(z)^{G_{i+1}} \leq \cdots \leq E(z)^{G_r} = E(z)\,.$$

en cuyo extremo están todas las raíces de f. □

Corolario 5 (Teorema de Abel)**.** *Todo polinomio cuyo grupo de Galois es conmutativo es resoluble por radicales.*

Debido al anterior resultado, los grupos conmutativos se llaman **abelianos**.

5.1. **El grupo de Galois como grupo de permutaciones.**

Supongamos que un polinomio $f = \sum_i a_i x^i \in K[x]$, con coeficientes en un cuerpo de numeros $K \leq \mathbb{C}$, tiene n raíces complejas diferentes, y que numeramos estas en la forma $\alpha_1, \ldots, \alpha_n$.

Si $\sigma \in G(f/K) = G\big(K(\alpha_1, \ldots, \alpha_n)/K\big)$, entonces para cualquier raíz α_j de f se tiene que

$$f(\sigma(\alpha_j)) = \sum_i a_i \sigma(\alpha_j) = \sum_i \sigma(a_i)\sigma(\alpha_j) = \sigma\big(\sum_i a_i \alpha_j\big) = \sigma(0) = 0.$$

Esto es, $\sigma(\alpha_j)$ es de nuevo una raíz del polinomio f. Se sigue que cada $\sigma \in G(f/K)$ define, por restricción, una aplicación, a la que denotaremos igual,

$$\sigma : \{\alpha_1, \ldots, \alpha_n\} \to \{\alpha_1, \ldots, \alpha_n\}\,, \qquad \alpha_j \mapsto \sigma(\alpha_j)\,,$$

que es inyectiva (σ lo es), y entonces biyectiva. Así que la restricción de σ al conjunto $\{\alpha_1, \ldots, \alpha_n\}$ de las raíces de f es una permutación en este conjunto. La aplicación

$$G(f/K) \to S_n, \quad \sigma \mapsto \sigma \mid \sigma(i) = j \text{ si } \sigma(\alpha_i) = \alpha_j,$$

es un homomorfismo de grupos que es de hecho un monomorfismo (si $\sigma, \sigma' \in\in G(f/K)$ definiesen la misma permutación de S_n, sería por que actúan igualmente sobre todos los generadores α_i de la extensión $K(\alpha_1, \cdots, \alpha_n)$ y sería $\sigma = \sigma'$; ver Lema 2.20 en Tema 2). Consecuentemente, esa aplicación establece un isomorfismo entre el grupo de Galois del polinomio y su imagen. De esta forma vemos que

"El grupo de Galois $G(f/K)$ es isomorfo a un subgrupo de S_n."

Ejemplo 6. Consideremos el polinomio

$$f = x^3 - 7x^2 + 12x - 4 = (x-2)(x^2 - 5x + 2) \in \mathbb{Q}[x].$$

Sus raíces son $\alpha_1 = 2$, $\alpha_2 = \frac{5-\sqrt{17}}{2}$ y $\alpha_3 = \frac{5+\sqrt{17}}{2}$. Su cuerpo de descomposición es $\mathbb{Q}(\sqrt{17})$. Su grupo de Galois es

$$G(f/\mathbb{Q}) = G\big(\mathbb{Q}(\sqrt{17})/\mathbb{Q}\big) = \{id, \sigma\},$$

donde $\sigma : \mathbb{Q}(\sqrt{17}) \to \mathbb{Q}(\sqrt{17})$ es el automorfismo definido por $\sigma(a + b\sqrt{17}) = a - b\sqrt{17}$. Puesto que $\sigma(\alpha_1) = \alpha_1$, $\sigma(\alpha_2) = \alpha_3$ y $\sigma(\alpha_3) = \alpha_2$, vemos que $G(f/\mathbb{Q})$ es isomorfo al subgrupo de S_3 que consiste de la identidad y de la trasposición $(2, 3)$. Esto es, salvo isomorfismo,

$$G\big(x^3 - 7x^2 + 12x - 4\big) = \{id, (2,3)\} \leq S_3,$$

Por supuesto, que también concluimos que $G\big(x^3 - 7x^2 + 12x - 4\big) \cong C_2$ es un grupo cíclico de orden dos.

En varias ocasiones nos será de utilidad recurrir al polinomio reducido asociado a un polinomio. Un polinomio mónico $f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in K[x]$, donde K es un cuerpo de números, diremos que es **reducido** si $a_{n-1} = 0$. Puesto que, si $\alpha_1, \ldots, \alpha_n$ son sus raíces, es $f = \prod_{i=1}^{n}(x - \alpha_i)$ y, por tanto, $a_{n-1} = -(\alpha_1 + \cdots + \alpha_n)$. Resulta que f es reducido si y solo si sus raíces suman cero.

Para cualquier $f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, mónico de grado n, se define su correspondiente **"reducido"** $\tilde{f}$ como el obtenido desde f al reemplazar la indeterminada x por $x - \frac{a_{n-1}}{n}$, esto es,

$$\tilde{f} = f\big(x - \tfrac{a_{n-1}}{n}\big)\,.$$

Si las raíces de $\tilde{f}$ son β_i, $i = 1, \ldots, n$, entonces las de f son $\alpha_i = \beta_i - \frac{a_{n-1}}{n}$, $i = 1, \ldots, n$. Como $\sum \beta_i = \sum(\alpha_i + \frac{a_{n-1}}{n}) = \sum \alpha_i + n\frac{a_{n-1}}{n} = -a_{n-1} + a_{n-1} = 0$, el polinomio $\tilde{f}$ es efectivamente reducido. Notemos también que f y $\tilde{f}$ tienen el mismo cuerpo de descomposición sobre K. Consecuentemente,

$$G(f/K) = G(\tilde{f}/K)\,.$$

Ejemplo 7. *Si $f = x^2 + 2x + 3$, su reducido es*

$$\tilde{f} = f(x-1) = (x-1)^2 + 2(x-1) + 3 = x^2 - 2x + 1 + 2x - 2 + 3 = x^2 + 2. \quad \square$$

5.2. **Ecuaciones cuadráticas.**

El grupo de Galois de un polinomio cuadrático sobre cualquier cuerpo de números es un subgrupo de S_1 o de S_2, según el número de raíces distintas que tenga, por tanto este siempre es resoluble por radicales. De hecho es bien familiar para todos la fórmula que permite el cálculo de sus raíces (y cuyo conocimiento histórico se remonta a la civilización babilónica):

Consideremos la ecuación cuadrática

$$x^2 + bx + c = 0\,,$$

cuyas soluciones son las raíces del polinomio cuadrático $f = x^2 + bx + c$. Reemplazando x por $x - \frac{b}{2}$, obtenemos su reducido

$$\tilde{f} = f\big(x - \frac{b}{2}\big) = x^2 - \frac{b^2 - 4c}{4},$$

cuyas raíces son claramente $\beta_1 = \frac{1}{2}\sqrt{b^2 - 4c}$ y $\beta_2 = -\frac{1}{2}\sqrt{b^2 - 4c}$. Entonces, las soluciones de la ecuación cuadrática original son $\alpha_i = \beta_i - \frac{b}{2}$, $i = 1, 2$; esto es,

$$\alpha_1 = \frac{-b - \sqrt{b^2 - 4c}}{2} \quad \text{y} \quad \alpha_2 = \frac{-b + \sqrt{b^2 - 4c}}{2}\,.$$

5.3. **Ecuaciones cúbicas.**

El grupo de Galois de un polinomio cúbico sobre cualquier cuerpo de números es un subgrupo de S_1, S_2 o S_3, según el número de raíces distintas que tenga, por tanto este siempre es resoluble. De hecho existen varios métodos para el cálculo de sus raíces. El primero es debido a Scipio del Ferro (1515: Martin Luther, La Reforma, El Renaciminento, ...), aunque una fórmula equivalente fue descubierta por Tartaglia sobre el mismo tiempo, y aparece impreso por primera vez en un libro de Cardano (1545), por lo que usualmente es conocida como el método de "Cardano".

Consideremos la ecuación cúbica

$$x^3 + bx^2 + cx + d = 0\,.$$

Obtengamos su reducida reemplazando x por $x - \frac{b}{3}$, que ser de la forma

$$x^3 + p\,x + q = 0\,,$$

cuyas soluciones $\beta_1, \beta_2, \beta_3$ nos darán las de la original por las igualdades $\alpha_i = \beta_i - \frac{b}{3}$, $i = 1, 2, 3$. La idea es obtener las soluciones x de la reducida como suma de dos números, digamos $x = y + z$, tales que $yz = \frac{-p}{3}$. Bajo esta última condición, obtener x es lo mismo que obtener y y z, pues dos números están totalmente determinados por quién sea su suma y su producto (si suman S y multiplica P, son las dos raíces del polinomio cuadrático $x^2 - Sx + P$). Ahora, $x = y + z$ es solución de la cúbica reducida si y solo si

$$\begin{aligned} 0 &= (y+z)^3 + p(y+z) + q = y^3 + z^3 + 3yz^2 + 3y^2 z + py + pz + q \\ &= y^3 + z^3 + 3z\frac{-p}{3} + 3y\frac{-p}{3} + py + pz + q = y^3 + z^3 - pz - py + py + pz + q \\ &= y^3 + z^3 + q. \end{aligned}$$

Esto es, si y solo si $y^3 + z^3 = -q$. Formamos entonces el sistema

$$\begin{cases} y^3 + z^3 = -q, \\ y^3 z^3 = \frac{-p^3}{27}, \end{cases}$$

que nos permite calcular y^3 y z^3 como las dos raíces del polinomio de segundo grado

$$x^2 + q\,x - \frac{p^3}{27} = 0,$$

obteniendo que (los valores de y y z son intercambiables sin que afecte al resultado de $x = y + z$)

$$y^3 = \frac{-q + \sqrt{q^2 + \frac{4}{27}p^3}}{2}, \quad z^3 = \frac{-q - \sqrt{q^2 + \frac{4}{27}p^3}}{2}\,.$$

Ahora, si $\omega = z_3 = e^{\frac{2\pi i}{3}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ es la raíz cúbica primitiva de la unidad, tenemos como posibles valores de y:

$$y_1 = \sqrt[3]{\frac{-q + \sqrt{q^2 + \frac{4}{27}p^3}}{2}}, \quad y_2 = \omega\sqrt[3]{\frac{-q + \sqrt{q^2 + \frac{4}{27}p^3}}{2}} \quad \text{e} \quad y_3 = \omega^2\sqrt[3]{\frac{-q + \sqrt{q^2 + \frac{4}{27}p^3}}{2}};$$

y de z:

$$z_1 = \sqrt[3]{\frac{-q - \sqrt{q^2 + \frac{4}{27}p^3}}{2}}, \quad z_2 = \omega\sqrt[3]{\frac{-q - \sqrt{q^2 + \frac{4}{27}p^3}}{2}} \quad \text{y} \quad z_3 = \omega^2\sqrt[3]{\frac{-q - \sqrt{q^2 + \frac{4}{27}p^3}}{2}}.$$

Para cualquiera de esas posibilidades se verifica que $y_j^3 + z_k^3 = -q$. Pero necesitamos que $y_j z_k = -p/3$ (para que $x = y_j + z_k$ sea solución de la cúbica reducida), y solo sabemos que $(y_j z_k)^3 = (-p/3)^3$ o, lo que es lo mismo, que $y_j z_k \in \{-p/3, -(p/3)\omega, -(p/3)\omega^2\}$. Entonces, cada y_j debe ser apareado con el z_k tal que su producto sea exactamente $-p/3$. Esto nos lleva a una breve discusión, que haríamos así:

- Si $y_1 z_1 = -p/3$, entonces $y_2 z_3 = -p/3 = y_3 z_2$, luego las soluciones de la reducida serían $\beta_1 = y_1 + z_1$, $\beta_2 = y_2 + z_3$ y $\beta_3 = y_3 + z_2$.
- Si fuese $y_1 z_1 = (-p/3)\omega$, entonces $y_1 z_3 = -p/3 = y_2 z_2 = y_3 z_1$, luego las soluciones serían $\beta_1 = y_1 + z_3$, $\beta_2 = y_2 + z_2$ y $\beta_3 = y_3 + z_1$.
- Si fuese $y_1 z_1 = (-p/3)\omega^2$, entonces $y_1 z_2 = -p/3 = y_2 z_1 = y_3 z_3$, y las soluciones $\beta_1 = y_1 + z_2$, $\beta_2 = y_2 + z_1$ y $\beta_3 = y_3 + z_3$.

Ejemplo 8. *Resolver la ecuación* $x^3 + 6x^2 + 9x + 4 = 0$

SOLUCIÓN: Sea $f = x^3 + 6x^2 + 9x + 4$. El reducido será

$$\tilde{f} = f(x-2) = (x-2)^3 + 6(x-2)^2 + 9(x-2) + 4 = \cdots = x^3 - 3x + 2.$$

Siguiendo el método de Cardano, buscamos sus raíces en la forma $x = y + z$ tal que $yz = 1$, y resulta que y^3 y z^3 han de ser soluciones al sistema

$$\begin{cases} y^3 + z^3 = -2, \\ y^3 z^3 = 1, \end{cases}$$

que nos permite calcular y^3 y z^3 como las dos soluciones de la ecuación $x^2 + 2x + 1 = 0$. Por tanto $y^3 = -1 = z^3$. Esto nos da tres posibles ys y zs:

$$\begin{cases} y_1 = e^{i\frac{\pi}{3}} = \frac{1}{2} + i\frac{\sqrt{3}}{2}, \\ y_2 = \omega y_1 = e^{i\frac{2\pi}{3}} e^{i\frac{\pi}{3}} = e^{i\pi} = -1, \\ y_3 = \omega^2 y_1 = e^{i\frac{4\pi}{3}} e^{i\frac{\pi}{3}} = e^{i\frac{5\pi}{3}} = \frac{1}{2} - i\frac{\sqrt{3}}{2}, \end{cases}$$

$$\begin{cases} z_1 = e^{i\frac{\pi}{3}} = \frac{1}{2} + i\frac{\sqrt{3}}{2}, \\ z_2 = \omega z_1 = e^{i\frac{2\pi}{3}} e^{i\frac{\pi}{3}} = e^{i\pi} = -1, \\ z_3 = \omega^2 z_1 = e^{i\frac{4\pi}{3}} e^{i\frac{\pi}{3}} = e^{i\frac{5\pi}{3}} = \frac{1}{2} - i\frac{\sqrt{3}}{2} \end{cases}$$

Estas han de emparejarse de manera que $y_j z_k = 1$. Vemos que $y_2 z_2 = (-1)(-1) = 1$, $y_1 z_3 = e^{i\frac{\pi}{3}} e^{i\frac{5\pi}{3}} = 1$ y que $y_3 z_1 = e^{i\frac{5\pi}{3}} e^{i\frac{\pi}{3}} = 1$, lo que nos da las raíces de la cúbica reducida

$$\begin{cases} \beta_1 = y_2 + z_2 = (-1) + (-1) = -2, \\ \beta_2 = y_1 + z_3 = \frac{1}{2} + i\frac{\sqrt{3}}{2} + \frac{1}{2} - i\frac{\sqrt{3}}{2} = 1, \\ \beta_3 = y_3 + z_1 = \frac{1}{2} - i\frac{\sqrt{3}}{2} + \frac{1}{2} + i\frac{\sqrt{3}}{2} = 1. \end{cases}$$

Luego las soluciones de la ecuación $x^3+6x^2+9x+4=0$ son

$$\begin{cases} \alpha_1=\beta_1-2=-4, \\ \alpha_2=\beta_2-2=-1, \\ \alpha_3=\beta_3-2=-1. \end{cases}$$

5.4. **Ecuaciones cuárticas.**

El grupo de Galois de un polinomio de grado cuatro es un subgrupo de S_1, de S_2, de S_3, o de S_4, según el número de raíces diferentes que tenga, por tanto este siempre es resoluble. Y también en este caso hay fórmulas para la determinación de sus raíces. La primera fórmula cuártica fue encontrada por Luigi Ferrari (1545), pero nosotros aprenderemos el método de Descartes (1637) que comentamos a continuación.

Consideremos la ecuación cuártica

$$x^4+bx^3+cx^2+dx+e=0\,,$$

cuyas soluciones, es decir la raíces del polinomio $f=x^4+bx^3+cx^2+dx+e$, las denotaremos por $\alpha_1,\alpha_2,\alpha_3$ y α_4 respectivamente. Reemplazando x por $x-\frac{b}{4}$, obtenemos su reducido

$$\tilde{f}=x^4+p\,x^2+qx+r\,,$$

cuyas soluciones $\beta_1,\beta_2,\beta_3,\beta_4$ nos darán las de la original por las igualdades $\alpha_i=\beta_i-\frac{b}{4}$.

Supuesto $q\neq 0$ (en otro caso estamos en presencia de una bicuadrática, fácil de resolver), el procedimiento de Descartes consiste en determinar números complejos k,ℓ y m, de tal manera que se de la igualdad

$$x^4+p\,x^2+qx+r=(x^2+kx+\ell)(x^2-kx+m)\,, \tag{2}$$

y, entonces, calcular las raíces de $\tilde{f}$ por la fórmula cuadrática para cada factor. Notemos que el término de grado uno en el segundo factor cuadrático ha de ser $-k$ puesto que la cuártica no tiene término cúbico.

Al desarrollar el miembro de la derecha e igualar coeficientes de términos del mismo grado, nos encontramos con el sistema

$$\begin{cases} -k^2+\ell+m &= p\,, \\ k(m-\ell) &= q\,, \\ \ell m &= r\,. \end{cases}$$

las primeras dos ecuaciones pueden expresarse como $m+\ell=p+k^2$ y $m-\ell=\frac{q}{k}$ ($k\neq 0$, pues $q\neq 0$), lo que nos lleva a que

$$\begin{aligned} m &= \tfrac{1}{2}(k^2+p+\tfrac{q}{k})=\tfrac{k^3+pk+q}{2k}\,, \\ \ell &= \tfrac{1}{2}(k^2+p-\tfrac{q}{k})=\tfrac{k^3+pk-q}{2k}, \end{aligned}$$

y sustituyendo en la tercera, obtenemos la ecuación para k

$$\tfrac{k^3+pk+q}{2k}\,\tfrac{k^3+pk-q}{2k}=r\Leftrightarrow (k^3+pk+q)(k^3+pk-q)=4k^2r\Leftrightarrow$$

$$k^6+2p\,k^4+(p^2-4r)k^2-q^2=0.$$

De manera que k^2 ha de solución de la ecuación cúbica

$$x^3+2p\,x^2+(p^2-4r)x-q^2=0\,, \tag{3}$$

(que es llamada la "resolvente cúbica" de la cuártica) y uno puede entonces determinar un valor de k^2 usando el método de Cardano. Desde ahí, es ahora fácil determinar valores de k, ℓ y m, de manera que se tenga la factorización (2), y entonces determinar las raíces de $\tilde{f}$.

Ejemplo 9. *Resolver la ecuación* $x^4-8x^3+24x^2-28x+11=0$

SOLUCIÓN: Si $f = x^4 - 8x^3 + 24x^2 - 28x + 11$, su reducido es

$$\tilde{f} = f(x+2) = (x+2)^4 - 8(x+2)^3 + 24(x+2)^2 - 28(x+2) + 11 = \cdots = x^4 + 4x + 3.$$

Siguiendo el método de Descartes, buscamos la factorización en $\mathbb{C}[x]$

$$x^4 + 4x + 3 = (x^2 + kx + l)(x^2 - kx + m),$$

donde los posibles valores de k, l, m habrán de satisfacer las ecuaciones

$$\begin{array}{rcl} l + m - k^2 & = & 0 \\ k(m-l) & = & 4 \\ lm & = & 3 \end{array}$$

Las dos primeras nos dicen que $m + l = k^2$ y $m - l = 4/k$ (por la ecuación 2^{a}, $k \neq 0$). Equivalentemente,

$$m = \frac{k^2 + \frac{4}{k}}{2} = \frac{k^3 + 4}{2k}, \qquad l = \frac{k^2 - \frac{4}{k}}{2} = \frac{k^3 - 4}{2k}.$$

Llevando esto a la última, obtenemos que $(k^3 + 4)(k^3 - 4) = 12k^2$, esto es, $k^6 - 16 = 12k^2$. En definitiva, k^2 es cualquier raíz de la ecuación cúbica ("resolvente cúbica de la cuártica")

$$x^3 - 12x - 16 = 0$$

Y procedemos a buscar una de sus soluciones, siguiendo el método de Cardano. Buscamos sus soluciones en la forma $x = y + z$ de manera que $yz = 4$, y resulta que y^3 y z^3 son las soluciones de la ecuación $x^2 - 16x + 64$:

$$\frac{16 \pm \sqrt{16^2 - 4 \cdot 64}}{2} = 8 \qquad \text{(solución doble)}.$$

Una de las soluciones de la resolvente cúbica es entonces $y_1 + z_1 = \sqrt[3]{8} + \sqrt[3]{8} = 2 + 2 = 4$. Entonces podemos tomar k cualquiera tal que $k^2 = 4$.

Tomemos $k = 2$, en cuyo caso $l = (8-4)/4 = 1$ y $m = (8+4)/4 = 3$. Así que

$$x^4 + 4x + 3 = (x^2 + 2x + 1)(x^2 - 2x + 3).$$

Y ya es fácil ver que las soluciones de la cuártica propuesta son

$$1 \ (doble), 3 + i\sqrt{2},\ 3 - i\sqrt{2}.$$

5.5. **Irresolubilidad en grado superior. Teorema de Abel-Ruffini.**

El resultado fundamental aquí es la existencia de ecuaciones quínticas irresolubles (y entonces de cualquier grado mayor o igual que cinco). Este resultado fue esencialmente probado por Ruffini (1799) y Abel (1824), aunque sus demostraciones no fueron correctas en todos los detalles (si bien la de Abel fue aceptada, al contrario de la de Ruffini).

Lema 10. *Si $f \in \mathbb{Q}[x]$ es irreducible, entonces el orden del grupo $G(f/\mathbb{Q})$ es un múltiplo del grado de f.*

DEMOSTRACIÓN. Podemos asumir que f es mónico, y supongamos que grado n. Sea α cualquier raíz de f en $\mathbb{C}$. Entonces $f = Irr(\alpha, \mathbb{Q})$ y tenemos que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$. Por la fórmula multiplicativa del grado para la torre $\mathbb{Q} \leq \mathbb{Q}(\alpha) \leq \mathbb{Q}(f)$, tenemos que

$$[\mathbb{Q}(f) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}][\mathbb{Q}(f) : \mathbb{Q}(\alpha)] = n\,[\mathbb{Q}(f) : \mathbb{Q}(\alpha)].$$

Así que el grado de la extensión $\mathbb{Q}(f)/\mathbb{Q}$ es un múltiplo de n. Como el grupo $G(f/\mathbb{Q}) = G(\mathbb{Q}(f)/\mathbb{Q})$ es de orden igual al grado de la extensión $\mathbb{Q}(f)/\mathbb{Q}$, se deduce el resultado. □

Lema 11. *Sea p un número primo. Si $G \leq S_p$ es un subgrupo cuyo orden es múltiplo de p y contiene una trasposición, entonces $G = S_p$.*

DEMOSTRACIÓN.: Supongamos que G contiene a la trasposición (a_1, a_2). Como p divide a su orden, G contendrá una permutación de orden p. Como p es primo y el orden de una permutación es igual al mínimo común múltiplo de las longitudes de los ciclos disjuntos en que descompone, esa permutación de orden p será necesariamente un ciclo de longitud p, digamos σ, que podremos escribir en la forma $\sigma = (b_1, \ldots, b_p)$ con $b_1 = a_1$. Si $a_2 = b_{r+1}$, entonces $\sigma^r(a_1) = \sigma^r(b_1) = b_{r+1} = a_2$. Como σ^r es también de orden p (pues p es primo), será también un p-ciclo, que se escribirá de la forma $(a_1, a_2, \ldots, a_p)$. Así que tenemos que el subgrupo G de S_p contiene a la trasposición (a_1, a_2) y al p-ciclo $(a_1, a_2, \ldots, a_p)$.

Por las igualdades

$$(a_1, a_2, \ldots, a_p)(a_i, a_{i+1})(a_1, a_2, \ldots, a_p)^{-1} = (a_{i+1}, a_{i+2})$$

y una fácil inducción, deducimos que todas las trasposiciones de la forma (a_i, a_{i+1}) están en el subgrupo G. Entonces, por las igualdades

$$(a_1, a_i)(a_i, a_{i+1})(a_1, a_i) = (a_1, a_{i+1})$$

deducimos que todas las trasposiciones de la forma (a_1, a_i) están en el subgrupo G. Finalmente, or las igualdades

$$(a_1, a_i)(a_1, a_j)(a_1, a_i) = (a_i, a_j)$$

concluimos que todas las trasposiciones (a_i, a_j) de S_p están en el subgrupo G. Puesto que toda permutación es producto de trasposiciones, $G = S_p$. □

Proposición 12. *Sea $f \in \mathbb{Q}[x]$ un polinomio irreducible de grado un número primo p y que tiene exactamente dos raíces complejas no reales. Entonces $G(f/\mathbb{Q}) \cong S_p$.*

DEMOSTRACIÓN. Sean $\alpha_1, \alpha_2, \ldots, \alpha_p \in \mathbb{C}$ las raíces del polinomio, donde $\alpha_1, \alpha_2 \in \mathbb{C}$, $\alpha_1, \alpha_2 \notin \mathbb{R}$ y $\alpha_3, \ldots, \alpha_p \in \mathbb{R}$. Recordemos el monomorfismo de grupos

$$G(f/K) \to S_p, \quad \sigma \mapsto \sigma \mid \sigma(i) = j \text{ si } \sigma(\alpha_i) = \alpha_j.$$

Así que, si $G \leq S_p$ es el subgrupo imagen, será $G(f/\mathbb{Q}) \cong G$. Probamos ahora que $G = S_p$:

Por el Lema 10, sabemos que el orden del grupo $G(f/\mathbb{Q})$ es múltiplo de p, por tanto también lo será el orden de G. Por el Lema 11 anterior, bastara probar que G contiene una trasposición. Para ello, observemos que la aplicación que asocia a cada complejo su conjugado, $z \mapsto \bar{z}$, restringe dando una $\mathbb{Q}$-inmersión compleja $\mathbb{Q}(f) \to \mathbb{C}$ que, por la normalidad, define un elemento del grupo $G(f/\mathbb{Q}) = G(\mathbb{Q}(f)/\mathbb{Q})$. Es evidente que este deja fijas todas las raíces reales y altera las complejas no reales. Por tanto, la permutación que define en S_p es precisamente la permutación $(1, 2)$. Esto es, $(1, 2) \in G$. □

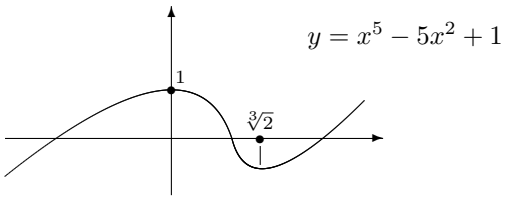
Teorema 13 (Abel-Ruffini)**.** *Para todo $n \geq 5$ existe un polinomio de grado n, $f \in \mathbb{Q}[x]$, que no es resoluble por radicales.*

DEMOSTRACIÓN. Sea $f = x^5 - 5x^2 + 1$. Al reducirlo módulo 2, obtenemos el polinomio $x^5 + x^2 + 1 \in \mathbb{Z}_2[x]$, que no tiene raíces ni es divisible por $x^2 + x + 1$ en $\mathbb{Z}_2[x]$. Luego el reducido es irreducible en $\mathbb{Z}_2[x]$ y el propio f lo es en $\mathbb{Q}[x]$.

Usamos ahora cálculo diferencial elemental para analizar la gráfica de la función $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto f(x)$. Puesto que $f' = 5x^4 - 10x = 5x(x^3 - 2)$, esta tiene tiene exactamente dos puntos críticos, en $x_1 = 0$ y en $x_2 = \sqrt[3]{2}$. Ahora, $f'' = 20x^3 - 10$. Como $f''(0) = -10 < 0$, el punto de la gráfica $(0, f(0)) = (0, 1)$ es un máximo. Como $f''(\sqrt[3]{2}) = 40 - 10 > 0$, el punto de la gráfica

$$(\sqrt[3]{2}, f(\sqrt[3]{2})) = (\sqrt[3]{2}, 2\sqrt[3]{4} - 5\sqrt[3]{4} + 1) = (\sqrt[3]{2}, 1 - 3\sqrt[3]{4})$$

es un mínimo. La gráfica es entonces de la forma



y se sigue fácilmente que f tiene exactamente 3 raíces reales (y, entonces, exactamente dos complejas no reales). Por la proposición anterior,

$$G(x^5 - 5x^2 + 1) = S_5\,,$$

que, sabemos, no es resoluble. Luego el polinomio no es resoluble.

Puesto que $G(x^m(x^5 - 5x^2 + 1)) = G(x^5 - 20x^2 + 2) = S_5$, para todo $m = 0, 1, \ldots$, tenemos un polinomio de grado $m + 5$ en $\mathbb{Q}[x]$ que no es resoluble. □