Algebra III

Tema 11: Extensiones radicales. Resolubilidad de ecuaciones por radicales. Gran teorema de Galois

Curso 2016-2017

1. Extensiones radicales

Definición 1.1. Una extensión finita E/K se llama *cíclica* si es de Galois y su grupo de Galois es cíclico

Cuando K sea un cuerpo con $car(K) = 0$ la siguiente definición proporcionará un concepto equivalente para las extensiones cíclicas en las condiciones oportunas.

Definición 1.2. Sea K con $car(K) = 0$. Una extensión E/K se dice que es radical si $E = K(\alpha)$ donde α es raíz de $X^n - a \in K[X]$, $n \in \mathbb{Z}^+$, es decir, si $E = K(\alpha)$ con $\alpha^n = a$, o si se quiere $E = K(\sqrt[n]{a})$.

Nótese que $X^n - a$ es separable (independientemente de que sea irreducible) pues si α es una raíz en $\bar{K} \subseteq \mathbb{C}$ las restantes raíces son $\xi^i\alpha$, $i = 1, \dots, n-1$, donde $\xi \in \mathbb{C}$ es una raíz n-ésima primitiva de 1.

Teorema 1.3 (Lagrange)**.** *Sea K un cuerpo con $car(K) = 0$ y conteniendo una raíz n-ésima primitiva de la unidad en K.*

1. *Sea E/K una extensión cíclica de grado n. Entonces existe $\alpha \in E$ tal que $E = K(\alpha)$ y $\mathrm{Irr}(\alpha, K) = X^n - a$ para algún $a \in K$ (y por tanto E/K es radical).*
2. *Reciprocamente, sea $a \in K$ y sea α una raíz de $X^n - a \in K[X]$. Entonces $K(\alpha)/K$ es cíclica de grado d, d divisor de n y $\alpha^d \in K$.*

Demostración.

1) Por la hipótesis sabemos que E/K es simple, $E = K(u)$, que $\mathrm{Gal}(E/K) = \langle\sigma\rangle$ es cíclico de orden n y que $\xi \in K$ es una raíz n-ésima primitiva de la unidad. Definimos la *resolvente de Lagrange* $\beta = \beta(u, \xi) \in E$ como

$$\beta = u + \xi\sigma(u) + \xi^2\sigma^2(u) + \cdots + \xi^{n-1}\sigma^{n-1}(u)$$

Por la independencia lineal de los homomorfismos $\{\sigma^i\}$ $i = 0, \dots, n-1$ tenemos que $\beta \neq 0$.
Aplicando el automorfismo σ obtenemos

$$\begin{aligned}\sigma(\beta) &= \sigma(u) + \xi\sigma^2(u) + \xi^2\sigma^3(u) + \cdots + \xi^{n-1}\sigma^n(u)\\ &= \xi^{-1}(u + \xi\sigma(u) + \xi^2\sigma^2(u) + \cdots + \xi^{n-1}\sigma^{n-1}(u))\\ &= \xi^{-1}\beta\end{aligned}$$

Por inducción sobre i, $\sigma^i(\beta) = \xi^{-i}\beta$. Luego los elementos $\xi^{-i}\beta$ son n conjugados distintos de β, por lo que $[K(\beta) : K] \geq n$. Como $K(\beta) \subseteq E$, queda que $E = K(\beta)$. Además, $\sigma(\beta^n) = \sigma(\beta)^n = (\xi^{-1}\beta)^n = \beta^n$. Luego $a = \beta^n$ es fijo bajo σ y todas sus potencias, por lo que $a \in K$. Así β es raíz de $X^n - \beta^n = X^n - a \in K[X]$ que atendiendo al grado será justo el $\mathrm{Irr}(\beta, K)$.

Nota.- Aunque $u \in E$, $u \notin K$, no sea un elemento primitivo de la extensión E/K podemos considerar otras *resolventes*

$$\beta_i = \beta_i^u = \beta_i(u, \xi) = u + \xi^i\sigma(u) + \xi^{2i}\sigma^2(u) + \cdots + \xi^{(n-1)i}\sigma^{n-1}(u), \quad i = 1, \cdots, n-1,$$

(donde β_1^u es justo la β anterior). Siempre que $\beta_i \neq 0$, estos elementos verifican, con el mismo razonamiento anterior (nótese que $\sigma^k(\beta_i) = (\xi^i)^{-k}\beta_i$, $k = 1, \cdots, n-1$), que son elementos primitivos de la extensión, i.e., $E = K(\beta_i)$, y que $\beta_i^n \in K$ de modo que cada β_i es raíz de $X^n - \beta_i^n \in K[x]$. Esta observación será de utilidad para expresar por radicales (cuando

esto sea posible) las raíces $\alpha_1, \cdots, \alpha_n$ de un polinomio $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in K[x]$. Usaremos para tal fin la resolvente (trivial) $\beta_0^{\alpha_1} = \alpha_1 + \sigma(\alpha_1) + \cdots + \sigma^{n-1}(\alpha_1) \in K$ junto a las resolventes necesarias $\beta_i = \beta_i^{\alpha_1} = \beta_i(\alpha_1, \xi)$ que sabemos que verifican $\beta_i^n \in K$.

2) Si E/K es radical $\Rightarrow E = K(\alpha)$ con α raíz $X^n - a \in K[X]$, $n \in \mathbb{Z}^+$, y como K contiene a ξ raíz n-ésima primitiva de la unidad y las raíces de $X^n - a$ son $\xi^i \alpha$, $i = 0, 1, \ldots, n-1$ se tiene que $E = K(\alpha)$ es el cuerpo de descomposición de $X^n - a$ $\Rightarrow E/K$ es normal y separable $\Rightarrow E/K$ es de Galois con $G = Gal(E/K) = \{\sigma : K(\alpha)/K \to K(\alpha)/K\}$. Cada $\sigma \in Gal(E/K)$ está determinado entonces por la imagen de α que ha de ser otra raíz de $\mathrm{Irr}(\alpha, K)$ y por tanto raíz de $X^n - a \Rightarrow \sigma(\alpha) = \xi^i \alpha$, para algún $i = 0, 1, \ldots, n-1$. Luego $\sigma(\alpha) = \xi_\sigma \alpha$, siendo ξ_σ una raíz de la unidad (no necesariamente primitiva). La aplicación $\sigma \mapsto \xi_\sigma$ es obviamente un monomorfismo de G en el grupo de las raíces n-ésimas de la unidad y como éste es cíclico de orden n, G es cíclico de orden d divisor de n. Sea $G = \langle \sigma \rangle$. Entonces ξ_σ es una raíz d-ésima primitiva de la unidad, y $\sigma(\alpha^d) = (\xi_\sigma \alpha)^d = \alpha^d$. Luego $\alpha^d \in K$ ya que es fijo bajo G y el teorema está demostrado.

□

2. Resolubilidad de ecuaciones por radicales

Definición 2.1 (torre radical)**.** Sea K con $car(K) = 0$. Una torre radical para una extensión E/K es una torre de cuerpos

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_{i-1} \subseteq K_i \subseteq \cdots \subseteq K_r = E$$

donde, para cada $i = 1, \ldots, r$, la extensión Ki/K_{i-1} es radical, es decir, $K_i = K_{i-1}(\alpha_i)$ con $\alpha_i \in K_i$ tal que $\alpha_i^{n_i} = a_i \in K_{i-1}$ para ciertos enteros positivos n_i.

Notemos que si E/K tiene una torre radical entonces $E = K(\alpha_1, \alpha_2, \ldots, \alpha_r)$ y por tanto E/K es finita (finitamente generada por elementos algebraicos) y todo elemento de E será una expresión algebraica de radicales con radicandos expresiones algebraicas de radicales con radicandos ... elementos de K.

Teorema 2.2.

1. *Si E/F y F/K tienen torres radicales, E/K tiene una torre radical.*
2. *Sean E y F cuerpos intermedios de una extensión L/K. Si E/K y F/K tienen torres radicales, EF/K tiene una torre radical.*
3. *Si E/K tiene una torre radical y $E'/K \overset{\tau}{\cong} E/K$, entonces E'/K tiene una torre radical.*

Demostración.

1. Es clara pues la concatenación de las dos torres radicales existentes por hipótesis proporciona una torre radical para la extensión E/K.

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_{i-1} \subseteq K_i \subseteq \cdots \subseteq K_r = F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_{j-1} \subseteq F_j \subseteq \cdots \subseteq F_s = E$$

2. Dada la torre de E/K

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_{i-1} \subseteq K_i \subseteq \cdots \subseteq K_r = E$$

   la componemos con F y obtenemos una torre radical de EF/F

$$FK = F = F_0 \subseteq FK_1 \subseteq \cdots \subseteq FK_{i-1} \subseteq FK_i \subseteq \cdots \subseteq FK_r = EF$$

   pues $FK_i = FK_{i-1}(\alpha_i)$ con $\alpha_i^{n_i} \in K_{i-1} \subseteq FK_{i-1}$. Entonces como EF/F y F/K tienen torres radicales, por 1) se tiene que EF/K tiene una torre radical.

3. Si $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_{i-1} \subseteq K_i \subseteq \cdots \subseteq K_r = E$ es una torre radical de se cumple $K_i = K_{i-1}(\alpha_i)$ con $\alpha_i^{n_i} \in K_{i-1}$ y tomando $K_i' = \tau(K_i)$ se tiene claramente que $K = K_0' \subseteq K_1' \subseteq \cdots \subseteq K_{i-1}' \subseteq K_i' \subseteq \cdots \subseteq K_r' = E'$ es una torre radical para E'/K.

□

Teorema 2.3. *Sea E/K finita, $[E:K]=n$, y sean $\sigma_1,\sigma_2,\dots,\sigma_r$ con $r\le n$ los distintos encajes de E en $\bar{K}$, $\sigma_i : E/K \hookrightarrow \bar{K}/K$. La clausura normal de E/K es la extensión N/K donde $N=E\sigma_2(E)\cdots\sigma_r(E)$ es el compuesto de todos los cuerpos conjugados de E sobre K.*

Demostración. La extensión N/K es finita al serlo todas las $\sigma_i(E)/K$, $i=1,\dots,r$. Además, para cualquier encaje $\tau : N/K \longrightarrow \bar{K}/K$ ($\bar{K}=\bar{E}=\bar{N}$), la composición de la restricción de τ a $\sigma_i(E)$ con σ_i es necesariamente uno de los encajes σ_j, $j=1,\dots,r$, así que $\tau(N)=\tau(E\sigma_2(E)\cdots\sigma_r(E))=\tau(E)\tau(\sigma_2(E))\cdots\tau(\sigma_r(E))=E\sigma_2(E)\cdots\sigma_r(E)=N$ pues la composición con τ lo único que hace es una permutación de los σ_i, $i=1,\dots,r$, y por tanto N/K es normal con $K\subseteq E\subseteq N$. Además, si F/K es normal con $K\subseteq E\subseteq F\subseteq N$ entonces F contiene a cada uno de los subcuerpos $\sigma_i(E)$ y por tanto $N\subseteq F$ asi que $F=N$ (nótese que cada encaje $\sigma_i : E\longrightarrow \bar{K}=\bar{E}=\bar{N}=\bar{F}$ sobre K se extiende a un encaje $\sigma_i' : F\longrightarrow \bar{K}$ que verifica $\sigma_i'(F)=F \Rightarrow \sigma_i(E)\subseteq\sigma_i'(F)=F$) □

Corolario 2.4. *Si E/K tiene una torre radical, entonces su clausura normal N/K también tiene una torre radical.*

Demostración. Es consecuencia del teorema 2.3 y los apartados 2 y 3 del teorema 2.2. □

Definición 2.5 (polinomio resoluble por radicales)**.** Sea K con $car(K)=0$. Un polinomio $f\in K[X]$ se dice que es resoluble por radicales sobre K (o que la ecuación $f(X)=0$ es resoluble por radicales sobre K) si existe una torre radical

$$K=K_0\subseteq K_1\subseteq\cdots\subseteq K_{i-1}\subseteq K_i\subseteq\cdots\subseteq K_r$$

tal que f descompone completamente en K_r (es decir, un cuerpo de descomposición de f está contenido en K_r).

3. Gran teorema de Galois

Teorema 3.1 (Gran teorema de Galois)**.** *Sea K con $car(K)=0$ y sea $f\in K[X]$ no constante. Entonces la ecuación $f(X)=0$ es resoluble por radicales sobre K si, y sólo si, el grupo de galois* $\mathrm{Gal}(f/K)$ *es un grupo soluble.*

Demostración.
⇒) Supongamos $f(X)=0$ resoluble por radicales sobre K. Entonces existe una torre radical

$$K=K_0\subseteq K_1\subseteq\cdots\subseteq K_{i-1}\subseteq K_i\subseteq\cdots\subseteq K_r=F$$

de forma que, si E es el cuerpo de descomposición de f sobre K, se tiene $E\subseteq F$. Tomamos una clausura algebraica $\bar{K}$ de K que contenga a F (por ejemplo una clausura algebraica de F) así que tenemos la situación $K\subseteq E\subseteq F\subseteq\bar{K}$. Podemos suponer que F/K es normal (y por tanto de Galois al ser $car(K)=0$) pues, en otro caso, la clausura normal N de F/K tomada dentro de $\bar{K}$ estaría, según el corolario anterior, en las mismas condiciones, es decir, tendríamos $K\subseteq E\subseteq N\subseteq\bar{K}$ donde N/K es una extensión finita de Galois con una torre radical. Supongamos entonces que tenemos una torre radical

$$K=K_0\subseteq K_1\subseteq\cdots\subseteq K_{i-1}\subseteq K_i\subseteq\cdots\subseteq K_r=F$$

donde F/K es de Galois, $c.d.d.(f)=E\subseteq F$ y $K_i=K_{i-1}(\alpha_i)$ con $\alpha_i\in K_i$ tal que $\alpha_i^{n_i}=a_i\in K_{i-1}$ para ciertos enteros positivos n_i. Sea $n=\prod_{i=1}^r n_i$ y sea $\xi\in\bar{K}$ una raíz primitiva n-ésima de la unidad. Entonces, poniendo $F_i=K_i(\xi)$, $i=0,1,\dots,r$, se tiene una torre

$$K=K_0\subseteq F_0\subseteq F_1\subseteq\cdots\subseteq F_{i-1}\subseteq F_i\subseteq\cdots\subseteq F_r=F(\xi)$$

que es radical pues $F_i=K_i(\xi)=K_{i-1}(\alpha_i)(\xi)=K_{i-1}(\xi)(\alpha_i)=F_{i-1}(\alpha_i)$ con $\alpha_i^{n_i}\in K_i\subseteq K_i(\xi)=F_i$ para todo $i=1,\dots,r$, además $F_0=K(\xi)$ con $\xi^n=1\in K$.

Notemos además que cada extensión F_i/F_{i-1}, $i=1,\dots,r$, es abeliana. En efecto, como $\xi^{n/n_i}\in F_0$ es una raíz primitiva n_i-ésima de la unidad, $i=1,\dots,r$, se tiene que en F_{i-1} hay una raíz n_i-ésima primitiva de la unidad y como F_i/F_{i-1} es radical, aplicando el teorema de Lagrange deducimos que F_i/F_{i-1}, $i=1,\dots,r$, es una extensión cíclica y por tanto abeliana. Pero además también es abeliana la extensión $F_0=K(\xi)/K$ pues es una extensión ciclotómica.

Además, la extensión $F(\xi)/K$ es una extensión finita de Galois ya que, al ser F/K normal, F es el c.d.d. de $f\in K[X]$ y entonces $F(\xi)=c.d.d.(f(X)(X^n-1))$ así que $F(\xi)/K$ es normal y por tanto de Galois. Usamos ahora la conexión de Galois para obtener la siguiente serie de G:

$$G=\mathrm{Gal}(F(\xi)/K)\trianglerighteq\mathrm{Gal}(F(\xi)/F_0)\trianglerighteq\mathrm{Gal}(F(\xi)/F_1)\trianglerighteq\cdots\trianglerighteq\mathrm{Gal}(F(\xi)/F_r)=1$$

que es una serie normal pues cada F_i/F_{i-1} es normal (es de Galois) y también lo es F_0/K. Además, si analizamos los factores de la serie

$$\frac{\mathrm{Gal}(F(\xi)/F_{i-1})}{\mathrm{Gal}(F(\xi)/F_i)} \cong \mathrm{Gal}(F_i/F_{i-1}) \qquad \text{y} \qquad \frac{\mathrm{Gal}(F(\xi)/K)}{\mathrm{Gal}(F(\xi)/F_0)} \cong \mathrm{Gal}(F_0/K) = \mathrm{Gal}(K(\xi)/K)$$

son abelianos. Así $\mathrm{Gal}(F(\xi)/K)$ tiene una serie normal con factores abelianos y por tanto es un grupo soluble y puesto que tenemos la torre $K \subseteq E \subseteq F(\xi)$ deducimos que

$$\mathrm{Gal}(f/K) \cong \mathrm{Gal}(E/K) \cong \frac{\mathrm{Gal}(F(\xi)/K))}{\mathrm{Gal}(F(\xi)/E)} \cong \frac{G}{\mathrm{Gal}(F(\xi)/E)}$$

y por tanto $\mathrm{Gal}(f/K)$ es soluble por ser isomorfo a un cociente de un grupo soluble.

$\Leftarrow$) Supongamos ahora que $G = \mathrm{Gal}(f/K)$ es soluble. Buscamos una torre radical que empiece en K y cuyo último eslabón contenga un c.d.d. E del polinomio $f \in K[X]$. Supongamos que $|G| = [E:K] = n$ (que $|G| = [E:K]$ es consecuencia de que E/K es de Galois) y sea ξ una raíz n-ésima primitiva de la unidad. Considerando la extensión $K(\xi) \supseteq K$ sabemos que $\mathrm{Gal}(f/K(\xi))$ es un subgrupo de $\mathrm{Gal}(f/K) \cong \mathrm{Gal}(E/K)$ y como éste es soluble $\mathrm{Gal}(f/K(\xi))$ también será soluble. Existirá entonces una serie de composición suya

$$\mathrm{Gal}(f/K(\xi)) = G_1 \rhd G_2 \rhd \cdots \rhd G_{r-1} \rhd G_r = 1$$

con factores $\dfrac{G_i}{G_{i+1}}$ cíclicos de orden primo. Ahora, si F es el c.d.d. de f sobre $K(\xi)$, tenemos que $\mathrm{Gal}(f/K(\xi)) \cong \mathrm{Gal}(F/K(\xi))$ y por la conexión de Galois la serie anterior corresponde a la torre de cuerpos

$$K(\xi) = F^{G_1} \subset F^{G_2} \subset \cdots \subset F^{G_{r-1}} \subset F^{G_r} = F$$

y, por el teorema fundamental,

$$\mathrm{Gal}(F^{G_{i+1}}/F^{G_i}) \cong \frac{\mathrm{Gal}(F/F^{G_i})}{\mathrm{Gal}(F/F^{G_{i+1}})} = \frac{G_i}{G_{i+1}}$$

que son cíclicos de orden primo p_i, $i = 1, \ldots, r-1$, y además $p_i \mid n \ \forall i$ (pues $p_i = [G_i : G_{i+1}] = [F^{G_{i+1}} : F^{G_i}] \mid [F : K(\xi)]$ que a su vez divide a $[E:K] = n$).

Entonces $F^{G_{i+1}}/F^{G_i}$ es una extensión cíclica de grado p_i y en F^{G_i} hay una raíz p_i-ésima primitiva de la unidad (porque como $\xi \in K(\xi) \subset F^{G_i}$ y $p_i \mid n$ entonces ξ^{n/p_i} que es una raíz p_i-ésima primitiva de la unidad también pertenece a F^{G_i}). Consecuentemente, por el teorema de Lagrange se tiene que $F^{G_{i+1}}/F^{G_i}$ es una extensión radical $\forall i = 1, \ldots, r-1$. Por tanto, puesto que la extensión $K(\xi)/K$ también es radical (ξ es raíz de $X^n - 1 \in K[X]$) a partir de la torre anterior obtenemos la torre

$$K \subset K(\xi) = F^{G_1} \subset F^{G_2} \subset \cdots \subset F^{G_{r-1}} \subset F^{G_r} = F$$

que es una torre radical para F/K con $E \subset F$ lo que asegura que $f(X) = 0$ es resoluble por radicales sobre K. □

Corolario 3.2. *Sea K con $car(K) = 0$ y consideramos el polinomio ciclotómico $\Phi_n \in K[X]$. Entonces la ecuación $\Phi_n(X) = 0$ es resoluble por radicales sobre K.*

Demostración. Sabemos que $\mathrm{Gal}(K(\xi)/K)$ es un grupo abeliano y por tanto soluble. Por el teorema resulta que $\Phi_n(X) = 0$ es resoluble por radicales sobre K. □

Teorema 3.3. *Sea K con $car(K) = 0$ y sea $f \in K[X]$ no constante con $gr(f) \leq 4$. Entonces la ecuación $f(X) = 0$ es resoluble por radicales sobre K.*

Demostración. Sabemos que $\mathrm{Gal}(f/K)$ es un subgrupo de S_n, $n \leq 4$, y como cualquiera de éstos es soluble $\mathrm{Gal}(f/K)$ será soluble y consecuentemente $f(X) = 0$ resoluble por radicales. □

Nota.- Para $n \geq 5$ hay ecuaciones $f(X) = 0$ con $gr(f) \geq 5$, que no son resolubles por radicales. Por ejemplo, si $gr(f) = 5$ y $\mathrm{Gal}(f/K) = S_5$, que sabemos que no es soluble, se tendrá que dicha ecuación no será resoluble por radicales sobre K (por ejemplo, $\mathrm{Gal}(X^5 - 6X + 3/\mathbb{Q}) = S_5$ y por tanto $X^5 - 6X + 3 = 0$ no se puede resolver por radicales sobre $\mathbb{Q}$).