# Soluciones por radicales

Facultad de Ciencias UNAM

# Introducción

En esta sección (la ultima del curso) demostramos el teorema de Abel-Ruffini. De nuevo, hacemos la siguiente convención:

*Todos los campos tienen característica 0.*

# La resolubilidad de un campo de descomposición solo depende del polinomio

**Lema 1**

Supongamos que $F$ es un campo, que $f(x) \in F[x]$, y que $L_1$ y $L_2$ son campos de descomposición de $f(x)$. Entonces $L_1/F$ es resoluble si y solo si $L_2/F$ es resoluble.

*Demostración.* Antes que nada, recordemos que como $L_1$ y $L_2$ son campos de descomposición de $f(x)$, entonces $L_1 \cong L_2$ y por lo tanto, $\mathrm{Gal}(L_1/F) \cong \mathrm{Gal}(L_2/F)$.

Por otro lado, (de nuevo) como $L_1$ y $L_2$ son campos de descomposición de $f(x)$, entonces $L_1/F$ y $L_2/F$ son extensiones de Galois. Por lo tanto,

$$\begin{aligned} L_1/F \text{ es resoluble} &\iff \mathrm{Gal}(L_1/F) \text{ es resoluble} && \text{(por el teorema de Galois)} \\ &\iff \mathrm{Gal}(L_2/F) \text{ es resoluble} && (\mathrm{Gal}(L_1/F) \cong \mathrm{Gal}(L_2/F)) \\ &\iff L_2/F \text{ es resoluble} && \text{(por el teorema de Galois)} \end{aligned}$$

□

# Polinomios resolubles por radicales

## Definición

Supongamos que $F$ es un campo, que $f(x) \in F[x]$, y que $L$ es un campo de descomposición de $f(x)$ sobre $F$.

- Una raíz $\alpha \in L$ de $f(x)$ es **expresable por radicales sobre** $F$ si $\alpha$ pertenece a una extensión radical de $F$.
- El polinomio $f(x)$ es **resoluble por radicales sobre** $F$ si $L/F$ es una extensión resoluble.

Por el lema anterior, la definición de polinomio resoluble por radicales no depende del campo de descomposición que ocupemos.

Por otro lado, el lector podrá fácilmente verificar que si un polinomio no constante es resoluble por radicales sobre $F$, entonces *todas* sus raíces son expresables por radicales sobre $F$.

En lo que sigue, veremos que para polinomios irreducibles, la relación entre resolubilidad por radicales y la existencia de raíces expresables por radicales es muy interesante.

# Una caracterización de resolubilidad por radicales para polinomios irreducibles

## Proposición 2

Supongamos que $F$ es un campo y que $f(x) \in F[x]$. Si $f(x)$ es irreducible en $F[x]$, entonces $f(x)$ es resoluble por radicales sobre $F$ si y solo si $f(x)$ tiene *alguna* raíz expresable por radicales sobre $F$.

*Demostración.* La implicación "$\Longrightarrow$" es trivial. Conversamente, supongamos que $f(x)$ tiene alguna raíz $\alpha$ expresable por radicales sobre $F$.

*Afirmación.* $F(\alpha)/F$ es resoluble.

Por definición, $\alpha$ es expresable por radicales sobre $F$ si $\alpha$ pertenece a una extensión radical de $F$, digamos $K$. Entonces $F(\alpha) \subset K$ y $K/F$ es radical, lo cual implica que $F(\alpha)/F$ es resoluble.

*Fin de afirmación.*

Por otro lado, recordemos que en el corolario 2.25.6 vimos que la cerradura de Galois de una extensión finita resoluble de característica 0 es resoluble (recuerda que en esta sección estamos asumiendo que todo campo tiene característica 0). Juntando esto con la afirmación anterior, obtenemos que si $M$ es la cerradura de Galois de $F(\alpha)/F$, entonces $M/F$ es resoluble.

Ahora bien, como (i) $M/F$ es normal[1], (ii) $f(x)$ es irreducible en $F[x]$, y (iii) $f(x)$ tiene una raiz en $M$, entonces $f(x)$ se descompone en $M/F$. En particular, $M$ contiene a un campo de descomposición de $f(x)$, digamos $L \subset M$. Como $M/F$ es radical, lo anterior implica que $L/F$ es resoluble o equivalentemente[2], $f(x)$ es resoluble por radicales sobre $F$. □

[1] Recuerda que toda extensión de Galois es normal.

[2] Recuerda que un polinomio es resoluble por radicales sobre $F$ si su campo de descomposición sobre $F$ es resoluble.

# Comentario

En lo que sigue, aplicaremos el material presentado en las secciones anteriores para caracterizar a los polinomios resolubles por radicales en términos de su grupo de Galois. Recordemos que si $f(x) \in F[x]$, entonces el grupo de Galois de $f(x)$ sobre $F$ es $\mathrm{Gal}(L/F)$ donde $L$ es un campo de descomposición de $f(x)$ sobre $F$.

# Un polinomio es resoluble por radicales sobre $F$ si y solo si su grupo de Galois sobre $F$ es resoluble

**Teorema 3**

Supongamos que $F$ es un campo y que $f(x) \in F[x]$. Entonces $f(x)$ es resoluble por radicales sobre $F$ si y solo si su grupo de Galois sobre $F$ es resoluble.

*Demostración.* Supongamos que $L$ es un campo de descomposición de $f(x)$ sobre $F$. Entonces (por definición),

$$f(x) \text{ es resoluble por radicales sobre } F \iff L/F \text{ es resoluble} \tag{1}$$

Por otro lado, como $L$ es un campo de descomposición sobre $F$, entonces $L/F$ es de Galois y por lo tanto el teorema de Galois implica que

$$L/F \text{ es resoluble} \iff \mathrm{Gal}(L/F) \text{ es resoluble} \tag{2}$$

Juntando (1) y (2) obtenemos lo deseado. $\square$

# Los polinomios de grado $\leq 4$ son resolubles por radicales

**Proposición 4**

Supongamos que $F$ es un campo y que $f(x) \in F[x]$. Si $\deg f(x) \leq 4$, entonces $f(x)$ es resoluble por radicales.

*Demostración.* Es consecuencia inmediata de los siguientes resultados:

- Un polinomio es resoluble por radicales sobre $F$ si y solo si su grupo de Galois sobre $F$ es resoluble. (c.f. teorema 3)
- El grupo de Galois de un polinomio es isomorfo a un subgrupo de $S_n$ con $n =$ el numero de raíces del polinomio. (c.f. proposición 2.19.3)
- $S_n$ es resoluble si $n \leq 4$. (c.f. teorema 2.29.5)
- Todo subgrupo de un grupo resoluble es resoluble. (c.f. proposición 2.26.1)

# El caso $\deg f(x) \geq 5$

Es un hecho conocido[3] que el grupo de Galois sobre $\mathbb{Q}$ del polinomio $f(x) = x^5 - 6x + 3$ es isomorfo a $S_5$. Pero $S_5$ no es resoluble y por lo tanto (por el teorema 3, $f(x)$ no es resoluble por radicales. Mas aun, como $f(x)$ es irreducible[4] en $\mathbb{Q}[x]$, entonces (por la proposición 2) *ninguna* raíz de $f(x)$ es expresable por radicales.

Lo anterior implica que las raíces de un polinomio $\in \mathbb{Q}[x]$ no necesariamente son números como (por ejemplo)

$$\sqrt{2}+\sqrt{3}, \quad \sqrt{2+\sqrt{2}}, \quad \sqrt[7]{12+7i}.$$

Es interesante notar que la palabra "raíz" para referirse al elemento $\alpha \in \mathbb{C}$ que satisface $f(\alpha) = 0$ con $f(x) \in \mathbb{Q}[x]$ nace la errónea idea de que las raíces de un polinomio se construyen a partir de sacar *raíces* cuadradas, cubicas, etc.

[3] c.f. Cox, Galois Theory, Sección 6.4.C.

[4] Por el criterio de Eisenstein.

# Comentario

En lo que sigue, demostraremos el famoso teorema de Abel-Ruffini. Intuitivamente, este teorema dice que no existe un análogo de la chicharronera para ecuaciones de grado $\geq 5$. Formalmente, el teorema dice que si $n \geq 5$, entonces el polinomio universal de grado $n$ no es resoluble por radicales y ninguna de sus raíces es expresable por radicales.

Para poder entender porque el enunciado formal coincide con nuestra intuición, hay que

a. precisar a que nos referimos con "un análogo de la chicharronera para ecuaciones de grado $n$" y
b. convencernos de que el polinomio universal de grado $n$ es resoluble por radicales sobre $F(\sigma_1, \ldots, \sigma_n)$ si y solo si existe un análogo de la chicharronera para polinomios de grado $n$.

El lector estará de acuerdo que la formulación precisa de la existencia de "un análogo de la chicharronera para ecuaciones de grado $n$" es:

$\forall F$ campo $\forall f(x) \in F[x]$ (todas las raíces de $f(x)$ son expresables por radicales sobre $F$).

El inciso (b) es el siguiente lema.

# La intuición de Abel-Ruffini

## Lema 5

Supongamos que $n \in \mathbb{Z}_{\geq 2}$. Son equivalentes:

a. $\forall F$ campo $\forall f(x) \in F[x]$ (todas las raíces de $f(x)$ son expresables por radicales sobre $F$)

b. $\forall K$ campo (todas las raíces del polinomio universal $\tilde{f}(x) \in K(\sigma_1, \ldots, \sigma_n)[x]$ son expresables por radicales sobre $K(\sigma_1, \ldots, \sigma_n)$)

*Demostración.* Claramente, (a) implica (b). Para el converso, supongamos (b) y supongamos que $F$ es un campo, que $f(x) \in F[x]$, que $L$ es un campo de descomposición de $f(x)$ sobre $F$ y que

$$f(x) = c(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n), \quad \alpha_1, \ldots, \alpha_n \in L.$$

Mas aun, denotemos por $\phi : F(x_1, \ldots, x_n, x) \to L[x]$ a el homomorfismo que satisface $x_i \mapsto \alpha_i$ y $a \mapsto a$ para toda $a \in F$.

Por otro lado, como las raíces del polinomio universal $\tilde{f}(x) \in F(\sigma_1, \ldots, \sigma_n)[x]$ son $x_1, \ldots, x_n$, entonces (b) implica que el polinomio $x_i \in F(x_1, \ldots, x_n, x)$ es expresable por radicales sobre $F(\sigma_1, \ldots, \sigma_n)$. Esto significa que para cada $i = 1, \ldots, n$, existe $L_i$ tal que $L_i/F(\sigma_1, \ldots, \sigma_n)$ es una extensión radical. Como $\phi$ es un homomorfismo, entonces (por el lema 2.25.5) esto implica que $\phi(L_i)/\phi(F(\sigma_1, \ldots, \sigma_n))$ es una extensión radical.

Por otro lado, como $\sigma_i$ es simétrico y $\alpha_1, \ldots, \alpha_n$ son raíces de un polinomio, entonces el corolario 2.16.5 implica que $\sigma_i(\alpha_1, \ldots, \alpha_n) \in F$. Pero $\sigma_i(\alpha_1, \ldots, \alpha_n) = \phi(\sigma_i)$ y por lo tanto

$$F = F\left(\phi(\sigma_1), \ldots, \phi(\sigma_n)\right) = \phi\left(F(\sigma_1, \ldots, \sigma_n)\right)$$

donde la ultima igualdad es una sencilla verificación.

Por lo tanto, $\phi(L_i)/F = \phi(L_i)/\phi(F(\sigma_1, \ldots, \sigma_n))$ es una extensión radical. Como $\alpha_i = \phi(x_i) \in \phi(L_i)$, esto implica que $\alpha_i$ es expresable por radicales sobre $F$ para toda $i$ y por lo tanto, todas las raíces de $f(x)$ son expresables por radicales sobre $F$. $\square$

# El teorema de Abel-Ruffini

## Teorema 6

Supongamos que $K$ es un campo. Si $n \geq 5$, entonces el polinomio universal $\tilde{f}(x) \in K(\sigma_1, \ldots, \sigma_n)[x]$ no es resoluble por radicales sobre $K(\sigma_1, \ldots, \sigma_n)$.

En particular[5], ninguna raíz de $\tilde{f}(x)$ es expresable por radicales sobre $K(\sigma_1, \ldots, \sigma_n)$. Por lo tanto[6], si $n \geq 5$, entonces existe $F$ campo y $f(x) \in F[x]$ con *alguna* raíz que no es expresable por radicales sobre $F$. En otras palabras, no existe un análogo de la chicharronera para polinomios de grado $\geq 5$.

*Demostración.* En el teorema 3 vimos que un polinomio es resoluble por radicales si y solo si su grupo de Galois es resoluble. Como el grupo de Galois de $\tilde{f}(x)$ sobre $K(\sigma_1, \ldots, \sigma_n)$ es $S_n$ (c.f. teorema 2.20.3), entonces lo anterior implica que $\tilde{f}(x)$ no es resoluble por radicales sobre $K(\sigma_1, \ldots, \sigma_n)$. □

[5] Por la proposición 2 y porque $\tilde{f}(x)$ es es irreducible en $F(\sigma_1, \ldots, \sigma_n)[x]$.

[6] Por el lema anterior.