Álgebra III - 2do C. 2020 - Clase 16 - 23/10/2020

Obtenemos como consecuencia de la independencia lineal de caracteres, que volveremos a encontrarnos más adelante, el resultado siguiente sobre extensiones Galois cíclicas cuando el cuerpo contiene raíces primitivas de la unidad.

Teorema 12.1.2 (Extensiones cíclicas radicales)
Sea K cuerpo y $m \in \mathbb{N}$ con $\operatorname{car}(K) \nmid m$ tal que existe en K una raíz primitiva ω de la unidad de orden m. Entonces

1. *Si E/K es Galois cíclica de orden m, se tiene que existe $\theta \in E$ tal que $E = K(\theta)$ con $\theta^m = a \in K$.*

   En particular $E = K(X^m - a)$.

2. *Si $E = K(\theta)$ con $\theta^m = a \in K$, entonces E/K es Galois cíclica*

   con $|\operatorname{Gal}(E/K)| =: d \,|\, m$, y $E = K(\alpha)$ con $\alpha^d \in K$.

Prueba.–

1. Por hipotesis, $\operatorname{Gal}(E/K) = \langle\sigma\rangle$ con $o(\sigma) = m$, o sea $\mathrm{id}_E, \sigma, \ldots, \sigma^{m-1}$ son todos automorfismos distintos y $\sigma^m = \mathrm{id}_E$.

   Por la independencia lineal de caracteres, existe $\alpha \in E$ tq

   $$\theta := \alpha + \omega\sigma(\alpha) + \cdots + \omega^{m-1}\sigma^{m-1}(\alpha) \neq 0 \quad \text{en} \quad E.$$

   Probemos que $E = K(\theta)$ y $\theta^m \in K$.

   Para ello primero calculemos $\sigma^k(\theta)$ para $0 \leq k \leq m-1$ y veamos que son todos distintos, pues entonces θ será elemento primitivo:

   $$\begin{aligned}
   \sigma^k(\theta) &= \sigma^k(\alpha) + \omega\sigma^{k+1}(\alpha) + \cdots + \omega^{m-1}\sigma^{k+m-1}(\alpha) \\
   &= \sigma^k(\alpha) + \omega\sigma^{k+1}(\alpha) + \cdots + \omega^{m-1-k}\sigma^{m-1}(\alpha) + \omega^{m-k}\alpha + \cdots + \omega^{m-1}\sigma^{k-1}(\alpha) \\
   &= \omega^{m-k}\big(\alpha + \cdots + \omega^{k-1}\sigma^{k-1}(\alpha) + \omega^k\sigma^k(\alpha) + \cdots + \omega^{m-1}\sigma^{m-1}(\alpha)\big) \\
   &= \omega^{m-k}\,\theta
   \end{aligned}$$

   así que son todos distintos nomás para $0 \leq k \leq m-1$. Por lo tanto

$$E = K(\theta) \quad \text{y} \quad f(\theta, K) = \prod_{0 \le k \le m-1} \big(X - \sigma^k(\theta)\big)$$
$$= \prod_{0 \le k \le m-1} \big(X - \omega^{m-k}\theta\big)$$
$$= X^m - \theta^m \ \in \ K[X].$$

Por lo tanto $\theta^m =: a \in K$ como se quería probar, y $E = K(\theta) = K(X^m - a)$, el cuerpo de descomposición de $X^m - a$ sobre K pues

2. Sea
$$\begin{array}{rccl} \Phi: & \mathrm{Gal}(E/K) & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \\ & \sigma & \longmapsto & k \ \text{ si } \ \sigma(\theta) = \omega^k\theta, \end{array}$$
que es un morfismo de grupos pues $f(\theta, K) \,|\, X^m - a = \prod_{0 \le k \le m-1} \big(X - \omega^k\theta\big)$.

Es monomorfismo pues $\omega^k\theta = \omega^j\theta \ \Leftrightarrow \ k \equiv j \ (m)$.

Concluimos que $\mathrm{Gal}(E/K) < \mathbb{Z}/m\mathbb{Z}$ y por lo tanto es cíclico de orden $d \,|\, m$.

Y dado que K contiene una raíz primitiva $\omega^{m/d}$ de orden d de 1, se concluye por (1).

■

12.2 Extensiones radicales según Galois y después

En lo que sigue $\mathrm{car}(K) = 0$, o sea $\mathbb{Q} \subset K$.

Definición 12.2.1 (Extensión Galois-radical)
Diremos que E/K es una extensión G-radical *(por Galois-radical) si existen cuerpos K_i, $0 \le i \le n$, tales que*

- $K =: K_0 \ \subset \ K_1 \ \subset \ \cdots \ \subset \ K_n := E$
- $\exists\, \alpha_i \in K_i \ \ tq \ \ \alpha_i^{m_i} \in K_{i-1} \ \ para\ algún \ \ m_i \in \mathbb{N} \ \ y \ \ K_i = K_{i-1}(\alpha_i)$,
  y además K_{i-1} *contiene una raíz m_i-ésima primitiva de* 1, $\ 1 \le i \le n$.

Observación 12.2.2 ($\mathbb{Q}(\xi_m)$ no es directamente G-radical)
$\mathbb{Q}(\xi_m)/\mathbb{Q}$ *no es directamente* G*-radical pensando en* $\mathbb{Q} =: K_0 \subset K_1 := \mathbb{Q}(\xi_m)$
y $\xi_m^m = 1 \in \mathbb{Q}$ *pues* $\mathbb{Q}$ *no contiene una raíz* m*-ésima primitiva de 1.*

Ejemplos

- $\mathbb{Q}(\xi_3) = \mathbb{Q}(\sqrt{-3})$ es G-radical sobre $\mathbb{Q}$ pues $\sqrt{-3}^2 = -3 \in \mathbb{Q}$ y $-1 \in \mathbb{Q}$.
- $\mathbb{Q}(\xi_4) = \mathbb{Q}(\sqrt{-1})$ es G-radical sobre $\mathbb{Q}$ pues $\sqrt{-1}^2 = -1 \in \mathbb{Q}$ y $-1 \in \mathbb{Q}$.
- $\mathbb{Q}(\xi_5) = \mathbb{Q}\Big(\dfrac{\frac{-1+\sqrt{5}}{2} + \sqrt{\frac{-5-\sqrt{5}}{2}}}{2}\Big)$ es G-radical sobre $\mathbb{Q}$ con

  $$\mathbb{Q} \subset \mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\sqrt{5})\Big(\sqrt{\frac{-5-\sqrt{5}}{2}}\Big)$$

  pues $\sqrt{5}^2 \in \mathbb{Q}$ y $-1 \in \mathbb{Q}$ y $\Big(\sqrt{\frac{-5-\sqrt{5}}{2}}\Big)^2 \in \mathbb{Q}(\sqrt{5})$ con $-1 \in \mathbb{Q}(\sqrt{5})$.
- $\mathbb{Q}(\xi_7)$ no parece ser así nomás G-radical sobre $\mathbb{Q}$ porque

  $$\mathbb{Q} \subset \mathbb{Q}(\sqrt{-7}) \subset \mathbb{Q}(\sqrt{-7})\big(\xi_7\big)$$

  pues para pasar de $\mathbb{Q}(\sqrt{-7})$ a $\mathbb{Q}(\sqrt{-7})\big(\xi_7\big)$ vamos a necesitar agregarle una raíz cúbica de la unidad a $\mathbb{Q}(\sqrt{-7})$...

  Pero está contenida en una extensión G-radical de $\mathbb{Q}$.

Proposición 12.2.3 ($\mathbb{Q}(\xi_n)$ está contenido en una extensión G-radical de $\mathbb{Q}$)
Sea $E_n := \mathbb{Q}\big(\prod_{m \le n}(X^m - 1)\big)$ *para* $n \in \mathbb{N}$.
Entonces E_n *es G-radical.*
En particular $\mathbb{Q}(\xi_n)$ *está contenido en una extensión G-radical de* $\mathbb{Q}$.

Prueba.–
Obervar que $E_m \subset E_n$ para $m < n$. Por inducción en n para $n > 2$:
Caso n compuesto:
– Si $n = m\,k$ con $\mathrm{mcd}(m,k) = 1$, entonces $E_n = E_{n-1}$.
– Si $n = p^k$ con $k > 1$, entonces $\xi_p \in E_{n-1}$ y $\xi_{p^k}^p = \xi_{p^{k-1}} \in E_{n-1}$:

$E_n = E_{n-1}(\xi_{p^k})$ con $\xi_{p^k}^p \in E_{n-1}$ y E_{n-1} contiene la raíz p-ésima primitiva de 1 ξ_p.
– Si $n = p$ primo:
$E_n = E_{n-1}(\xi_p)$ y $\mathrm{Gal}(E_n/E_{n-1}) < \mathrm{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q}) \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ implica
$\mathrm{Gal}(E_n/E_{n-1})$ cíclico de orden $m \,|\, p-1$.
Además E_{n-1} contiene una raíz primitiva de 1 de orden m.
Por lo tanto, por el teorema 12.1.2, existe $\theta \in E_n$ tq $E_n = E_{n-1}(\theta)$ y $\theta^m \in E_{n-1}$.
Se concluye dado que por HI E_{n-1} es G-radical.

■

Observación 12.2.4 (G-radical de Galois)
En realidad la definición de Galois es con pisos de grado primo pero esto es equivalente, ya que si E/K es G-radical con pisos de grado primo, claramente es G-radical con nuestra definición, mientras que si es G-radical, vamos a quebrar cada piso de grado m en pisos de grado primo:

Sea $K(\alpha)/K$ de grado m con $\alpha^m = a \in K$ y $\xi_m \in K$ y $p \,|\, m$.
Entonces $(\alpha^{m/p})^p = a \in K$ y $\xi_p = \xi_m^{m/p} \in K$.
Así $K(\alpha^{m/p})/K$ es un piso de grado p.
Y $K(\alpha)/K(\alpha^{m/p})$ satisface que $\alpha^{m/p} \in K(\alpha^{m/p})$
y $\xi_{m/p} = \xi_m^p \in K \subset K(\alpha^{m/p})$.

El hecho que las raíces de la unidad estén contenidas en extensiones G-radicales justifica las definiciones actuales de extensiones radicales, donde no se tienen en cuenta las raíces de la unidad, se considera directamente que se tienen en forma gratuita en el cuerpo de base.

12.3 Extensiones puras, radicales y resolubles

Definición 12.3.1 (Extensiones puras, radicales y resolubles)
Sea E/K una extensión con $\mathrm{car}(K) = 0$. *Se dice que*

- *E/K es* pura *si $E = K(\alpha)$ con $\alpha^m \in K$ para algún $m \in \mathbb{N}$.*
- *E/K es* radical *si existen cuerpos $K_0, \ldots, K_n$ con*

$$K =: K_0 \subset K_1 \subset \cdots \subset K_n := E \quad y \quad K_i/K_{i-1} \text{ pura para } 1 \leq i \leq n.$$

- E/K *es* resoluble (por radicales) *si está contenido en alguna extensión radical de* K.
- $f \in K[X]$ *es* resoluble por radicales *si su cuerpo de descomposición* $K(f)/K$ *es resoluble.*

Observaciones

- Si $\alpha^m =: a \in K$, entonces $\alpha = \sqrt[m]{a}$, alguna raíz m-ésima en $\overline{K}$ de a.
- E/K radical $\Rightarrow$ E/K finita pues si $K_i/K_{i-1} = K(\alpha_i)$, entonces $E = K(\alpha_1, \ldots, \alpha_n)$.
- Cada piso se podría definir equivalentemente de grado primo para la definición de radical.

Ejemplo interesante *(de extensión resoluble que no es radical)*
Existen extensiones resolubles que no son radicales.
Sea $f = X^3 + X^2 - 2X - 1 \in \mathbb{Q}[X]$, que es irreducible por Gauss, por no tener raíz.
f es resoluble por radicales pues tiene grado 3.
f tiene 3 raíces reales, y por lo tanto $\mathbb{Q}(f) \subset \mathbb{R}$ pues

$$f(-\infty) = -\infty \quad , \quad f(-1) = 1 \quad , \quad f(0) = -1 \quad , \quad f(+\infty) = +\infty$$

Además $\Delta(f) = 7^2 \in \mathbb{Q}^2 \Rightarrow \mathrm{Gal}(f/\mathbb{Q}) \subset A_3 \simeq \mathbb{Z}/3\mathbb{Z}$.
Por lo tanto si $\mathbb{Q}(f)/\mathbb{Q}$ es radical, hay un solo piso de grado 3.
¿Puede ser $\mathbb{Q}(f) = \mathbb{Q}(\alpha)$ con $\alpha^3 \in \mathbb{Q}$?

Comportamiento de extensiones radicales

- *Por torres:* E/F y F/K radicales $\Longrightarrow$ E/K radical.
- *Por trasladado:* F/K radical $\Longrightarrow$ LF/L radical.
- *Por compuesto:* F/K y L/K radicales $\Longrightarrow$ FL/K radical.

- *Por K-inmersiones:*

$$E/K \text{ radical y } \sigma \in \mathrm{Hom}(E/K, \overline{K}/K) \implies \sigma(E)/K \text{ radical :}$$

Por inducción en la cantidad de pisos, o sea lo probamos primero para una extensión pura.

Si $E = K(\alpha)$ con $\alpha^m =: a \in K$,

entonces $\sigma(E) = K(\sigma(\alpha))$

con $\sigma(\alpha)^m = \sigma(\alpha^m) = \sigma(a) = a \in K$.

Ahora $E = K_n = K_{n-1}(\alpha_n)$ con $\alpha_n^m =: a_n \in K_{n-1}$,

y $\sigma \in \mathrm{Hom}(E/K, \overline{K}/K)$.

Entonces $\sigma|_{K_{n-1}} \in \mathrm{Hom}(K_{n-1}/K, \overline{K}/K)$

y $\sigma(K_{n-1})/K$ radical.

Pero $\sigma(E) = \sigma(K_{n-1})(\sigma(\alpha_n))$

y $\sigma(\alpha_n)^m = \sigma(\alpha_n^m) = \sigma(a_n) \in \sigma(K_{n-1})$.

Corolario 12.3.2 (Extensión radical y clausura normal)

1. *Sea E/K radical. Entonces la clausura normal N/K de E/K es radical también.*
2. *Sea $f \in K[X]$ irreducible. Entonces*

   f es resoluble por radicales $\iff$ $\exists\, \alpha$ raíz de f tq $K(\alpha)/K$ es resoluble.

Prueba.–

1. Recordemos que $\#\mathrm{Hom}(E/K, \overline{K}/K) \leq [E : K]$ y se tiene

$$N = \prod_{\sigma \in \mathrm{Hom}(E/K, \overline{K}/K)} \sigma(E) :$$

(esta caracterización es demasiado importante para esta perdida en una demostración)

2. Si $K(\alpha) \subset E$ con E/K radical, $K(\alpha) \subset N$, la clausura normal, con N/K radical,

   y si β es otra raíz de $f(\alpha, K)$, entonces $K(\beta) = K(\sigma(\alpha)) \subset \sigma(E)/K \subset N/K$. ∎

Relación con grupos resolubles

Recuerdo:

Definición 12.3.3 (Grupo resoluble)
Sea G un grupo finito. Se dice que es resoluble *si existen subgrupos $G_0, \ldots, G_n$ de G tq*

$$\{1\} =: G_n < G_{n-1} < \cdots < G_1 < G_0 := G$$

con

- $G_i \lhd G_{i-1}$ *para* $0 < i \leq n$,
- $[G_{i-1} : G_i] = |G_{i-1}/G_i|$ *es primo, i.e.* $G_{i-1}/G_i \simeq \mathbb{Z}/p_i\mathbb{Z}$ *para algún primo* p_i, $0 < i \leq n$.

Ejemplo
Los grupos abelianos finitos son resolubles.

Propiedad de grupos resolubles que utilizaremos
Sea G grupo finito y $H \lhd G$. Entonces

$$G \text{ es resoluble} \iff H \text{ y } G/H \text{ son resolubles.}$$
