Álgebra III - 2do C. 2020 - Clase 17 - 3/11/2020

Lema 12.3.4 (Resolubilidad y raíces de la unidad)
Sea E/K Galois finita y sea ω raíz de la unidad. Entonces

1. $\mathrm{Gal}(E/K)$ *resoluble* $\iff$ $\mathrm{Gal}(E(\omega)/K)$ *resoluble*
2. $\mathrm{Gal}(E/K)$ *resoluble* $\iff$ $\mathrm{Gal}(E(\omega)/K(\omega))$ *resoluble.*

Prueba.–
Notar que $E(\omega)/K$ es Galois pues E/K y $K(\omega)/K$ lo son,
y esto implica que $E(\omega)/K(\omega)$ también.

(1) E/K Galois $\Rightarrow$ $\mathrm{Gal}(E(\omega)/E) \lhd \mathrm{Gal}(E(\omega)/K)$
y $\mathrm{Gal}(E/K) \simeq \mathrm{Gal}(E(\omega)/K) \,/\, \mathrm{Gal}(E(\omega)/E)$.
Pero $\mathrm{Gal}(E(\omega)/E)$ es resoluble por ser abeliana. Así

$\mathrm{Gal}(E/K)$ resoluble $\iff$ $\mathrm{Gal}(E(\omega)/K)$ resoluble.

(2) $K(\omega)/K$ Galois $\Rightarrow$ $\mathrm{Gal}(E(\omega)/K(\omega)) \lhd \mathrm{Gal}(E(\omega)/K)$
y $\mathrm{Gal}(K(\omega)/K) \simeq \mathrm{Gal}(E(\omega)/K) \,/\, \mathrm{Gal}(E(\omega)/K(\omega))$.
Pero $\mathrm{Gal}(K(\omega)/K)$ es resoluble por ser abeliana. Así

$\mathrm{Gal}(E(\omega)/K)$ resoluble $\iff$ $\mathrm{Gal}(E(\omega)/K(\omega))$ resoluble.

■

Proposición 12.3.5 (Galois radical implica grupo resoluble)
Sea E/K Galois y radical con pisos primos $E_0 \subset \cdots \subset E_n$, donde $E_i = E_{i-1}(\alpha_i)$ con $\alpha_i^{p_i} \in E_{i-1}$, y supongamos que K contiene raíces primitivas de la unidad de orden p_i, $1 \leq i \leq n$.
Entonces $\mathrm{Gal}(E/K)$ es resoluble.

Prueba.–
Por el teorema 12.1.2, E_i/E_{i-1} es Galois cíclica con $|\mathrm{Gal}(E_i/E_{i-1})| \,|\, p_i$.
Pero $E_i \neq E_{i-1}$ y por lo tanto $|\mathrm{Gal}(E_i/E_{i-1})| = p_i$.
Así, $\mathrm{Gal}(E/E_i) \lhd \mathrm{Gal}(E/E_{i-1})$ y además
$\mathrm{Gal}(E_i/E_{i-1}) \simeq \mathrm{Gal}(E/E_{i-1}) \,/\, \mathrm{Gal}(E/E_i)$.

O sea

$$\{\mathrm{id}\} = \mathrm{Gal}(E/E) \lhd \mathrm{Gal}(E/E_{n-1}) \lhd \cdots \lhd \mathrm{Gal}(E/E_1) \lhd \mathrm{Gal}(E/E_0) = \mathrm{Gal}(E/K)$$

y

$$\mathrm{Gal}(E/E_{i-1}) \,/\, \mathrm{Gal}(E/E_i) \simeq \mathrm{Gal}(E_i/E_{i-1}) \simeq \mathbb{Z}/p_i\mathbb{Z}.$$

Por lo tanto $\mathrm{Gal}(E/K)$ es resoluble.

■

Proposición 12.3.6 (Grupo resoluble implica radical)
Sea E/K Galois finita con $\mathrm{Gal}(E/K)$ resoluble con serie de descomposición $G_n \lhd \cdots \lhd G_0$ con cocientes primos $p_1, \ldots, p_n$, y supongamos que K contiene raíces primitivas de la unidad de orden p_i, $1 \leq i \leq n$.
Entonces E/K es radical.

Prueba.–
Tenemos

$$\{\mathrm{id}\} = \mathrm{Gal}(E/E) =: G_n \lhd G_{n-1} \lhd \cdots \lhd G_1 \lhd G_0 := \mathrm{Gal}(E/K)$$

con G_{i-1}/G_i cíclico de orden p_i primo.
Sea $E_i := E^{G_i}$. Entonces E/E_i es Galois con $\mathrm{Gal}(E/E_i) = G_i$, y luego

$$K = E_0 \subset E_1 \subset \cdots \subset E_{n-1} \subset E_n = E,$$

con E_i/E_{i-1} Galois pues $\mathrm{Gal}(E/E_i) \lhd \mathrm{Gal}(E/E_{i-1})$,
y además

$$\mathrm{Gal}(E_i/E_{i-1}) \simeq \mathrm{Gal}(E/E_{i-1})/\mathrm{Gal}(E/E_i) \simeq G_{i-1}/G_i$$

es cíclico de orden p_i primo, y E_{i-1} contiene una raíz primitiva de orden p_i de 1. Por el teorema 12.1.2, $E_i = E_{i-1}(\alpha_i)$ con $\alpha_i^{p_i} \in E_{i-1}$.

■

Juntemos todo ahora (recordemos que estamos con $\mathrm{car}(K) = 0$ sino hay sutilezas).

Teorema 12.3.7 *(Resolubilidad de ecuaciones)*
Sea $f \in K[X]$. Entonces

$$f \text{ es resoluble por radicales} \iff \mathrm{Gal}(K(f)/K) \text{ es un grupo resoluble.}$$

Prueba.–

($\Rightarrow$) Por hipótesis, $K(f) \subset E$ con E/K radical.

Tomando la clausura normal, podemos suponer directamente que E/K es *Galois* y radical, con pisos primos E_i, $1 \leq i \leq n$, donde $E_i = E_{i-1}(\alpha_i)$ con $\alpha_i^{p_i} \in E_{i-1}$.
Sean $\omega_i \in \overline{K}$ raíces primitivas de orden p_i de 1, $1 \leq i \leq n$.

Entonces E/K Galois radical $\Rightarrow$ $E(\omega_1, \ldots, \omega_n)/K(\omega_1, \ldots, \omega_n)$ Galois radical,

y por lo tanto, por la proposición 12.3.5,

$\mathrm{Gal}(E(\omega_1, \ldots, \omega_n)/K(\omega_1, \ldots, \omega_n))$ es resoluble.

Esto implica por el lema 12.3.4 que $\mathrm{Gal}(E/K)$ es resoluble.

Concluimos con:

$K(f)/K$ Galois $\Rightarrow$ $\mathrm{Gal}(E/K(f)) \lhd \mathrm{Gal}(E/K)$

y $\mathrm{Gal}(K(f)/K) \simeq \mathrm{Gal}(E/K)/\mathrm{Gal}(E/K(f))$,

y sabiendo que

$$\mathrm{Gal}(E/K) \text{ resoluble} \iff \mathrm{Gal}(E/K(f)) \text{ y } \mathrm{Gal}(E/K)/\mathrm{Gal}(E/K(f)) \text{ resolubles.}$$

Al ser $\mathrm{Gal}(E/K)$ resoluble se concluye que $\mathrm{Gal}(K(f)/K)$ es resoluble.

($\Leftarrow$) Por hipótesis, $\mathrm{Gal}(K(f)/K)$ es resoluble con cocientes primos $p_1, \ldots, p_n$.

Entonces por el lema 12.3.4, $\mathrm{Gal}(K(f)(\omega_1, \ldots, \omega_n)/K(\omega_1, \ldots, \omega_n))$ es resoluble, donde $\omega_1, \ldots, \omega_n$ son raíces primitivas de 1 de orden $p_1, \ldots, p_n$ resp.

Y por la proposición 12.3.6, $K(f)(\omega_1, \ldots, \omega_n)/K(\omega_1, \ldots, \omega_n)$ es radical.

Como $K(\omega_1, \ldots, \omega_n)/K$ es radical, ent. $K(f)(\omega_1, \ldots, \omega_n)/K$ es radical, y por lo tanto $K(f)/K$ es resoluble por estar contenida en una extensión radical.

■

Consecuencias

- Las ecuaciones generales de grado 2,3 y 4 son resolubles por radicales pues S_2, S_3 y S_4 lo son.
- La ecuación general de grado ≥ 5 no es resoluble por radicales pues S_n no es resoluble para $n \geq 5$.

  (Niels Enrik Abel, 1802-1829)
- Un ejemplo concreto:

  $$f = X^5 - 6X + 3$$

  es irreducible en $\mathbb{Q}[X]$ por

  $\mathrm{Gal}(f/\mathbb{Q}) < S_5$ y $5 \,|\, |\mathrm{Gal}(f/\mathbb{Q})|$:

Por lo tanto existe en $\mathrm{Gal}(f/\mathbb{Q})$ un ciclo de orden 5 por

Probaremos que $\mathrm{Gal}(f/\mathbb{Q})$ contiene además una transposición:

f tiene 3 raíces reales, 2 positivas y 1 negativa pues

$f(0) = 3\,,\ f(-2) < 0\,,\ f(1) < 0$ y $f(2) > 0$

Pero no tiene más de 3 por la regla de los signos de Descartes.

O sea f tiene dos raíces en $\mathbb{C} \setminus \mathbb{R}$ que son conjugadas.

Notar que $\sigma : \mathbb{C} \to \mathbb{C}$ es un $\mathbb{Q}$-automorfismo de $\mathbb{C}$

Y $\sigma|_{\mathbb{Q}(f)} \in \mathrm{Gal}(f/\mathbb{Q})$ manda la raíz compleja no real de f a su conjugada.

Por lo tanto $\mathrm{Gal}(f/\mathbb{Q})$ contiene un 5-ciclo y una transposición:

contiene todo S_5. O sea $\mathrm{Gal}(f/\mathbb{Q}) = S_5$.

Se concluye que f no es resoluble por radicales.

12.4 Existencia para $n \in \mathbb{N}$ de $f \in \mathbb{Q}[X]$ con $\mathrm{Gal}(f, \mathbb{Q}) = S_n$

$f = X^3 - s_1(X_1, X_2, X_3)X^2 + s_2(X_1, X_2, X_3)X - s_3(X_1, X_2, X_3)$ es irreducible en $\mathbb{Q}(s_1, s_2, s_3)[X]$ pues

Sabemos que $\mathrm{Gal}(f/\mathbb{Q}(s_1, s_2, s_3)) = S_3$.
¿Qué pasa cuando especializamos los coeficientes?

- $s_1 = s_2 = 0, s_3 = 1$: $\quad f = X^3 - 1$ no es irreducible y $\mathrm{Gal}(f/\mathbb{Q}) \neq S_3$.
- $s_1 = s_2 = 0, s_3 = 2$: $\quad f = X^3 - 2$ es irreducible y $\mathrm{Gal}(f/\mathbb{Q}) = S_3$.
- $s_1 = 1, s_2 = -2, s_3 = -1$: $\quad f = X^3 + X^2 - 2X - 1$, ejemplo visto antes, es irreducible pero $\mathrm{Gal}(f/\mathbb{Q}) = A_3 \neq S_3$.

Así que que el grupo de Galois sea S_n no depende solo de la irreducibilidad de f, como ya sabemos, sino que depende de que el grado del polinomio minimal de un elemento primitivo θ de la extensión $\mathbb{Q}(f)/\mathbb{Q}$ sea $n!$.

Teorema de irreducibilidad de Hilbert

Sea $\boldsymbol{Y} = (Y_1, \ldots, Y_n)$ y $g(\boldsymbol{Y}, X) \in \mathbb{Q}[\boldsymbol{Y}, X]$ irreducible.
Entonces existen infinitos $\boldsymbol{a} \in \mathbb{Q}^n$ tales que $g_{\boldsymbol{a}}(X) := g(\boldsymbol{a}, X)$ es irreducible en $\mathbb{Q}[X]$.

■

Ejemplo
$X^2 - Y$ es irreducible en $\mathbb{Q}[Y, X]$ y $X^2 - a$ es irreducible en $\mathbb{Q}[X]$ para todo $a < 0$ y para todo $a > 0$ con $a \notin \mathbb{Q}^2$.

Existencia para cada $n \in \mathbb{N}$ de $f \in \mathbb{Q}[X]$ con $\mathrm{Gal}(f, \mathbb{Q}) = S_n$:

Para $\boldsymbol{X} = (X_1, \ldots, X_n)$, sean

$$K := \mathbb{Q}(s_1(\boldsymbol{X}), \ldots, s_n(\boldsymbol{X})) \quad \text{y} \quad f_{\boldsymbol{X}} = X^n - s_1(\boldsymbol{X})X^{n-1} + \cdots + (-1)^n s_n(\boldsymbol{X}) \in K[X]$$

de manera que $E = K(f_{\boldsymbol{X}}) = K(X_1, \ldots, X_n) = \mathbb{Q}(X_1, \ldots, X_n)$ satisface como sabemos $\mathrm{Gal}(E/K) = S_n$.
Entonces E/K es simple y existen $c_1, \ldots, c_n \in \mathbb{Q}$ tq

$$\theta_{\boldsymbol{X}} = c_1 X_1 + \cdots + c_n X_n$$

es un elemento primitivo:

$$E = K(f_{\boldsymbol{X}}) = K(\theta_{\boldsymbol{X}}) \quad \text{y} \quad f(\theta_{\boldsymbol{X}}, K) = \prod_{\sigma \in S_n} \big(X - \sigma(\theta_{\boldsymbol{X}})\big) \in K[X]$$

es un polinomio irreducible de $K[X]$ de grado $n!$.

Nuestro objetivo es especializar $(s_1, \ldots, s_n) \mapsto (a_1, \ldots, a_n) \in \mathbb{Q}^n$
de manera que el polinomio

$$f_{\boldsymbol{a}} = X^n - a_1 X^{n-1} + \cdots + (-1)^n a_n = (X - \alpha_1) \cdots (X - \alpha_n)$$

con $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ satisfaga que para $\theta_{\boldsymbol{\alpha}} := c_1\alpha_1 + \cdots + c_n\alpha_n$,

$$\prod_{\sigma \in S_n} \big(X - \sigma(\theta_{\boldsymbol{\alpha}})\big)$$

(que como se ve tiene grado $n!$) sea un polinomio irreducible de $\mathbb{Q}[X]$.
Así se tendrá $[\mathbb{Q}(\theta_{\boldsymbol{\alpha}}) : \mathbb{Q}] = n!$ y como $\mathbb{Q}(\theta_{\boldsymbol{\alpha}}) \subset \mathbb{Q}(\alpha_1, \ldots, \alpha_n) = \mathbb{Q}(f_{\boldsymbol{a}})$, concluiremos que

$$\mathbb{Q}(f_{\boldsymbol{a}}) = \mathbb{Q}(\theta_{\boldsymbol{\alpha}}) \quad \text{y} \quad [\mathbb{Q}(f_{\boldsymbol{a}}) : \mathbb{Q}] = n!, \quad \text{o sea} \quad \mathrm{Gal}(\mathbb{Q}(f_{\boldsymbol{a}})/\mathbb{Q}) = S_n.$$

Afirmación: $f(\theta_{\boldsymbol{X}}, K) \in \mathbb{Q}[s_1(\boldsymbol{X}), \ldots, s_n(\boldsymbol{X})][X]$
(es decir sus coeficientes son polinomios en $s_1, \ldots, s_n$, y no fracciones racionales):

Esto es por el TFPSE, pues $f(\theta_{\boldsymbol{X}}, K) \in \mathbb{Q}[\boldsymbol{X}][X]$ (verificarlo) y para $\tau \in S_n$,

$$\tau(f(\theta_{\boldsymbol{X}}, K)) = \prod_{\sigma \in S_n} \big(X - \tau \circ \sigma(\theta_{\boldsymbol{X}})\big) = f(\theta_{\boldsymbol{X}}, K),$$

dado que $\sigma(\theta_{\boldsymbol{X}}) = c_1\sigma(X_1) + \cdots + c_n\sigma(X_n)$.

O sea

$$f(\theta_{\boldsymbol{X}}, K) = \sum_{\boldsymbol{j},k} b_{\boldsymbol{j},k} s_1^{j_1} \cdots s_n^{j_n} X^k \in \mathbb{Q}[s_1, \ldots, s_n, X]$$

es un polinomio irreducible, pues es irreducible en $\mathbb{Q}(s_1, \ldots, s_n)[X]$ y primitivo.

Y puedo aplicar el teorema de irreducibilidad de Hilbert:
existe $\boldsymbol{a} = (a_1, \ldots, a_n) \in \mathbb{Q}^n$ tal que con la especialización $s_1 \mapsto a_1, \ldots, s_n \mapsto a_n$,

$$f(\theta_{\boldsymbol{X}}, K)(\boldsymbol{a}) = \sum_{\boldsymbol{j},k} b_{\boldsymbol{j},k} a_1^{j_1} \cdots a_n^{j_n} X^k \in \mathbb{Q}[X]$$

es un polinomio irreducible.

Afirmación: *El polinomio* $f_{\boldsymbol{a}} := X^n - a_1X^{n-1} + \cdots + (-1)^n a_n \in \mathbb{Q}[X]$
es irreducible y $\mathrm{Gal}(f_{\boldsymbol{a}}/\mathbb{Q}) = S_n$*:*

Verifiquemos para eso que $\theta_{\boldsymbol{\alpha}} = c_1\alpha_1 + \cdots + c_n\alpha_n$ es elemento primitivo de $\mathbb{Q}(f_{\boldsymbol{a}})/\mathbb{Q}$ con minimal

$$f(\theta_{\boldsymbol{\alpha}}, \mathbb{Q}) = f(\theta_{\boldsymbol{X}}, K)(\boldsymbol{a})$$

Notar que $f_{\boldsymbol{a}}$ es $X^n - s_1X^{n-1} + \cdots + (-1)^n s_n$ especializado en $s_1 = a_1, \ldots, s_n = a_n$.
Y si $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ son las raíces de $f_{\boldsymbol{a}}$, se tiene para $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$,

$$s_1(\boldsymbol{\alpha}) = a_1, \ldots, s_n(\boldsymbol{\alpha}) = a_n.$$

Así,

$$\prod_{\sigma \in S_n} \big(X - \sigma(\theta_{\boldsymbol{X}})\big) = f(\theta_{\boldsymbol{X}}, K) = \sum_{\boldsymbol{j},k} b_{\boldsymbol{j},k} s_1(\boldsymbol{X})^{j_1} \cdots s_n(\boldsymbol{X})^{j_n} X^k$$

$$\Longrightarrow$$

$$\prod_{\sigma \in S_n} \big(X - \sigma(\theta_{\boldsymbol{\alpha}})\big) = \sum_{\boldsymbol{j},k} b_{\boldsymbol{j},k} s_1(\boldsymbol{\alpha})^{j_1} \cdots s_n(\boldsymbol{\alpha})^{j_n} X^k$$

$$= \sum_{\boldsymbol{j},k} b_{\boldsymbol{j},k} a_1^{j_1} \cdots a_n^{j_n} X^k = f(\theta_{\boldsymbol{X}}, K)(\boldsymbol{a})$$

es un polinomio irreducible en $\mathbb{Q}[X]$ que tiene por raíz a $\theta_{\boldsymbol{\alpha}}$.
Por lo tanto $f(\theta_{\boldsymbol{\alpha}}, \mathbb{Q}) = f(\theta_{\boldsymbol{X}}, K)(\boldsymbol{a})$.

■