Álgebra III - 2do C. 2020 - Clase 8 - 25/9/2020

7.2 Extensiones separables

Definición 7.2.1 (Elemento separable - Extensión separable)
Sea E/K una extensión de cuerpos.

- *Sea $\alpha \in E$. Se dice que α es* separable sobre K *si α es algebraico sobre K y el polinomio minimal $f(\alpha, K) \in K[X]$ es separable.*
- *Se dice que E/K es una* extensión separable*, o que E* es separable sobre K *si para todo $\alpha \in E$, α es separable sobre K. (En particular una extensión separable es algebraica.)*

Observación 7.2.2 (En característica 0, algebraica = separable)
Sea K cuerpo con $\mathrm{car}(K) = 0$ y sea E/K extensión algebraica, entonces E/K es separable.

Observación 7.2.3 (Torres y separabilidad - I)
Sea $E/F/K$ una torre. Entonces

$$E/K \ \ \textit{separable} \quad \Longrightarrow \quad E/F \ \ \textit{y} \ \ F/K \ \ \textit{separable.}$$

Prueba.–

■

Proposición 7.2.4 (Separabilidad y K-inmersiones - I)
Sea K un cuerpo y $\alpha \in \overline{K}$

1.

$$\alpha \text{ \textit{es separable sobre} } K \iff \#\mathrm{Hom}(K(\alpha)/K, \overline{K}/K) \;=\; [K(\alpha):K],$$

y en ese caso,

$$f(\alpha, K) = \prod_{\sigma \in \mathrm{Hom}(K(\alpha)/K, \overline{K}/K)} (X - \sigma(\alpha)).$$

En particular el polinomio $\displaystyle\prod_{\sigma \in \mathrm{Hom}(K(\alpha)/K, \overline{K}/K)} (X - \sigma(\alpha))$ *pertenece a* $K[X]$ *y es irreducible.*

2.

$$\alpha \text{ \textit{es separable sobre} } K \iff K(\alpha)/K \text{ \textit{es separable.}}$$

Prueba.–

1. Esto es exactamente lo que dice el corolario 6.0.2(1), ya que α separable/K $\Leftrightarrow$ $f(\alpha, K)$ tiene todas sus raíces simples

2.

   $(\Leftarrow)$ OK

   $(\Rightarrow)$ Sea $\beta \in K(\alpha)$. Qpq β es separable sobre K.

   Por un lado,

   α separable sobre K $\Rightarrow$

   $\#\mathrm{Hom}(K(\alpha)/K, \overline{K}/K) \;=\; [K(\alpha):K]$.

   Por otro lado, considerando la torre $K(\alpha)/K(\beta)/K$:

   α separable sobre $K(\beta)$ $\Rightarrow$

   $\#\mathrm{Hom}(K(\alpha)/K(\beta), \overline{K}/K(\beta)) \;=\; [K(\alpha):K(\beta)]$.

   Pero sabemos que

   $[K(\alpha):K] \;=\; [K(\alpha):K(\beta)] \cdot [K(\beta):K]$ y
   $\#\mathrm{Hom}(K(\alpha)/K, \overline{K}/K) \;=\; \#\mathrm{Hom}(K(\alpha)/K(\beta), \overline{K}/K(\beta)) \cdot \#\mathrm{Hom}(K(\beta)/K, \overline{K}/K)$.

   La única forma que se cumpla la primera igualdad entonces es que

   $$\#\mathrm{Hom}(K(\beta)/K, \overline{K}/K) \;=\; [K(\beta):K],$$

   o equivalentemente β separable sobre K.

$\blacksquare$

Ya tenemos las herramientas para probar el full teorema.

Teorema 7.2.5 (Separabilidad y K-inmersiones)
Sea E/K finita. *Entonces*

$$E/K \text{ es separable} \iff \#\mathrm{Hom}(E/K, \overline{K}/K) = [E : K].$$

Prueba.–
($\Rightarrow$) Qpq E/K separable $\Rightarrow$ $\#\mathrm{Hom}(E/K, \overline{K}/K) = [E : K]$.
Por inducción en $[E : K]$.

- $[E : K] = 1$: $E = K$ y $\mathrm{Hom}(E/K, \overline{K}/K) = \{\mathrm{id}_K\}$.
- $[E : K] > 1$: Sea $\alpha \in E \setminus K$ y consideremos $E/K(\alpha)/K$. Se tiene por la proposición 7.2.4:

$$\begin{aligned} &K(\alpha)/K \text{ separable} \iff \#\mathrm{Hom}(K(\alpha)/K, \overline{K}/K) = [K(\alpha) : K], \quad \text{y además} \\ &E/K(\alpha) \text{ separable} \implies \#\mathrm{Hom}(E/K(\alpha), \overline{K}/K(\alpha)) = [E : K(\alpha)] \end{aligned}$$

por HI, ya que $E/K(\alpha)$ y $K(\alpha)/K$ son separables. Entonces

$$\begin{aligned} \#\mathrm{Hom}(E/K, \overline{K}/K) &= \#\mathrm{Hom}(E/K(\alpha), \overline{K}/K(\alpha)) \cdot \#\mathrm{Hom}(K(\alpha)/K, \overline{K}/K) \\ &= [E : K(\alpha)] \cdot [K(\alpha) : K] \quad = \quad [E : K] \end{aligned}$$

($\Leftarrow$) Qpq $\#\mathrm{Hom}(E/K, \overline{K}/K) = [E : K]$ $\Rightarrow$ E/K separable.
Para ello sea $\alpha \in K$. Probemos que $\#\mathrm{Hom}(K(\alpha)/K, \overline{K}/K) = [K(\alpha) : K]$.
Sabemos que

$$\begin{aligned} &\#\mathrm{Hom}(E/K, \overline{K}/K) = \#\mathrm{Hom}(E/K(\alpha), \overline{K}/K(\alpha)) \cdot \#\mathrm{Hom}(K(\alpha)/K, \overline{K}/K), \\ &[E : K] = [E : K(\alpha)] \cdot [K(\alpha) : K] \quad \text{y} \\ &\#\mathrm{Hom}(E/K(\alpha), \overline{K}/K(\alpha)) \leq [E : K(\alpha)]\ ,\ \#\mathrm{Hom}(K(\alpha)/K, \overline{K}/K) \leq [K(\alpha) : K] \end{aligned}$$

La única forma que se pueda cumplir $\#\mathrm{Hom}(E/K, \overline{K}/K) = [E : K]$ es que

$$\#\mathrm{Hom}(E/K(\alpha), \overline{K}/K(\alpha)) = [E : K(\alpha)] \quad \text{y} \quad \#\mathrm{Hom}(K(\alpha)/K, \overline{K}/K) = [K(\alpha) : K].$$

■

Proposición 7.2.6 (Torres y separabilidad)
Sea $E/F/K$ una torre. Entonces

$$E/K \ \textit{separable} \quad \Longleftrightarrow \quad E/F \ \textit{y} \ F/K \ \textit{separable.}$$

Prueba.–
Ya probamos $(\Rightarrow)$ así que probemos $(\Leftarrow)$.
Dado $\alpha \in E$, qpq α es separable/ K.
Pero α separable/ F implica $f(\alpha) = 0$ con $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ donde $a_{n-1}, \ldots, a_0 \in F$.
O sea α separable sobre $L = K(a_{n-1}, \ldots, a_0) \subset F$ que es separable/ K y finita:
Así, por la proposición anterior,

$$\#\mathrm{Hom}(L(\alpha)/L, \overline{K}/L) = [L(\alpha) : L] \quad \text{y} \quad \#\mathrm{Hom}(L/K, \overline{K}/K) = [L : K],$$

lo que implica

$$\#\mathrm{Hom}(L(\alpha)/K, \overline{K}/K) = [L(\alpha) : K].$$

Por otro lado,

$$\begin{aligned} &\#\mathrm{Hom}(L(\alpha)/K(\alpha), \overline{K}/K(\alpha)) \leq [L(\alpha) : K(\alpha)] \quad \text{y} \\ &\#\mathrm{Hom}(K(\alpha)/K, \overline{K}/K) \leq [K(\alpha) : K]. \end{aligned}$$

La única posibilidad para que se de la igualdad del renglón anterior es que en particular

$$\#\mathrm{Hom}(K(\alpha)/K, \overline{K}/K) = [K(\alpha) : K].$$

■

Otras consecuencias de todo esto *(Separabilidad vs. torres y compuestos)*

- $\alpha_1, \ldots, \alpha_n \in \overline{K}$:
$$K(\alpha_1, \ldots, \alpha_n)/K \text{ separable} \quad \Longleftrightarrow \quad \alpha_1, \ldots, \alpha_n \text{ separables}/K.$$

- $S \subset \overline{K}$:
$$K(S)/K \text{ separable} \quad \Longleftrightarrow \quad S \text{ separable}/K.$$

- $K \subset F, L \subset \overline{K}$:
$$F/K \text{ separable} \quad \Longrightarrow \quad FL/L \text{ separable}.$$

- $K \subset F, L \subset \overline{K}$:

$$FL/K \text{ separable} \quad \Longleftrightarrow \quad F/K \quad \text{y} \quad L/K \text{ separables.}$$

Corolario 7.2.7 (Separabilidad y cuerpo de descomposición)
El cuerpo de descomposición de un polinomio separable sobre K es una extensión separable de K.

Proposición 7.2.8 (Minimal en extensión separable)
Sea E/K una extensión separable, y sea $\alpha \in E$. Sea

$$\{\sigma(\alpha): \ \sigma \in \operatorname{Hom}(E/K, \overline{K}/K)\} = \{\sigma_1(\alpha), \ldots, \sigma_k(\alpha)\}$$

el conjunto de todos los valores distintos $\sigma(\alpha) \in \overline{K}$ *cuando se recorren los* $\sigma \in \operatorname{Hom}(E/K, \overline{K}/K)$. *Entonces*

$$f(\alpha, K) = \prod_{1 \le i \le k} \big(X - \sigma_i(\alpha)\big).$$

En particular el polinomio de la derecha pertenece a $K[X]$ y es irreducible.

Prueba.–
Sabemos que por ser α separable/K,

$$f(\alpha, K) = \prod_{\psi \in \operatorname{Hom}(K(\alpha)/K, \overline{K}/K)} \big(X - \psi(\alpha)\big),$$

pero cada $\psi \in \operatorname{Hom}(K(\alpha)/K, \overline{K}/K)$ es la restricción de algún $\sigma \in \operatorname{Hom}(E/K, \overline{K}/K)$, y todos los $\sigma \in \operatorname{Hom}(E/K, \overline{K}/K)$ que extienden a un ψ dado valen lo mismo en α.

∎

Ejemplo
Consideremos $E := \mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$ donde ω es raíz cúbica primitiva de 1.
Sabemos que esta extensión es separable,
que $[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = 6$,
y que $\operatorname{Hom}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}, \overline{\mathbb{Q}}/\mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$,
donde

$$\begin{array}{lcl}
\sigma_1 = \mathrm{id}_E & , & \sigma_2: \ \sqrt[3]{2} \mapsto \sqrt[3]{2}, \omega \mapsto \omega^2 \\
\sigma_3: \ \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega, \omega \mapsto \omega & , & \sigma_4: \ \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega, \omega \mapsto \omega^2 \\
\sigma_5: \ \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega^2, \omega \mapsto \omega & , & \sigma_6: \ \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega^2, \omega \mapsto \omega^2
\end{array}$$

Así, se vuelve a verificar que $f(\sqrt[3]{2},\mathbb{Q})=(X-\sqrt[3]{2})(X-\sqrt[3]{2}\omega)(X-\sqrt[3]{2}\omega^2)$ ya que esos son los 3 valores distintos tomados por $\sigma_i(\sqrt[3]{2})$, $1\le i\le 6$.
Análogamente, $f(\omega,\mathbb{Q})=(X-\omega)(X-\omega^2)$, pero también:

$$f(\sqrt[3]{2}+\omega,\mathbb{Q})=\prod_{1\le i\le 6}(X-\sigma_i(\sqrt[3]{2}+\omega)),$$

porque los 6 valores

$$\begin{array}{ccccc} \sqrt[3]{2}+\omega & , & \sqrt[3]{2}+\omega^2 & , & \sqrt[3]{2}\omega+\omega \\ \sqrt[3]{2}\omega+\omega^2 & , & \sqrt[3]{2}\omega^2+\omega & , & \sqrt[3]{2}\omega^2+\omega^2 \end{array}$$

son distintos entre sí. ¿Y por qué sabemos que son distintos entre sí?

Concluimos que la subextensión $\mathbb{Q}(\sqrt[3]{2}+\omega)/\mathbb{Q}$ de $\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q}$ tiene grado 6 también, lo que significa que

$$\mathbb{Q}(\sqrt[3]{2},\omega)=\mathbb{Q}(\sqrt[3]{2}+\omega)$$

y hemos determinado un elemento *primitivo* para esa extensión, un elemento que la genera ($\mathbb{Q}(\sqrt[3]{2}+\omega)$ es una extensión *simple* o *monógena* entonces).

Una cosa que podría (o tendría que) haber mencionado antes cuando hablamos de minimales, es la siguiente relación entre minimales via isomorfismos.

Observación 7.2.9 (Minimales via isomorfismos)
Sea F/K extensión, sea $\psi\in\operatorname{Hom}(F/K,\overline{K},K)$ y sea $\alpha\in\overline{K}$. Entonces

$$\psi(f(\alpha,F))=f(\overline{\psi}(\alpha),\psi(F)),$$

donde $\overline{\psi}$ es cualquier extensión de ψ a $\overline{K}$.

Prueba.–
Esto es porque si $f=f(\alpha,F)\in F[X]$ es irreducible en $F[X]$, con raíces $\alpha_1,\dots,\alpha_n$, entonces $\overline{\psi}(f)=\psi(f)\in\psi(F)[X]$ es irreducible en $\psi(F)[X]$ y sus raíces son $\overline{\psi}(\alpha_1),\dots,\overline{\psi}(\alpha_n)$.

∎

Proposición 7.2.10 (Relaciones de minimales en extensiones separables)

1. *Sea E/K separable y $\alpha\in E$. Entonces*

$$\prod_{\sigma\in\operatorname{Hom}(E/K,\overline{K}/K)}\big(X-\sigma(\alpha)\big)\;=\;f(\alpha,K)^{[E:K(\alpha)]}.$$

2. *Sea $E/F/K$ torre con $E = K(\theta)$ donde θ es separable/K.*

Entonces

$$\begin{aligned} f(\theta, K) &= \prod_{\psi \in \operatorname{Hom}(F/K, \overline{K}/K)} \psi(f(\theta, F)) \\ &= \prod_{\psi \in \operatorname{Hom}(F/K, \overline{K}/K)} f\big(\overline{\psi}(\theta), \psi(F)\big), \end{aligned}$$

cualquiera sea la extensión $\overline{\psi}$ a todo $\overline{K}$ fijada para cada $\psi \in \operatorname{Hom}(E/K, \overline{K}/K)$.

Prueba.–

1. Notamos que hay exactamente $[E : K(\alpha)]$ K-inmersiones $\sigma : E \underset{K}{\hookrightarrow} \overline{K}$ distintas que extienden a cada $\psi : K(\alpha) \underset{K}{\hookrightarrow} \overline{K}$, estas son:

$$\sigma = \overline{\psi} \circ \tau, \quad \tau \in \operatorname{Hom}(E/K(\alpha), \overline{K}/K(\alpha))$$

donde $\overline{\psi}$ es una extensión fijada de ψ a todo $\overline{K}$.

Por lo tanto, dado que para α, $\overline{\psi} \circ \tau(\alpha) = \overline{\psi}(\alpha) = \psi(\alpha)$, se tiene

$$\begin{aligned} \prod_{\sigma \in \operatorname{Hom}(E/K, \overline{K}/K)} \big(X - \sigma(\alpha)\big) &= \prod_{\substack{\psi \in \operatorname{Hom}(K(\alpha)/K, \overline{K}/K) \\ \tau \in \operatorname{Hom}(E/K(\alpha), \overline{K}/K(\alpha))}} \big(X - \overline{\psi} \circ \tau(\alpha)\big) \\ &= \prod_{\tau \in \operatorname{Hom}(E/K(\alpha), \overline{K}/K(\alpha))} \prod_{\psi \in \operatorname{Hom}(K(\alpha)/K)} \big(X - \psi(\alpha)\big) \\ &= \prod_{\tau \in \operatorname{Hom}(E/K(\alpha), \overline{K}/K(\alpha))} f(\alpha, K) \ = f(\alpha, K)^{[E:K(\alpha)]}. \end{aligned}$$

2. Dado que $E = K(\theta) = F(\theta)$, se tiene

$$\begin{aligned} f(\theta, K) = \prod_{\sigma \in \operatorname{Hom}(E/K, \overline{K}/K)} \big(X - \sigma(\theta)\big) \ &= \prod_{\substack{\psi \in \operatorname{Hom}(F/K, \overline{K}/K) \\ \tau \in \operatorname{Hom}(E/F, \overline{K}/F)}} \big(X - \overline{\psi} \circ \tau(\theta)\big) \\ = \prod_{\substack{\psi \in \operatorname{Hom}(F/K, \overline{K}/K) \\ \tau \in \operatorname{Hom}(E/F, \overline{K}/F)}} \overline{\psi}\big(X - \tau(\theta)\big) \ &= \prod_{\psi \in \operatorname{Hom}(F/K, \overline{K}/K)} \overline{\psi}\Big(\prod_{\tau \in \operatorname{Hom}(E/F, \overline{K}/F)} \big(X - \tau(\theta)\big)\Big) \\ = \prod_{\psi \in \operatorname{Hom}(F/K, \overline{K}/K)} \overline{\psi}\big(f(\theta, F)\big) \ &= \prod_{\psi \in \operatorname{Hom}(F/K, \overline{K}/K)} \psi\big(f(\theta, F)\big) \end{aligned}$$

ya que $f(\theta, F) \in F[X] \ \Rightarrow\ \overline{\psi}\big(f(\theta, F)\big) = \psi\big(f(\theta, F)\big)$ pues $\overline{\psi}$ extiende a ψ.

Se concluye con la observación anterior.

$\blacksquare$

Ejemplo retomado

$E = \mathbb{Q}(\sqrt[3]{2} + \omega)$ y $F = \mathbb{Q}(\sqrt[3]{2})$, o sea $\theta = \sqrt[3]{2} + \omega$ y $\alpha = \sqrt[3]{2}$

1.
$$\prod_{1 \le i \le 6} \big(X - \sigma_i(\sqrt[3]{2})\big) = \big((X - \sqrt[3]{2})(X - \sqrt[3]{2}\omega)(X - \sqrt[3]{2}\omega^2)\big)^2 = (X^3 - 2)^2.$$

2. Recordemos que $\mathrm{Hom}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}, \overline{\mathbb{Q}}/\mathbb{Q}) = \{\psi_1, \psi_2, \psi_3\}$
con $\psi_1 : \sqrt[3]{2} \mapsto \sqrt[3]{2},\ \psi_2 : \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega,\ \psi_3 : \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega^2$. También,
$$f(\theta, F) = \prod_{\tau : \mathbb{Q}(\sqrt[3]{2}+\omega) \underset{\mathbb{Q}(\sqrt[3]{2})}{\hookrightarrow} \overline{\mathbb{Q}}} \big(X - \tau(\theta)\big) = \big(X - (\sqrt[3]{2} + \omega)\big)\big(X - (\sqrt[3]{2} + \omega^2)\big).$$
Observamos que
$$\begin{aligned}
\psi_1\big(f(\theta, \mathbb{Q}(\sqrt[3]{2}))\big) &= f(\theta, \mathbb{Q}(\sqrt[3]{2})) = \big(X - (\sqrt[3]{2} + \omega)\big)\big(X - (\sqrt[3]{2} + \omega^2)\big) \ \in\ \mathbb{Q}(\sqrt[3]{2})[X] \\
\psi_2\big(f(\theta, \mathbb{Q}(\sqrt[3]{2}))\big) &= \big(X - (\sqrt[3]{2}\omega + \omega)\big)\big(X - (\sqrt[3]{2}\omega + \omega^2)\big) \ \in\ \mathbb{Q}(\sqrt[3]{2}\omega)[X] \\
\psi_3\big(f(\theta, \mathbb{Q}(\sqrt[3]{2}))\big) &= \big(X - (\sqrt[3]{2}\omega^2 + \omega)\big)\big(X - (\sqrt[3]{2}\omega^2 + \omega^2)\big) \ \in\ \mathbb{Q}(\sqrt[3]{2}\omega^2)[X]
\end{aligned}$$
y finalmente $f(\sqrt[3]{2} + \omega, \mathbb{Q})$ es el producto de esos 6 términos. Podemos observar también que
$$\psi_2\big(f(\theta, \mathbb{Q}(\sqrt[3]{2}))\big) = f\big(\overline{\psi}_2(\theta), \mathbb{Q}(\psi_2(F))\big),$$
cualquiera sea la extensión $\overline{\psi}_2$ de ψ_2 (que o bien manda $\sqrt[3]{2} + \omega$ a $\sqrt[3]{2}\omega + \omega$ o bien a $\sqrt[3]{2}\omega + \omega^2$). Análogamente para ψ_3.