Tema 12.-. Aplicaciones de la teoría de Galois

12.1. Resolubilidad por radicales

Se trata en este punto de caracterizar las ecuaciones que son resolubles por radicales en términos de su grupo de Galois. Aun cuando el resultado se puede enunciar con toda generalidad, nosotros nos restringiremos al caso de un cuerpo de característica cero, en cuyo caso todos los polinomios irreducibles son separables.

DEFINICIÓN 12.1.1.– Sea $f(X) \in k[X]$. Se dirá que f es resoluble por radicales, sobre k, si para K cuerpo de descomposición de f sobre k existe una extensión $L \supset K$, tal que $L \supset k$ es normal y *radical,* es decir, $L = k(\alpha_1, \ldots, \alpha_n)$, y para cada $i = 1, \ldots, n$, existe $n_i \in \mathbb{N}$ con $\alpha_i^{n_i} \in k(\alpha_1, \ldots, \alpha_{i-1})$.

NOTA 12.1.2.– En la definición anterior no es necesario suponer que $L \supset k$ sea normal. Basta añadir las demás raíces de $\prod_{i=1}^{n} f_i(X)$, donde $f_i(X)$ es el polinomio mínimo de α_i sobre k, y se puede probar que sigue conservando el carácter radical.

NOTA 12.1.3.– Si G_f es el grupo de Galois de f sobre k y $\Omega = \{\alpha_1, \ldots, \alpha_n\}$ es el conjunto de raíces de f, existe un homomorfismo inyectivo de G_f en S_n definido por las restricciones a Ω: si $\sigma \in G_f$, se tiene

$$0 = \sigma(0) = \sigma(f(\alpha_i)) = f(\sigma(\alpha_i)),$$

por tanto, $\sigma(\alpha_i) = \alpha_j$; además, $\sigma_{|\Omega} = id$ si y sólo si $\sigma = id$. Luego siempre podemos suponer que $G_f \subset S_n$.

Vamos a tratar la resolubilidad por radicales empezando por las ecuaciones más sencillas.

LEMA 12.1.4.– (*Extensiones ciclotómicas*) Si $f = X^n - 1 \in k[X]$, entonces G_f es abeliano y, por tanto, resoluble.

Demostración. El conjunto Ω de raíces de f es evidentemente un subgrupo multiplicativo finito de k^*, y por el teorema 11.1.7 es cíclico. A los generadores de este grupo se les llama *raíces primitivas n-ésimas de la unidad.* Si ζ es una tal raíz primitiva, $K = k(\zeta)$ es un cuerpo de descomposición de f. Utilizando los argumentos de la nota precedente, si $\sigma, \tau \in G_f$, sea $\sigma(\zeta) = \zeta^i$, $\tau(\zeta) = \zeta^j$ entonces $\sigma\tau(\zeta) = \zeta^{ij} = \tau\sigma(\zeta)$, y por tanto $\sigma\tau = \tau\sigma$. □

LEMA 12.1.5.– Sea $f = X^n - a \in k[X]$, y $\zeta \in k$ una raíz primitiva n-ésima de la unidad. Entonces G_f es abeliano y, por tanto, resoluble.

Demostración. Si α es una raíz de f, entonces $\alpha, \zeta\alpha, \ldots, \zeta^{n-1}\alpha$ son las raíces de f. Entonces $K = k(\alpha)$ es un cuerpo de descomposición de f sobre k, ya que $\zeta \in k$ por hipótesis. Sean $\sigma, \tau \in G_f$, $\sigma(\alpha) = \zeta^i\alpha$, $\tau(\alpha) = \zeta^j\alpha$ entonces $\sigma\tau(\alpha) = \zeta^{i+j}\alpha = \tau\sigma(\alpha)$, y por tanto $\sigma\tau = \tau\sigma$. □

LEMA 12.1.6.– Sea $f = X^n - a \in k[X]$. Entonces G_f resoluble.

Demostración. Si α es una raíz de f y ζ una raíz primitiva n-ésima de la unidad entonces $\alpha, \zeta\alpha, \ldots, \zeta^{n-1}\alpha$ son las raíces de f. Entonces $K = k(\zeta, \alpha)$ es un cuerpo de descomposición de f sobre k. Se tiene la torre de cuerpos: $k \subset k(\zeta) \subset K$, que son extensiones normales. Por el teorema fundamental de la Teoría de Galois, se tiene que $1 \lhd G(K|k(\zeta)) \lhd G_f$ es una torre de subgrupos normales y, además, los cocientes son: $G(K|k(\zeta))$, que es abeliano por el lema 12.1.5, y

$$G_f/G(K|k(\zeta)) \cong G(k(\zeta)|k),$$

que es abeliano por el lema 12.1.4. □

Teorema 12.1.7.– *(Galois, 1829)* Si $f \in k[X]$ es resoluble por radicales entonces G_f es resoluble.

Demostración. Sea K el cuerpo de descomposición de f sobre k y $L \supset K$, con $L \supset k$ normal y radical, $L = k(\alpha_1, \ldots, \alpha_n)$, con $\alpha_i^{n_i} \in k(\alpha_1, \ldots, \alpha_{i-1})$. Sea $N = \text{mcm}(n_{i\{i=1,\ldots,n\}})$, y ζ una raíz primitiva $N-$ésima de la unidad. Se tiene la torre de subcuerpos:

$$k = k_0 \subset k_1 = k_0(\zeta) \subset k_2 = k_1(\alpha_1) \subset k_3 = k_2(\alpha_2) \subset \cdots \subset k_{n+1} = L(\zeta).$$

Aplicando el teorema fundamental de la teoría de Galois a la extensión normal $k_{n+1}|k$, se tiene la torre de subgrupos correspondiente:

$$G(k_{n+1}|k) \rhd G(k_{n+1}|k_1) \supset G(k_{n+1}|k_2) \supset \cdots \supset \{1\}$$

ya que $k_1 \supset k_0$ es normal y

$$G(k_{n+1}|k_0)/G(k_{n+1}|k_1) \cong G(k_1|k_0)$$

que es abeliano por el lema 12.1.4. El siguiente cociente es

$$G(k_{n+1}|k_1)/G(k_{n+1}|k_2) \cong G(k_2|k_1)$$

ya que $k_2 \supset k_1$ es normal puesto que ζ^{N/n_1} es una raíz primitiva n_1-ésima de la unidad. Repitiendo el razonamiento se obtiene que $G(k_{n+1}|k)$ es resoluble. Considerando ahora la torre

$$k_{n+1} \supset K \supset k,$$

se tiene que $G(K|k)$ es cociente de un grupo resoluble, y por tanto resoluble. □

El recíproco también es cierto, pero la demostración requiere conocer el teorema de estructura de los grupos abelianos finitamente generados, que se escapa del ámbito de nuestra materia.

Corolario 12.1.8.– El polinomio $X^5 - 4X + 2 \in \mathbb{Q}[X]$ no es resoluble por radicales sobre $\mathbb{Q}$.

Demostración. El polinomio es irreducible por el criterio de Eisenstein para $p = 2$. Como $f(-2) = -22$, $f(-1) = 5$, $f(0) = 2$, $f(1) = -1$, $f(2) = 26$, por el teorema de Bolzano-Weierstrass, existen raíces reales $t_1 \in (-2, -1)$, $t_2 \in (0, 1)$, $t_3 \in (1, 2)$. Observando las raíces de la derivada $f'(X) = 5X^4 - 4$, por el teorema de Rolle, se tiene que f tiene sólo las tres raíces reales citadas. Por tanto f tiene también dos raíces complejas no reales: z y $\overline{z}$. Está claro que el automorfismo conjugación de $\mathbb{C}$, restringido al cuerpo de descomposición de f, $K = \mathbb{Q}(t_1, t_2, t_3, z, \overline{z})$ define un elemento $\sigma \in G_f$ que, a su vez, corresponde a la trasposición $(45) \in S_5$. Por otra parte $[\mathbb{Q}(t_1) : \mathbb{Q}] = 5$, por lo que $|G_f| = [K : \mathbb{Q}]$ es divisible por 5. El teorema de Cauchy para grupos (cfr. Xambó-Delgado-Fuertes 'Introducción al Álgebra', 2.12, p.147) afirma que, en ese caso, existe en G_f un elemento τ de orden 5. Por el ejercicio 63 de la relación de problemas, G_f es igual a S_5. Como probamos en el tema 4, S_5 no es resoluble, y por el teorema anterior, f no es resoluble por radicales. □

12.2. Construcciones con regla y compás

En esta sección trabajaremos con el plano euclídeo $\mathbb{R}^2$ que lo identificaremos, cuando sea preciso con el plano complejo $\mathbb{C}$. Daremos la definición natural de constructibilidad con regla y compás que sigue.

Definición 12.2.1.– Un 'punto $P \in \mathbb{R}^2$ es constructible con regla y compás si existe una sucesión finita de puntos $P_0, P_1, \ldots, P_n$ con $P_0 = (0, 0)$, $P_1 = (1, 0)$, $P_n = P$ y tal que cada P_i, $i = 2, \ldots, n$ se obtiene a partir de los anteriores $P_0, \ldots, P_{i-1}$:

- como intersección de dos rectas, definidas por dos de los puntos anteriores.
- como intersección de una recta con una circunferencia, con centro en uno de los puntos anteriores y de radio el segmento que une dos de los puntos anteriores.
- como intersección de dos circunferencias como la del apartado anterior.

Ejemplo 12.2.2.– Se pueden construir los siguientes puntos:

- El punto $(n, 0)$ para cada $n \in \mathbb{Z}$.
- El punto $(0, m)$ para cada $m \in \mathbb{Z}$.
- El punto (n, m) para cada $n, m \in \mathbb{Z}$, trazando paralelas por un punto a una recta.
- El punto $(\frac{n}{m}, 0)$ para cada $n, m \in \mathbb{Z}$, $m \neq 0$, usando el teorema de Thales.
- El punto (q, q'), para cada $q, q' \in \mathbb{Q}$.
- El punto $(\sqrt{q}, 0)$, para cada $q \in \mathbb{Q}$, usando el teorema de las alturas

Teorema 12.2.3.– Un punto P es constructible con regla y compás si y sólo si existe una torre de cuerpos:

$$\mathbb{Q} = k_1 \subset k_2 \subset \cdots \subset k_n = \mathbb{Q}(z)$$

donde $z \in \mathbb{C}$ es el afijo de P y $[k_{i+1} : k_i] = 1$ o 2

Demostración. Supongamos que P es constructible con regla y compás. Sea k_i el cuerpo que contiene a $\mathbb{Q}$ y a las coordenadas de los puntos $P_0, P_1, \ldots, P_i$, para $i = 1, \ldots, n$. Si P_{i+1} se obtiene como intersección de rectas, entonces sus coordenadas están en k_i, luego $k_{i+1} = k_i$. Si P_{i+1} se obtiene como intersección de una recta con una circunferencia, habrá que resolver una ecuación de segundo grado, luego $[k_{i+1} : k_i] = 1$ o 2. Lo mismo sucede para el caso del corte de dos circunferencias.

Recíprocamente, si $[k_{i+1} : k_i] = 2$, se tiene que $k_{i+1} = k_i(\sqrt{d})$ con $d \in k_i$. Por lo visto en los ejemplos anteriores, los puntos de k_{i+1} se pueden construir con regla y compás a partir de los de k_i. □

Corolario 12.2.4.– Si P es constructible con regla y compás entonces $[\mathbb{Q}(z) : \mathbb{Q}] = 2^n$, para $n \in \mathbb{N}$.

Corolario 12.2.5.– (*Problema deliano*). No se puede duplicar un cubo con regla y compás.

Demostración. Se trata de construir la arista de un cubo de volumen 2, es decir de construir el punto $P = (\sqrt[3]{2}, 0)$, que no es constructible con regla y compás porque $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. □

Corolario 12.2.6.– No se puede cuadrar un círculo con regla y compás.

Demostración. Se trata de construir un cuadrado cuya área sea la del círculo unidad, es decir π. Para ello hay que construir el punto $P = (\sqrt{\pi}, 0)$, que no es constructible con regla y compás porque $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}]$ no es finito, por ser π un número trascendente (teorema de Lindemann (1882)). □

Corolario 12.2.7.– No se puede trisecar un ángulo con regla y compás.

Demostración. Se trata de dividir un ángulo en tres partes iguales. Veremos que el ángulo de 60 grados no se puede trisecar. Por trigonometría sabemos que

$$\cos(3x) = 4\cos^3(x) - 3\cos(x).$$

Por tanto, si $y = \cos(20)$, debe ser $y^3 - 3y - 1 = 0$. Como este polinomio es irreducible, se tiene que $[\mathbb{Q}(y) : \mathbb{Q}] = 3$, por lo que y no es constructible con regla y compás. □

Teorema 12.2.8.– Un punto P es constructible con regla y compás si existe una extensión normal $K \supset \mathbb{Q}$ con $[K : \mathbb{Q}] = 2^n$,para cierto $n \in \mathbb{N}$, y $z \in K$.

Demostración. Sea $G = G(K|\mathbb{Q})$. Como $|G| = 2^n$, invocando el Teorema de Cauchy para grupos, ya citado, existen subgrupos G_i de G, $1 \leq i \leq n$, tales que $1 \subset G_1 \subset \cdots G_n = G$ con $|G_i| = 2^i$. Aplicando el teorema fundamental de la teoría de Galois se tiene la torre de cuerpos del enunciado del anterior teorema. □