# Álgebra III - 2do C. 2020 - Clase 19 - 10/11/2020

**Proposición 13.5.5** Extensiones p.i. vs. torres y compuestos

1. *Torres: Sea $E/F/K$ torre. Entonces*
$$E/K \ \text{p.i.} \iff E/F \ \text{y} \ F/K \ \text{p.i.}$$
2. *Generadores: Sea $S \subset \overline{K}$. Entonces*
$$K(S)/K \ \text{p.i.} \iff S \ \text{p.i.}/K$$
3. *Trasladado: Sean $K \subset F, L \subset \overline{K}$. Entonces*
$$F/K \ \text{p.i.} \implies LF/L \ \text{p.i.}$$
4. *Compuesto: Sean $K \subset F, L \subset \overline{K}$. Entonces*
$$F/K \ \text{y} \ L/K \ \text{p.i.} \iff FL/K \ \text{p.i.}$$

*Prueba.–*

1. $(\Rightarrow)$ $E/K$ p.i. $\Rightarrow$ $E/F$ p.i pues $f(\alpha, F) \mid f(\alpha, K) = (X-\alpha)^{p^e}$

   $E/K$ p.i. $\Rightarrow$ $F/K$ p.i por ser subextensión.

   $(\Leftarrow)$ $E/F$ p.i $\Rightarrow$ $\alpha^{p^k} \in F$ para algún $k \in \mathbb{N}_0$.

   $\alpha^{p^k} \in F$ y $F/K$ p.i. $\Rightarrow$ $(\alpha^{p^k})^{p^j} \in K$ para algún $j \in \mathbb{N}_0$

   $\Rightarrow$ $\alpha^{p^{k+j}} \in K$ $\Rightarrow$ $\alpha$ p.i.$/K$.

2. $(\Leftarrow)$

   $\forall\, \alpha \in S$, $\mathrm{Hom}(K(\alpha)/K, \overline{K}/K) = \{\mathrm{id}_{K(\alpha)}\} \Rightarrow \mathrm{Hom}(K(S)/K, \overline{K}/K) = \{\mathrm{id}_{K(S)}\}$.

3. $F/K$ p.i. $\Rightarrow$ $F$ p.i.$/L$ $\Rightarrow$ $LF = L(F)$ p.i.$/L$

4. Por (1) y (3)

■

**Corolario 13.5.6** (Grado de una extensión finita p.i.)
*Sea $E/K$ finita y puramente inseparable. Entonces*

1. *Existe $e \in \mathbb{N}_0$ tal que $[E:K] = p^e$.*
2. *Para todo $\alpha \in E$, $\alpha^{[E:K]} \in K$.*

## 13.6 Descomposición de extensiones algebraicas

**Observación 13.6.1** (Extensiones simples)
*Sea* $\alpha \in \overline{K}$ *tal que* $f(\alpha, K) =: f(X) = g(X^{p^e})$ *con*

$$g = (X - \beta_1) \cdots (X - \beta_r) \quad \textit{irreducible y separable en } K[X],$$
$$f = \big((X - \alpha_1) \cdots (X - \alpha_r)\big)^{p^e} \quad \textit{donde } \alpha_i^{p^e} = \beta_i,\ 1 \le i \le r$$

*y notemos* $\alpha = \alpha_1$ *y* $\beta = \beta_1 = \alpha^{p^e}$. *Entonces,*

- $K(\beta)/K$ *es separable con* $[K(\beta) : K] = r$
  *y* $f(\beta, K) = g = (X - \beta_1) \cdots (X - \beta_r)$,
- $K(\alpha)/K(\beta)$ *es p.i. con* $[K(\alpha) : K(\beta)] = p^e$
  *y* $f(\alpha, K(\beta)) = X^{p^e} - \beta$.

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

**Definición-Proposición 13.6.2** (Máxima subextensión separable)
*Sea* $E/K$ *algebraica, y definamos*

$$E_s := \{\beta \in E \,:\, \beta \ \ \textit{es separable}/K\}.$$

*Entonces* $E_s$ *es una subextensión de* $E/K$, *que es separable.*
*Es la máxima subextensión de* $E/K$ *que es separable*$/K$,
*y* $E/E_s$ *es p.i.*

*Prueba.–*
Probamos solo la última afirmación, ya que el resto se charla...
Dado $\alpha \in E$ con $f(\alpha, K) = g(X^{p^e})$
donde $g = (X - \beta_1) \cdots (X - \beta_r)$ es separable,
se tiene $\alpha^{p^e} = \beta \in E_s$, o sea $\alpha$ p.i.$/E_s$.

$\blacksquare$

**Ejemplos**
Sea $E/K$ algebraica. Entonces

- $E = E_s \iff E/K$ separable.

- Sea $E = K(\alpha)$ como en la observación 13.6.1, donde $f(\alpha, K(\beta)) = X^{p^e} - \beta$.

  Entonces $K(\alpha)_s = K(\beta)$,

  pues claramente $K(\beta) \subset K(\alpha)_s$ por ser $\beta$ separable $/K$,

  pero además $K(\alpha)_s/K(\beta)$ es separable y p.i. a la vez $\Rightarrow \quad K(\alpha)_s = K(\beta)$.

  Notar que en ese caso $\#\mathrm{Hom}(K(\alpha)/K, \overline{K}/K) = [K(\alpha)_s : K]$.

Este argumento que usamos de ser separable y p.i. a la vez se puede generalizar:

**Observación 13.6.3**
*Sea $E/K$ algebraica y sea $F/K$ subextensión tal que $E/F$ es p.i. y $F/K$ es separable, entonces $F = E_s$, pues por un lado $F \subset E_s$ pero además $E_s/F$ es separable por ser parte de de $E_s/K$ separable, y $E_s/F$ es p.i. por ser parte de $E/F$ p.i. O sea $E_s = F$.*

**Definición-Proposición 13.6.4** (Grado de separabilidad/inseparabilidad)
*Sea $E/K$ finita. Entonces*

- $[E : K]_i := [E : E_s]$ *es el* grado de inseparabilidad de $E/K$
- $[E : K]_s := [E_s : K]$ *es el* grado de separabilidad de $E/K$

*Se tiene*

- $[E : K] = [E : K]_i \cdot [E : K]_s$
- $[E : K]_s = \#\mathrm{Hom}(E/K, \overline{K}/K)$

  *pues* $\mathrm{Hom}(E/E_s) = \{\mathrm{id}_E\} \;\Rightarrow\; \#\mathrm{Hom}(E/E_s, \overline{K}/E_s) = 1$
  *y* $\#\mathrm{Hom}(E/K, \overline{K}/K) = \#\mathrm{Hom}(E/E_s, \overline{K}/E_s) \cdot \#\mathrm{Hom}(E_s/K, \overline{K}/K)$.
- *Existe* $e \in \mathbb{N}_0$ *tal que* $[E : K]_i = p^e$ *y para todo* $\alpha \in E$, $\alpha^{[E:K]_i} \in E_s$.

■

**Ejemplo**
Retomemos el ejemplo de la observacion 13.6.1 donde sabemos que $K(\alpha)_s = K(\beta)$ y $[K(\alpha) : K(\beta)] = p^e$ para algún $e \in \mathbb{N}_0$. Entonces

$$[K(\alpha) : K]_s = [K(\beta) : K] \quad \text{y} \quad [K(\alpha) : K]_i = [K(\alpha) : K(\beta)] = p^e,$$

$$\text{y} \;\; f(\alpha, K) = \big((X - \alpha_1) \cdots (X - \alpha_r)\big)^{p^e} = \prod_{\sigma \in \mathrm{Hom}(K(\alpha)/K, \overline{K}/K)} \big(X - \sigma(\alpha)\big)^{[K(\alpha):K]_i}.$$

**Corolario 13.6.5** (Grados de sep/insep vs. torres)
*Sea $E/F/K$ finita. Entonces*

1. $[E:K]_s = [E:F]_s \cdot [F:K]_s$ ,
2. $[E:K]_i = [E:F]_i \cdot [F:K]_i$ .

*Prueba.–*

1. $$\begin{aligned} [E:K]_s &= \#\mathrm{Hom}(E/K, \overline{K}/K) = \#\mathrm{Hom}(E/F, \overline{K}/F) \cdot \#\mathrm{Hom}(F/K, \overline{K}/K) \\ &= [E:F]_s [F:K]_s \,. \end{aligned}$$
2. $$[E:K]_i = \frac{[E:K]}{[E:K]_s} = \frac{[E:F]\cdot[F:K]}{[E:F]_s[F:K]_s} = [E:F]_i \cdot [F:K]_i \,.$$

■

---

**Conclusión**
Sea $E/K$ algebraica, y $E_s = \{\beta \in E \,:\, \beta \text{ es separable}\,/K\}$. Entonces

- $E/E_s$ es p.i. y $E_s/K$ es separable.
- Si además $E/K$ es finita,
  - $[E:K]_i = [E:E_s] = p^e$ para algún $e \in \mathbb{N}_0$ , y $\alpha^{p^e} \in E_s$ , $\forall\, \alpha \in E$ .
  - $[E:K]_s = [E_s:K] = \#\mathrm{Hom}(E/K, \overline{K}/K)$.

---

Ahora bien, ¿podemos hacer al revés? ¿Poner una extensión p.i. abajo de todo de manera que la de arriba sea separable?

**Definición-Proposición 13.6.6** (Máxima subextensión puramente inseparable)
*Sea $E/K$ algebraica, y definamos*

$$\begin{aligned} E_i :&= \{\beta \in E \,:\, \beta \;\; \textit{es puramente inseparable}/K\} \\ &= \{\beta \in E \,:\, \beta^{p^e} \in K \;\; \textit{para algún} \;\; e = e(\beta)\} \\ &= \{\beta \in E \,:\, \sigma(\beta) = \beta, \; \forall\, \sigma \in \mathrm{Hom}(E/K, \overline{K}/K)\} \end{aligned}$$

*Entonces $E_i$ es una subextensión de $E/K$ , que es puramente inseparable.*
*Es la máxima subextensión de $E/K$ que es puramente inseparable$/K$ .*

*Prueba.–*
Probamos solo la última igualdad de conjuntos, ya que el resto se charla...
$(\subset)$: $f(\beta,K)=(X-\beta)^{p^e} \;\Rightarrow\; \sigma(\beta)=\beta,\ \forall\,\sigma\in\mathrm{Hom}(E/K,\overline{K}/K)$.
$(\supset)$: $\sigma(\beta)=\beta,\ \forall\,\sigma\in\mathrm{Hom}(E/K,\overline{K}/K) \;\Rightarrow\; f(\beta,K)=(X-\beta)^{p^e}$
para algún $e\in\mathbb{N}_0$.

■

**Observación 13.6.7**

- $E_s\cap E_i=K$.
- $E_i/K$ *finita* $\;\Rightarrow\;$ $[E_i:K]=p^e$ *para algún* $e\in\mathbb{N}_0$.

Peeeero!!!! Lamentablemente $E/E_i$ no tiene por qué ser separable... porque entre p.i. y separable ¡está todo lo del medio!

**Ejemplo**
Sea $p\neq 2$, $K=\mathbb{F}_p(t,u)$ y $E=K(\alpha)$ donde $\alpha\in\overline{K}$ es tal que

$$\begin{aligned} f(\alpha,K) &= X^{2p}+tX^p+u \\ &= \left(X^2+\sqrt[p]{t}X+\sqrt[p]{u}\right)^p \;=\; \big((X-\alpha_1)(X-\alpha_2)\big)^p \\ &\quad\text{con } \alpha=\alpha_1\neq\alpha_2 \text{ raíces de } X^2+\sqrt[p]{t}X+\sqrt[p]{u} \end{aligned}$$

Entonces $E/K$ no es separable, $[E:K]=2p \;\Rightarrow\; [E_i:K]=1$ o $p$.

<u>*Afirmación:*</u> $E_i=K$, con lo cual $E/E_i$ no es separable.
Supongamos que $[E_i:K]=p$.
Entonces, $f(\alpha,E_i)\,|\,f(\alpha,K)=\big((X-\alpha_1)(X-\alpha_2)\big)^p$,
pero $[E:E_i]=2$, o sea $f(\alpha,E_i)\;=\;(X-\alpha_1)(X-\alpha_2)$
(por como son los minimales y $p\neq 2$).
Es decir

$$\begin{aligned} f(\alpha,E_i) &= X^2-(\alpha_1+\alpha_2)X+\alpha_1\alpha_2 \;\in\; E_i[X] \\ &= X^2+aX+b \;\text{ con }\; a,b\in E_i \end{aligned}$$

Esto implica

$$\begin{aligned} f(\alpha,K)=(X^2+aX+b)^p \;=\; X^{2p}+a^pX^p+b^p \quad&\Longrightarrow\quad t=a^p \;\text{ y }\; u=b^p \\ \Longrightarrow\quad a=\sqrt[p]{t},b=\sqrt[p]{u}\;\in\;E_i \quad&\Longrightarrow\quad K(\sqrt[p]{t},\sqrt[p]{u})\;\subset\;E_i. \end{aligned}$$

Pero $[K(\sqrt[p]{t}, \sqrt[p]{u}) : K] = p^2$ y $[E_i : K] = p$. ¡Absurdo!
Por lo tanto $E_i = K$.

¡Lo bueno es que sí vale en el caso de extensiones finitas *normales*!

**Teorema 13.6.8** (Descomposición de extensiones algebraicas finitas *normales*)
*Sea* $E/K$ *finita y* normal *y sea* $G := \mathrm{Gal}(E/K) = \{\sigma : \sigma\ K\text{-}automorfismo\ de\ E\}$.
*Entonces*

1. $E^G = E_i$.

2. $E/E_i$ *es Galois finita y* $\mathrm{Gal}(E/E_i) = G$.

3. $[E : K]_s = |G| = [E : E_i]$
   *y* $[E : K]_i = [E_i : K]$.

4. $E_s \cap E_i = K$ *y* $E_s E_i = E$

5. $E_s/K$ *es Galois*

*Prueba.-*

1. Por definición,
$$\begin{aligned} E^G &= \{\beta \in E \,:\, \sigma(\beta) = \beta,\ \forall\, \sigma \in G\} \\ &= \{\beta \in E \,:\, \sigma(\beta) = \beta,\ \forall\, \sigma \in \mathrm{Hom}(E/K, \overline{K}/K)\} \ = \ E_i \end{aligned}$$
   donde la segunda igualdad es por la normalidad de $E/K$.

2. $|G| < \infty$ pues $|G| \leq [E : K]$, y este es el lema de Artin, pues $E^G = E_i$.

3. Tenemos
   $[E : K]_s = [E_s : K] = \#\mathrm{Hom}(E/K, \overline{K}/K) = \#\mathrm{Gal}(E/K) = |G| = [E : E_i]$,
$$[E : K]_s = \frac{[E : K]}{[E : K]_i} = \frac{[E : E_i][E_i : K]}{[E : K]_i} = \frac{[E : K]_s[E_i : K]}{[E : K]_i} \ \Rightarrow\ [E : K]_i = [E_i : K]$$

4. $E_s \cap E_i = K$ por ser sep. y p.i.
   y $E/E_sE_i$ es separable por ser Galois y p.i. por ser parte de $E/E_s$
   $\Longrightarrow \quad E = E_sE_i$.

5. $E_s/K$ es separable, y es normal pues $\sigma(E) \subset E \ \Rightarrow\ \sigma(E_s) \subset E_s$
   (pues si $E_s$ es separable, $\sigma(E_s)$ es separable también).

■