Álgebra III - 2do C. 2020 - Clase 9 - 29/9/2020

Busquemos ahora cuando hay elementos que generan nuestras extensiones separables finitas.

Definición 7.2.10 (Extensiones simples - elemento primitivo)
Sea E/K extensión de cuerpos. Se dice que E es simple *sobre K (o* monógena*) si existe $\theta \in E$ tal que $E = K(\theta)$.*
En ese caso se dice que $\theta \in E$ es un elemento primitivo *de E/K.*

El interés es porque es mucho más fácil trabajar con extensiones simples, porque conocemos todo su Hom.

Observación 7.2.11 (¿Cuándo es $E = K(\theta)$ para E separable/K?)
Sea E/K separable finita, y $\theta \in E$. Entonces

$$E = K(\theta) \iff \forall\, \sigma \neq \sigma' \in \mathrm{Hom}(E/K, \overline{K}/K),\ \sigma(\theta) \neq \sigma'(\theta).$$

Prueba.–
Sabemos que como E/K es separable, $[E:K] = \#\mathrm{Hom}(E/K, \overline{K}/K)$ y

$$f(\theta, K) = \prod_{1 \leq i \leq k} \big(X - \sigma_i(\theta)\big)$$

donde $\sigma_i(\theta)$ recorre todos los valores *distintos* de $\sigma(\theta)$ para $\sigma \in \mathrm{Hom}(E/K, \overline{K}/K)$.
Por lo tanto,

$$\begin{aligned} \forall\, \sigma \neq \sigma' \in \mathrm{Hom}(E/K, \overline{K}/K),\ \sigma(\theta) \neq \sigma'(\theta) &\iff \mathrm{gr}(f(\theta, K)) = \#\mathrm{Hom}(E/K, \overline{K}/K) \\ &\iff [K(\theta):K] = [E:K] \\ &\iff K(\theta) = E, \end{aligned}$$

pues como $K(\theta) \subset E$, $K(\theta) = E \Leftrightarrow [K(\theta):K] = [E:K]$.

■

Teorema 7.2.12 Las extensiones separables finitas son simples
Sea E/K separable finita. Entonces existe $\theta \in E$ tal que $E = K(\theta)$.
Más aún, si K es infinito, y $E = K(\alpha_1, \ldots, \alpha_n)$, entonces para cualquier subconjunto infinito $S \subset K$, existen $c_2, \ldots, c_n \in S$ tales que $\theta = \alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n$.

Prueba.–

La vamos a hacer primero para el caso K infinito y luego para el caso K finito.

(1) *Caso K infinito:*

Por inducción en la cantidad de generadores $\alpha_1, \ldots, \alpha_n$ tal que $E = K(\alpha_1, \ldots, \alpha_n)$.

- El caso clave es el caso $E = K(\alpha, \beta)$, dos generadores.

Sean

$$f(\alpha, K) = (X - \alpha_1) \cdots (X - \alpha_r) \quad \text{y} \quad f(\beta, K) = (X - \beta_1) \cdots (X - \beta_t).$$

Recordemos que $\sigma \in \mathrm{Hom}(K(\alpha, \beta)/K, \overline{K}/K)$ está determinado por donde manda α y β, y que obligatoriamente $\sigma(\alpha) = \alpha_i$ para algún i y $\sigma(\beta) = \beta_j$ para algún j, y por lo tanto, para todo $c \in K$,

$$\sigma(\alpha + c\,\beta) = \alpha_i + c\,\beta_j$$

para algún par (i, j).

Buscamos aplicar la observación anterior: probar que existe algún $c \in K$ para el cual

$$\sigma(\alpha + c\,\beta) \neq \sigma'(\alpha + c\,\beta) \quad \forall\, \sigma \neq \sigma' \in \mathrm{Hom}(K(\alpha, \beta)/K, \overline{K}/K).$$

Para ello alcanza con pedir

$$\alpha_i + c\,\beta_j \neq \alpha_k + c\,\beta_\ell, \quad \forall\, (i, j) \neq (k, \ell).$$

Pero notemos que si $j = \ell$, entonces automáticamente $\alpha_i + c\,\beta_j \neq \alpha_k + c\,\beta_\ell$ para $i \neq k$ pues las raíces de $f(\alpha, K)$ son simples. Por lo tanto pedimos

$$\alpha_i + c\,\beta_j \neq \alpha_k + c\,\beta_\ell, \quad \forall\, j \neq \ell.$$

Ahora, para $j \neq \ell$,

$$\alpha_i + c\,\beta_j = \alpha_k + c\,\beta_\ell \iff c(\beta_j - \beta_\ell) = \alpha_k - \alpha_i \iff c = \frac{\alpha_k - \alpha_i}{\beta_j - \beta_\ell}.$$

Sea entonces $c \in K$ (o $c \in S \subset K$) tal que

$$c \notin \left\{ \frac{\alpha_k - \alpha_i}{\beta_j - \beta_\ell} : 1 \leq i, k \leq s,\ 1 \leq j \neq \ell \leq t \right\},$$

y verifiquemos que $\theta := \alpha + c\,\beta \in K(\alpha, \beta)$ es elemento primitivo, o sea que

$$\sigma(\theta) \neq \sigma'(\theta) \ \text{ para } \ \sigma \neq \sigma' \in \mathrm{Hom}(K(\alpha, \beta)/K, \overline{K}/K) :$$

Existen i, j tq $\sigma(\alpha) = \alpha_i$ y $\sigma(\beta) = \beta_j$ y para $\sigma' \neq \sigma$, existen k, ℓ con $(k, \ell) \neq (i, j)$ tq $\sigma'(\alpha) = \alpha_k$ y $\sigma'(\beta) = \beta_\ell$.
Si $j = \ell$ entonces $i \neq k$ y $\sigma(\theta) = \alpha_i + c\beta_j \neq \alpha_k + c\beta_\ell = \sigma'(\theta)$.
Mientras que si $j \neq \ell$, $\sigma(\theta) = \alpha_i + c\beta_j \neq \alpha_k + c\beta_\ell = \sigma'(\theta)$ pues $c \neq \dfrac{\alpha_k - \alpha_i}{\beta_j - \beta_\ell}$.

- El caso $n > 2$ para K infinito se reduce al caso $n = 2$ por torres:

Dado $E = K(\alpha_1, \ldots, \alpha_n) = K(\alpha_1, \ldots, \alpha_{n-1})(\beta)$ con $\beta := \alpha_n$,
por HI, existen $c_2, \ldots, c_{n-1} \in K$ (o S) tq
para $\alpha := \alpha_1 + c_2\alpha_2 + \cdots + c_{n-1}\alpha_{n-1}$,
$F := K(\alpha_1, \ldots, \alpha_{n-1}) = K(\alpha)$.
Y por el caso 2, existe $c \in K$ (o S) tq
para $\theta := \alpha + c\beta$ se tiene

$$E = K(\alpha_1, \ldots, \alpha_n) = F(\beta) = K(\alpha, \beta) = K(\theta).$$

(1) *Caso K finito:*
En ese caso E es una extensión finita de un cuerpo finito.
Esto implica que E es un cuerpo finito.
O sea $(E^\times, \cdot)$ es un grupo abeliano finito.
¿Qué pasa cuando uno tiene un cuerpo E tal que $E^\times$ es un grupo abeliano finito?
¿Cómo es el grupo $E^\times$?

Notar que hemos probado que cualquier extensión finita de un cuerpo finito es simple, independientemente de si fuera separable o no...
(Más adelante vamos a probar que en realidad son todas separables.)

■

Concluimos esta parte con la caracterización de las extensiones finitas simples aún en el caso no separable. Empezamos con el lema siguiente.

Lema 7.2.13 (Igualdad de subextensiones en extensiones finitas simples)
Sea $E = K(\theta)$ *algebraica sobre* K *y sean* $F, L/K$ *subextensiones. Entonces*

$$F = L \iff f(\theta, F) = f(\theta, L).$$

Prueba.–
($\Rightarrow$) OK
($\Leftarrow$) Investigamos $F \cap L$:
Si $f := f(\theta, F) = f(\theta, L)$,
entonces $[K(\theta) : F] = [K(\theta) : L]$
Pero también $f \in (F \cap L)[X]$, y por lo tanto
$[K(\theta) : F \cap L] = [K(\theta) : F]$ también.
Por lo tanto $F \cap L = F = L$.

■

Teorema 7.2.14 (Caracterización de extensiones finitas simples)
Sea E/K *finita. Entonces*

$$E \text{ es simple} \iff E \text{ tiene finitas subextensiones sobre } K.$$

Prueba.–
($\Rightarrow$) Sea F/K subextensión de $E = K(\theta)$. Entonces $f(\theta, F) \mid f(\theta, K)$. Pero $f(\theta, K)$ tiene solo finitos divisores, luego hay finitos $f(\theta, F)$ posibles. Por el lema anterior hay finitos F posibles.
($\Leftarrow$) Si K es finito, o sea E es finito, ya probamos que E/K es simple en la demostración del teorema 7.2.12.
Nos dedicamos al caso K infinito:
Supongamos $E = K(\alpha_1, \ldots, \alpha_n)$. Nuevamente inducción en n donde el caso clave es $E = K(\alpha, \beta)$.
Existen solo finitas subextensiones $K(\alpha + c\,\beta)$ para $c \in K$. Por lo tanto existen $c \neq c' \in K$ tq $K(\alpha + c\,\beta) = K(\alpha + c'\beta)$.
Esto implica $K(\alpha, \beta) = K(\alpha + c\,\beta)$.
Para el caso n, sigo así...

■

8 Teoría de Galois

Évariste Galois, 25 de octubre 1811- 31 de mayo de 1832

Pregunta
¿Quiénes son todas las subextensiones de $\mathbb{Q}(\sqrt[3]{2},\omega)=\mathbb{Q}(\theta)$ con $\theta=\sqrt[3]{2}+\omega$?

$$f:=f(\theta,\mathbb{Q})=X^6+3X^5+6X^4+3X^3+X^2+9X+9.$$

¿Cuántas subextensiones podría haber en principio si miramos los candidatos de f?

¿ Pero definen todos los divisores de f que contienen a $X-\theta$ subextensiones?
Ya conocemos 4 subextensiones no triviales:

$F_1=\mathbb{Q}(\sqrt[3]{2})\quad$ con $\quad f(\theta,F_1)=\big(X-\theta\big)\big(X-(\sqrt[3]{2}+\omega^2)\big)$
$F_2=\mathbb{Q}(\sqrt[3]{2}\omega)\quad$ con $\quad f(\theta,F_2)=\big(X-\theta\big)\big(X-(\sqrt[3]{2}\omega^2+\omega^2)\big)$
$F_3=\mathbb{Q}(\sqrt[3]{2}\omega^2)\quad$ con $\quad f(\theta,F_3)=\big(X-\theta\big)\big(X-(\sqrt[3]{2}\omega+\omega^2)\big)$
$L=\mathbb{Q}(\omega)\quad$ con $\quad f(\theta,L)=\big(X-\theta\big)\big(X-(\sqrt[3]{2}\omega+\omega)\big)\big(X-(\sqrt[3]{2}\omega^2+\omega)\big)$

Por ejemplo, supongamos que F es tal que
$(X-(\sqrt[3]{2}+\omega))(X-(\sqrt[3]{2}\omega+\omega))\,|\,f(\theta,F)\,.$
Entonces existe $\sigma\in\mathrm{Hom}(\mathbb{Q}(\theta)/F,\overline{\mathbb{Q}}/F)$ tal que $\sigma(\theta)=\sqrt[3]{2}\omega+\omega\,.$
Sabemos que σ extiende a algún $\psi\in\mathrm{Hom}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q},\overline{\mathbb{Q}}/\mathbb{Q})\,,$
y σ extiende a algún $\tau\in\mathrm{Hom}(\mathbb{Q}(\omega)/\mathbb{Q},\overline{\mathbb{Q}}/\mathbb{Q})\,.$
Las únicas posibilidades son
σ extiende a $\psi:\sqrt[3]{2}\mapsto\sqrt[3]{2}\omega$
y σ extiende a $\tau:\omega\mapsto\omega\,.$

Además, como $\mathbb{Q}(\theta)=\mathbb{Q}(X^3-2)$ es normal, $\mathrm{Hom}(\mathbb{Q}(\theta)/\mathbb{Q},\overline{\mathbb{Q}}/\mathbb{Q})=\mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q})$ que es un grupo con la composición.
O sea, si $\sigma\in\mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q})\,,$ σ^2 también, y dado que $\sigma^2(\theta)=\sqrt[3]{2}\omega^2+\omega\,,$ se tiene que $X-\sigma^2(\theta)=X-(\sqrt[3]{2}\omega^2+\omega)\,|\,f(\theta,F)$ también...

¿Qué complicado, no?

Esta es una de las preguntas que vamos a poder responder sencillamente con la Teoría de Galois.

8.1 Extensiones de Galois o extensiones galoisianas

Definición 8.1.1 (Extensión de Galois)
Sea E/K una extensión. Se dice que es Galois *si es una extensión algebraica que es normal y separable.*

Observación 8.1.2 (Propiedades de las extensiones de Galois)
Sea E/K Galois. Entonces

- $\mathrm{Hom}(E/K, \overline{K}/K) = \mathrm{Gal}(E/K)$ *¡que es un grupo con la composición!*

Si además E/K es finita, entonces

- $[E : K] = |\mathrm{Gal}(E/K)|$.
- *$E = K(\theta)$ para algún $\theta \in E$, y*

$$f(\theta, K) = \prod_{\sigma \in \mathrm{Gal}(E/K)} \big(X - \sigma(\theta)\big).$$

De hecho para extensiones finitas hay equivalencias:

Proposición 8.1.3 (Extensiones Galois finitas)
Sea E/K finita. Entonces son equivalentes

1. *E/K es normal y separable,*
2. *E/K es el cuerpo de descomposición de un polinomio separable sobre K,*
3. *$[E : K] = |\mathrm{Gal}(E/K)|$.*

Y en cualquiera de estos casos, E/K es Galois.

Prueba.–
$(1 \Leftrightarrow 2)$

($\Rightarrow$) Cpo de descomposición por ser normal finita, de un pol. separable por ser separable.

($\Leftarrow$) Normal por ser cpo de descomposición, separable por estar generada por eltos separables.

$(1 \Leftrightarrow 3)$

($\Rightarrow$) Hecho arriba.

($\Leftarrow$) Sabemos que $|\mathrm{Gal}(E/K)| \leq |\mathrm{Hom}(E/K, \overline{K}/K)| \leq [E : K]$. La segunda igualdad se cumple si y solo si es separable, y la primera implica que es normal.

■

Ejemplos

- $\overline{\mathbb{Q}}/\mathbb{Q}$

- $\mathbb{Q}(\sqrt[3]{2},\xi_3)/\mathbb{Q} \quad , \quad |\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2},\xi_3)/\mathbb{Q})| = 6 \quad , \quad \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2},\xi_3)/\mathbb{Q}) \simeq$

- $\mathbb{Q}(\xi_n)/\mathbb{Q} \quad , \quad |\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q})| = \varphi(n) \quad , \quad \mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) \simeq \mathcal{U}(\mathbb{Z}/n\mathbb{Z})\,.$

- Extensiones cuadráticas de un cuerpo K con $\mathrm{car}(K) \neq 2$

  ¿Y en característica 2?

- $K(f)/K$ donde $f \in K[X]$ es un polinomio separable sobre K.
  En ese caso $\mathrm{Gal}(K(f)/K)$ se notará $\mathrm{Gal}(f/K)$.