Álgebra III - 2do C. 2020 - Clase 22 - 20/11/2020

Proposición 14.1.5 (Comportamiento en torres)
Sea $E/F/K$ una torre, y sea S base trasc. de F/K y T base trasc. de E/F.
Entonces $S \cup T$ es base de trascendencia de E/K.
En particular, $\operatorname{trdeg}_K(E) = \operatorname{trdeg}_K(F) + \operatorname{trdeg}_F(E)$.

Prueba.–
Qpq $S \cup T$ es alg.ind./ K y que E es alg./ $K(S \cup T)$.

- $S \cup T$ alg.ind./ K: Sea $f \in K[\boldsymbol{X}, \boldsymbol{Y}]$ tq $f(\boldsymbol{s}, \boldsymbol{t}) = 0$. Entonces

$$0 = f(\boldsymbol{s}, \boldsymbol{t}) = \sum \underbrace{a_{\boldsymbol{k}}(\boldsymbol{s})}_{\in F} \boldsymbol{t}^{\boldsymbol{k}} \quad \text{con} \quad a_{\boldsymbol{k}} \in K[\boldsymbol{X}] \text{ y } \sum \boldsymbol{a_k}(\boldsymbol{s}) \boldsymbol{Y}^{\boldsymbol{k}} \in F[\boldsymbol{Y}]$$

  Por lo tanto, como T alg.ind./ F, $a_{\boldsymbol{k}}(\boldsymbol{s}) = 0$ en F.

  Pero S alg.ind./ K implica $a_{\boldsymbol{k}} = 0$ en $K[\boldsymbol{X}]$.

  Se concluye $f = \sum a_{\boldsymbol{k}}(\boldsymbol{X}) \boldsymbol{Y}^{\boldsymbol{k}} = 0$ en $K[\boldsymbol{X}, \boldsymbol{Y}]$.

- E es alg./ $K(S \cup T)$:

■

¡Ojo!
S, T b.t. de $E/K \quad \not\Longrightarrow \quad [E : K(S)] = [E : K(T)]$.

Ejemplo ya visto implícitamente

$$\begin{array}{c} K(X_1,\dots,X_n) \\ | \\ K(s_1(\boldsymbol{X}),\dots,s_n(\boldsymbol{X})) \\ | \\ K \end{array}$$

14.2 Extensiones trascendentes puras

Definición 14.2.1 (Extensión trascendente pura)
Sea E/K extensión. Se dice que E/K es trascendente pura *si existe $T \subset E$ alg.ind./K tq $E = K(T)$.*

Ejemplos
$K(X_1,\dots,X_n)/K$, $K(s_1(\boldsymbol{X}),\dots,s_n(\boldsymbol{X}))/K$

Observación 14.2.2
En ese caso T es base de trascendencia de E sobre K y $\mathrm{trdeg}_K(E) = \#(T)$.

Proposición 14.2.3 (Ext. trasc. puras y eltos trascendentes)
Sea E/K trascendente pura. Entonces, $\forall\, t \in E \setminus K$, t es trascendente/K.

Prueba.–
Sea $T \subset E$ tq T es alg.ind./K y $E = K(T)$, y sea $t \in E$. Entonces

$$t = \frac{f(t_1,\dots,t_N)}{g(t_1,\dots,t_N)} \text{ con } t_1,\dots,t_N \in T \text{ y } \mathrm{mcd}(f,g) = 1 \text{ en } K[X_1,\dots,X_N].$$

Sup. que $0 \neq F = \displaystyle\sum_{k=0}^{n} a_k X^k \in K[X]$ satisface $F(t) = 0$. Entonces

$$\begin{aligned} \sum a_k \Big(\frac{f(\boldsymbol{t})}{g(\boldsymbol{t})}\Big)^k = 0 \implies & \sum a_k g(\boldsymbol{t})^{n-k} f(\boldsymbol{t})^k = 0 \\ \implies & a_0 g(\boldsymbol{t})^n + a_1 g(\boldsymbol{t})^{n-1} f(\boldsymbol{t}) + \dots + a_{n-1} g(\boldsymbol{t}) f(\boldsymbol{t})^{n-1} + a_n f(\boldsymbol{t})^n = 0 \\ \implies & g(\boldsymbol{t}) \mid a_n f(\boldsymbol{t})^n \quad \text{y} \quad f(\boldsymbol{t}) \mid a_0 g(\boldsymbol{t})^n \\ \underset{\mathrm{mcd}(f,g)=1}{\implies} & g(\boldsymbol{t}) \mid a_n \quad \text{y} \quad f(\boldsymbol{t}) \mid a_0 \\ \implies & g \text{ y } f \text{ son constantes} \quad \implies \quad t \in K. \end{aligned}$$

■

¡Ojo! *¡No vale la recíproca!*

$\forall\, t \in E \setminus K$, t trasc.$/K \;\not\Rightarrow\; E/K$ trasc. pura:

Sea $F = \mathbb{Q}(t)$ y $E = F(\alpha)$ con $f(\alpha, F) = X^2 + t^2 + 1$,

que es irreducible pues

Afirmación: $\forall\, \beta \in E \setminus \mathbb{Q}$, β es trasc.$/\mathbb{Q}$:

si $\beta = \dfrac{f_0(t)}{g_0(t)} + \dfrac{f_1(t)}{g_1(t)}\alpha$ con $\operatorname{mcd}(f_i, g_i) = 1$,

entonces existe $\sigma : E \underset{\mathbb{Q}}{\hookrightarrow} \overline{\mathbb{Q}(t)}$ tq $\sigma(\beta) = \dfrac{f_0(t)}{g_0(t)} - \dfrac{f_1(t)}{g_1(t)}\alpha$.

Si β es alg.$/\mathbb{Q}$, con $f := f(\beta, \mathbb{Q})$, entonces $\sigma(\beta)$ es raíz de f también,

y $\beta + \sigma(\beta) = 2\dfrac{f_0(t)}{g_0(t)}$ alg.$/\mathbb{Q}$, y pertenece a $\mathbb{Q}(t)$ que es trascendente pura$/\mathbb{Q}$.

Por la proposición, concluimos que $\dfrac{f_0(t)}{g_0(t)} \in \mathbb{Q}$.

Por otro lado también tenemos $\dfrac{f_1(t)}{g_1(t)}\alpha$ alg.$/\mathbb{Q}$, y

$$\frac{f_1^2(t)}{g_1^2(t)}\alpha^2 = \frac{f_1^2(t)}{g_1^2(t)}\big(-(t^2+1)\big) \text{ alg.}/\mathbb{Q} \text{ y pertenece a } \mathbb{Q}(t).$$

Nuevamente, por la proposición, $\dfrac{-(t^2+1)f_1^2(t)}{g_1^2(t)} \in \mathbb{Q}$.

Esto implica $g_1^2 \mid t^2 + 1$, o sea $g_1^2 \in \mathbb{Q}$ pero $g_1 \in \mathbb{Q}[t]$.

En definitiva $g_1 \in \mathbb{Q}$. Por lo tanto

$$-(t^2+1)f_1^2(t) \in \mathbb{Q} \quad \Longrightarrow \quad f_1 = 0 \quad \Longrightarrow \quad \beta = \frac{f_0(t)}{g_0(t)} \in \mathbb{Q}.$$

Afirmación: $E/\mathbb{Q}$ no es trascendente pura.

Como $\operatorname{trdeg}_{\mathbb{Q}}(E) = 1$, si E fuera trasc. pura$/\mathbb{Q}$, tendríamos $E = \mathbb{Q}(s)$ para algún $s \in E = \mathbb{Q}(t)(\alpha)$.

Tendríamos $\alpha = \dfrac{f_1(s)}{g_1(s)}$ y $\alpha^2 = -(t^2+1) = \dfrac{f_1^2(s)}{g_1^2(s)}$ con $t = \dfrac{f_2(s)}{g_2(s)}$. Así

$$\frac{f_1^2(s)}{g_1^2(s)} = -\Big(\frac{f_2^2(s)}{g_2^2(s)} + 1\Big) \quad \Longrightarrow \quad \frac{f_1^2}{g_1^2}(s) + \frac{f_2^2}{g_2^2}(s) = -1$$

¡Absurdo en $\mathbb{Q}(s)$!

■

14.3 Extensiones trascendentes puras con $\operatorname{trdeg} 1$

Observación 14.3.1
Sea $E = K(y)$ *trasc. pura/*K *.*
Entonces, $\forall\, z \in E \setminus K$ *,* z *es trasc./*K *,*
Y por lo tanto $\{z\}$ *es base de trasc. de* E/K *.*
En particular $K(y)/K(z)$ *es algebraica y finita*
(por ser simple).
¿Cuál es su grado $[K(y) : K(z)]$ *?*

Definición 14.3.2 (Altura de z)
Sea $z \in K(y)$ *. Entonces* $z = \dfrac{f(y)}{g(y)}$ *con* $f, g \in K[X]$ *coprimos y* $g \neq 0$ *.*
Se define la altura de z *como*

$$\operatorname{ht}(z) = \max\{\operatorname{gr}(f), \operatorname{gr}(g)\}.$$

(Verificar que está bien definida.)

Observación 14.3.3 $\operatorname{ht}(z) = 0 \iff z \in K$ *.*

Proposición 14.3.4 (Grado y altura)
Sea $K(y)/K$ *trascendente pura, y sea* $z \in K(y)$ *. Entonces,*

$$[K(y) : K(z)] = \operatorname{ht}(z) \quad y \quad f(y, K(z)) = g(X)z - f(X) \;\; si\; z = \frac{f(y)}{g(y)} \;\; con\; \operatorname{mcd}(f, g) = 1.$$

(En realidad hay que hacer ese polinomio mónico pero no cambia nada.)

Prueba.–
Si $z = \dfrac{f(y)}{g(y)}$, entonces $g(y)z - f(y) = 0$ con lo cual y es raíz del polinomio

$$F := g(X)z - f(X) \;\in\; K(z)[X].$$

Además F es irreducible en $K(z)[X]$ por ser irreducible y primitivo en $K[X][z]$ (dado que f y g son coprimos):

$$\begin{aligned} F = h_1 h_2 \in K(z)[X] \;&\Rightarrow\; F = \tilde{h}_1(z, X)\tilde{h}_2(z, X) \text{ con } \tilde{h}_1, \tilde{h}_2 \in K[z, X] \text{ y } \operatorname{gr}_X(\tilde{h}_i) = \operatorname{gr}_X(h_i) \\ &\Rightarrow\; \tilde{h}_1 \in K[X] \text{ pues } \operatorname{gr}_z(F) = 1 \\ &\Rightarrow\; F = \tilde{h}_1(X)\tilde{h}_2(z, X) \text{ pero } f \text{ y } g \text{ coprimos } \;\Rightarrow\; \tilde{h}_1 \in K. \end{aligned}$$

Se concluye observando que $\operatorname{gr}(F) = \max\{\operatorname{gr}(f), \operatorname{gr}(g)\} = \operatorname{ht}(z)$.

■

Corolario 14.3.5 (Automorfismos en $K(y)$)
Sea $K(y)/K$ trascendente pura y $z \in K(y)$. Entonces

$$K(y) = K(z) \;\Leftrightarrow\; \mathrm{ht}(z) = 1 \;\Leftrightarrow\; z = \frac{ay+b}{cy+d} \text{ con } a, b, c, d \in K, ad - bc \neq 0.$$

(La condición $ad - bc \neq 0$ garantiza $z \notin K$.)
En particular,

$$\begin{aligned} \mathrm{Aut}(K(y)/K) = &\ \big\{\sigma : y \mapsto z \in K(y) \quad \textit{con} \quad K(y) = K(z)\big\} \\ = &\ \big\{\sigma : y \mapsto \frac{ay+b}{cy+d} \textit{ con } a, b, c, d \in K, ad - bc \neq 0 \quad \textit{(homografía)}\big\} \end{aligned}$$

Una caracterización de las subextensiones de $K(y)/K$ está dado por el famoso

Teorema 14.3.6 (Teorema de Luroth, 1876 - Jacob Luroth, 1844-1910)
Sea $K(y)/K$ trascendente pura con trdeg *1, y sea E/K subextensión con $K \subsetneq E$.*
Entonces existe $z \in K(y) \setminus K$ tq $E = K(z)$.
O sea E/K también es trascendente pura.

Prueba.–
En vista de la discusión anterior,
el candidato para z es $z \in E$ con $\mathrm{ht}(z) \geq 1$ mínima,
pues para $z \in E$ siempre vale $[K(y) : E] \leq [K(y) : K(z)] = \mathrm{ht}(z)$.
Sea entonces $z \in E \setminus K$ con $\mathrm{ht}(z) =: n \geq 1$ *mínima.*
Sabemos que $[K(y) : K(z)] = n$ y queremos probar que $[K(y) : E] = n$
también, sabiendo, como $z \in E$, que $[K(y) : E] =: m \leq n$.
Definimos entonces

$$q(X) := f(y, E) \text{ con } \mathrm{gr}(q) = m \quad \text{y} \quad p(X) := f(y, K(z)) = g(X)z - f(X) \text{ con } \mathrm{gr}(p) = n.$$

Como $p \in E[X]$, sabemos que $q(X) \,|\, p(X)$ en $E[X]$, donde

$$q(X) := X^m + z_{m-1}X^{m-1} + \cdots + z_1X + z_0 \;\text{ con }\; z_0, \ldots, z_m \in E$$

y para aquellos k tq $z_k \notin K$, $\mathrm{ht}(z_i) \geq \mathrm{ht}(z) = n$, y al menos un $z_k \notin K$ pues y no es algebraico$/K$.
Recordemos $z = \dfrac{f(y)}{g(y)}$ y escribamos $z_k = \dfrac{f_k(y)}{g_k(y)}$, $0 \leq k \leq m-1$ (siempre en forma coprima).

Asociamos a q y p los polinomios de $K(y)[X]$:

$$\overline{q}(X) = X^m + \frac{f_{m-1}(y)}{g_{m-1}(y)}X^{m-1} + \cdots + \frac{f_0(y)}{g_0(y)} \quad \text{y} \quad \overline{p}(X) = g(X)\frac{f(y)}{g(y)} - f(X).$$

Observemos que $\quad q(X)\,|\,p(X)$ en $E[X] \quad \Longrightarrow \quad \overline{q}(X)\,|\,\overline{p}(X)$ en $K(y)[X]$.
Pero entonces

$$\widetilde{q}(y,X)\,|\,\widetilde{p}(y,X) \quad \text{en} \quad K[y,X]$$

donde $\widetilde{q}(y,X)$ y $\widetilde{p}(y,X)$ son los polinomios primitivos en $K[y][X]$ asociados a $\overline{q}(X)$ y $\overline{p}(X)$ (simplemente limpiamos denominadores).

<u>Afirmación:</u> $\quad \mathrm{gr}_X(\widetilde{p}) = \mathrm{gr}_y(\widetilde{p}) = n = \mathrm{gr}(p)$:

Se tiene $\widetilde{p}(y,X) = g(X)f(y) - f(X)g(y)$, y como es simétrico, $\mathrm{gr}_X(\widetilde{p}) = \mathrm{gr}_y(\widetilde{p})$, pero hay que ver que no se produce cancelación del monomio de grado n en X, que podría eventualmente pasar si fuera $\mathrm{gr}(f) = \mathrm{gr}(g) = n$.
En ese caso el coeficiente en grado n de X en $\widetilde{p}$ es $c_1 f(y) - c_2 g(y) \neq 0$, pues f y g coprimos. O sea que todo OK.

<u>Afirmación:</u> $\quad$ Más aún, $\widetilde{p} \in K[y,X]$ es primitivo, tanto como polinomio en y como polinomio en X:

Es facil ver que $\widetilde{p}$ es primitivo si $\mathrm{gr}(f) = 0$ o (excluyente) $\mathrm{gr}(g) = 0$ pues en esos casos,

$$\widetilde{p}(y,X) = a\big(g(X) - g(y)\big) \ \text{ o } \ a\big(f(y) - f(X)\big)$$

es "mónico" como polinomio en X (y en y).
Por lo tanto, podemos asumir $\mathrm{gr}(f), \mathrm{gr}(g) \geq 1$.
Al ser simétrico, si no es primitivo en X, tampoco lo es en y.
Sup. entonces que h es tal que $\widetilde{p}(y,X) = g(X)f(y) - f(X)g(y) = h(y)h(X)\widetilde{h}(y,X)$.
Sean $x_1, x_2 \in \overline{K}$ tq $f(x_1) = 0$ y $g(x_1) \neq 0$, y $f(x_2) \neq 0$ y $g(x_2) = 0$ (que existen por ser coprimos f y g).
Entonces

$$h(y)h(x_1)\widetilde{h}(y,x_1) = g(x_1)f(y) \quad \text{y} \quad h(y)h(x_2)\widetilde{h}(y,x_2) = -f(x_2)g(y).$$

Esto implica $h(y)\,|\,f(y)$ y $h(y)\,|\,g(y)$ que son coprimos,
y por lo tanto h es constante.

<u>Afirmación:</u> $\quad \mathrm{gr}_y(\widetilde{q}) = n$:

Se tiene $\widetilde{q}(y,X) = \widetilde{g}(y)X^m + \widetilde{f}_{m-1}(y)X^{m-1} + \cdots + \widetilde{f}_0(y)$

donde $\widetilde{g} = \mathrm{mcm}(g_{m-1}, \dots, g_0)$ y $f_k(y) \,|\, \widetilde{f}_k(y)$ para $0 \le k \le m-1$.
Por lo tanto $\mathrm{gr}_y(\widetilde{q}) \ge n$ pues si existe k tq $\mathrm{gr}(g_k) \ge n$, ent. $\mathrm{gr}(\widetilde{g}) \ge n$
y si no, existe k tq $\mathrm{gr}(f_k) \ge n$, lo que implica $\mathrm{gr}(\widetilde{f}_k) \ge n$.
Pero por otro lado, $\widetilde{q} \,|\, \widetilde{p}$ en $K[y, X]$ implica $\mathrm{gr}_y(\widetilde{q}) \le \mathrm{gr}_y(\widetilde{p}) = n$.
Así, $\mathrm{gr}_y(\widetilde{q}) = n$.

<u>Objetivo final:</u> Probar que $m = n$, o sea probar que $\mathrm{gr}_X(\widetilde{p}) = \mathrm{gr}_X(\widetilde{q})$ ya que

$$m = \mathrm{gr}(q) = \mathrm{gr}_X(\overline{q}) = \mathrm{gr}_X(\widetilde{q}) \quad \text{y} \quad n = \mathrm{gr}(p) = \mathrm{gr}_X(\widetilde{p}).$$

Pero como $\mathrm{gr}_y(\widetilde{q}) = \mathrm{gr}_y(\widetilde{p})$ y $\widetilde{q} \,|\, \widetilde{p}$ en $K[y, X]$, $\widetilde{p}(y, X) = h(X)\widetilde{q}(y, X)$,
o sea $h(X)$ divide al contenido de $\widetilde{p}(y, X)$ como polinomio en y,
pero ya vimos que $\widetilde{p}(y, X)$ es primitivo como polinomio en y,
y por lo tanto $h(X)$ es constante,
y concluimos ¡finalmente! que $\mathrm{gr}_X(\widetilde{p}) = \mathrm{gr}_X(\widetilde{q})$ como queríamos.

■