Álgebra III - 2do C. 2020 - Clase 21 - 17/11/2020

Finalicemos esta sección con un importante teorema de extensiones cíclicas, conocido como el teorema 90 de Hilbert.

De Wikipedia: *El nombre viene de que es el teorema 90 en el famoso Zahlbericht de David Hilbert, 1897, aunque es originalmente debido a Kummer (1855, 1861). Frecuentemente se menciona también con ese nombre un teorema más general de Emmy Noether (1933) sobre el primer grupo de cohomología de extensiones Galois finitas.*

Teorema 13.7.8 (Teorema 90 de Hilbert)
Sea E/K Galois finita y cíclica*, con* $\mathrm{Gal}(E/K) = \langle\sigma\rangle$ *de orden* n*, y sea* $\beta \in E$*. Entonces*

1. $\mathrm{Tr}_{E/K}(\beta) = 0 \iff \exists\, \alpha \in E \quad tq \quad \beta = \alpha - \sigma(\alpha)$ *(Forma aditiva).*
2. $\mathrm{N}_{E/K}(\beta) = 1 \iff \exists\, \alpha \in E^\times \quad tq \quad \beta = \dfrac{\alpha}{\sigma(\alpha)}$ *(Forma multiplicativa).*

Prueba.–
(1) $(\Leftarrow)$ $\mathrm{Tr}_{E/K}(\beta) = \mathrm{Tr}_{E/K}(\alpha) - \mathrm{Tr}_{E/K}(\sigma(\alpha)) = 0$.
$(\Rightarrow)$ Como E/K es separable, $\mathrm{Tr}_{E/K} \neq 0$: $\exists\, \gamma \in E$ tq $\mathrm{Tr}_{E/K}(\gamma) \neq 0$.
Definamos

$$\alpha = \frac{\beta\sigma(\gamma) + \big(\beta + \sigma(\beta)\big)\sigma^2(\gamma) + \cdots + \big(\beta + \cdots + \sigma^{n-2}(\beta)\big)\sigma^{n-1}(\gamma)}{\mathrm{Tr}_{E/K}(\gamma)}.$$

Entonces,

$$\sigma(\alpha) = \frac{\sigma(\beta)\sigma^2(\gamma) + \big(\sigma(\beta) + \sigma^2(\beta)\big)\sigma^3(\gamma) + \cdots + \big(\sigma(\beta) + \cdots + \sigma^{n-1}(\beta)\big)\sigma^n(\gamma)}{\mathrm{Tr}_{E/K}(\sigma(\gamma))}.$$

Pero $o(\sigma) = n \;\Rightarrow\; \sigma^n = \mathrm{id}$ y $\mathrm{Tr}_{E/K}(\beta) = 0 \;\Rightarrow\; \sigma(\beta) + \cdots + \sigma^{n-1}(\beta) = -\beta$.
Así, como además $\mathrm{Tr}_{E/K}(\sigma(\gamma)) = \mathrm{Tr}_{E/K}(\gamma)$, se tiene

$$\sigma(\alpha) = \frac{\sigma(\beta)\sigma^2(\gamma) + \big(\sigma(\beta) + \sigma^2(\beta)\big)\sigma^3(\gamma) + \cdots \big(\sigma(\beta) + \cdots + \sigma^{n-2}(\beta)\big)\sigma^{n-1}(\gamma) - \beta\gamma}{\mathrm{Tr}_{E/K}(\gamma)},$$

y

$$\begin{aligned}\alpha - \sigma(\alpha) &= \frac{\beta\big(\sigma(\gamma) + \cdots + \sigma^{n-1}(\gamma)\big) + \beta\gamma}{\mathrm{Tr}_{E/K}(\gamma)} \\ &= \frac{\beta\mathrm{Tr}_{E/K}(\gamma)}{\mathrm{Tr}_{E/K}(\gamma)} \;=\; \beta\end{aligned}$$

(2) $(\Leftarrow)$ $\mathrm{N}_{E/K}(\beta) = \dfrac{\mathrm{N}_{E/K}(\alpha)}{\mathrm{N}_{E/K}(\sigma(\alpha))} = 1\,.$

$(\Rightarrow)$ Como $1, \sigma, \ldots, \sigma^{n-1}$ son automorfismos distintos, por independencia lineal de caracteres, sea $\gamma \in E$ tal que

$$\begin{aligned}\alpha :&= \big(\mathrm{id}_E + \beta\sigma + \beta\sigma(\beta)\sigma^2 + \cdots + \beta\sigma(\beta)\cdots\sigma^{n-2}(\beta)\sigma^{n-1}\big)(\gamma)\\ &= \gamma + \beta\sigma(\gamma) + \beta\sigma(\beta)\sigma^2(\gamma) + \cdots + \beta\sigma(\beta)\cdots\sigma^{n-2}(\beta)\sigma^{n-1}(\gamma) \;\neq\; 0.\end{aligned}$$

Entonces,

$$\sigma(\alpha) = \sigma(\gamma) + \sigma(\beta)\sigma^2(\gamma) + \sigma(\beta)\sigma^2(\beta)\sigma^3(\gamma) + \cdots + \sigma(\beta)\sigma^2(\beta)\cdots\sigma^{n-1}(\beta)\sigma^n(\gamma)$$

Pero $o(\sigma) = n \;\Rightarrow\; \sigma^n = \mathrm{id}$ y $\mathrm{N}_{E/K}(\beta) = 1 \;\Rightarrow\; \sigma(\beta)\cdots\sigma^{n-1}(\beta) = \dfrac{1}{\beta}\,.$

Así,

$$\beta\sigma(\alpha) = \beta\sigma(\gamma) + \beta\sigma(\beta)\sigma^2(\gamma) + \cdots + \beta\sigma(\beta)\cdots\sigma^{n-2}(\beta)\sigma^{n-1}(\gamma) + \gamma = \alpha,$$

y por lo tanto $\beta = \dfrac{\alpha}{\sigma(\alpha)}\,.$

■

Como aplicación del teorema 90 de Hilbert, obtenemos una suerte de generalización para cualquier cuerpo de característica p del hecho que $\mathbb{F}_{p^p} = \mathbb{F}_p(\theta)$ donde $f(\theta, \mathbb{F}_p) = X^p - X - a\,,\ a \in \mathbb{F}_p^{\times}\,.$

Corolario 13.7.9
Sea K con $\mathrm{car}(K) = p$ y sea E/K Galois finita con $[E:K] = p\,.$
Entonces existe $\alpha \in E$ tal que $E = K(\alpha)$
y $f(\alpha, K) = X^p - X - a$ para algún $a \in K\,.$

Prueba.–
$[E:K] = p \;\Rightarrow\; \mathrm{Gal}(E/K) = \langle\sigma\rangle$ cíclica de orden $p\,.$
Observemos que para $\beta = -1\,,\ \mathrm{Tr}_{E/K}(\beta) = \underbrace{-1 - \cdots - 1}_{p} = 0$ en $E\,,$ y por lo tanto,
por el teorema 90 de Hilbert, existe $\alpha \in E$ tal que $-1 = \beta = \alpha - \sigma(\alpha)\,,$
o sea $\sigma(\alpha) = \alpha + 1\,.$ Lo que implica $\sigma^k(\alpha) = \alpha + k\,.$
Y como $o(\sigma) = p\,,\ \sigma^k(\alpha) \neq \sigma^j(\alpha)$ para $0 \leq k \neq j < p$ y $\sigma^p(\alpha) = \alpha\,.$
Así, α es elemento primitivo y

$$\begin{aligned}f(\alpha, K) \;&=\; \prod_{0\leq k<p} \big(X - \sigma^k(\alpha)\big) \;=\; \prod_{0\leq k<p} \big(X - (\alpha + k)\big)\\ &= \prod_{0\leq k<p} \big((X-\alpha) - k\big) \;=\; (X-\alpha)^p - (X-\alpha) \;=\; X^p - X - \underbrace{\alpha^p - \alpha}_{a} \;\in\; K[X]\end{aligned}$$

■

14 Extensiones trascendentes (o no algebraicas)

Recuerdo: Sea E/K extensión de cuerpos.
Se dice que $t \in E$ es *trascendente sobre* K si

$$f(t) = 0 \text{ con } f \in K[X] \implies f = 0 \text{ en } K[X].$$

En ese caso,

$$K(t) = \left\{ \frac{f(t)}{g(t)},\ f, g \in K[X] \right\} \text{ cuerpo} \quad \neq \quad K[t] = \{ f(t),\ f \in K[X] \} \text{ anillo.}$$

Se tiene

$$t \text{ trascendente}/K \iff K[t] \subsetneq K(t) \iff [K(t) : K] = \infty$$

Para la primera equivalencia: $(\Rightarrow)$ $\frac{1}{t} \notin K[t]$ pues sino $1 - tf(t) = 0$ ...
y t algebraico$/K \Rightarrow K[t] = K(t)$.
Para la otra equivalencia: $(\Rightarrow)$ $1, t, \ldots, t^n, \ldots$ son l.i.$/K$
y si t es algebraico$/K$, ent. $[K(t) : K] < \infty$.

■

Entremos ahora en las extensiones trascendentes.

Definición 14.0.1 (Extensión trascendente (o no algebraica))
Se dice que una extensión E/K es trascendente *(o* no algebraica*) cuando existe $t \in E$ tal que t es trascendente$/K$.*
(Ojo que eso no significa que todos los elementos de E son trascendentes$/K$: alcanza con uno.)

Observación 14.0.2 *E/K trascendente $\implies [E : K] = \infty$,*
Pero puede haber muchos elementos en E que son algebraicamente independientes*...*

Definición 14.0.3 (Dependencia algebraica/ Independencia algebraica)
Sea E/K extensión de cuerpos, y $T \subset E$.

- *Se dice que T es* algebraicamente dependiente$/K$ *si existen $t_1, \ldots, t_N \in T$ (distintos) y $f \in K[X_1, \ldots, X_n]$* no nulo *tq $f(t_1, \ldots, t_N) = 0$.*

- *Se dice que* T *es* algebraicamente independiente sobre$/K$ *si no es algebraicamente dependiente*$/K$.

  Es decir,

  $$\forall\, N \in \mathbb{N},\ f(t_1,\dots,t_N)=0 \text{ para } f \in K[X_1,\dots,X_N] \text{ y } \underbrace{\{t_1,\dots,t_N\}}_{\neq} \subset T \ \Rightarrow\ f=0.$$

Ejemplo $\mathbb{Q}(\sqrt{\pi},\pi+1)/\mathbb{Q}$
Tanto $\sqrt{\pi}$ y $2\pi+1$ son trascendentes$/\mathbb{Q}$ (Teorema de Lindemann, 1882), pero son alg.dep.$/\mathbb{Q}$ pues $f=2X^2-Y+1$ se anula en $X\mapsto\sqrt{\pi}$ e $Y\mapsto 2\pi+1$.

Observación 14.0.4

1. t *trascendente*$/K \iff \{t\}$ *alg.indep.*$/K$.
2. $T\subset E$ *alg.indep.*$/K \iff \forall\, S\subset T,\ S$ *alg.indep.*$/K$.
3. $T\neq\emptyset$ *alg.indep.*$/K \implies \forall\, t\in T,\ t$ *trasc.*$/K$.
   (La recíproca no vale como muestra el ejemplo anterior.)
4. T *alg.indep.*$/K$ *y* t *trasc.*$/K(T) \iff T\cup\{t\}$ *alg.indep.*$/K$.
5. T *alg.indep.*$/K \iff \forall\, t\in T,\ t$ *trasc.*$/K(T\setminus\{t\})$.

Prueba.–
(1), (2) y (3) son directos, así que los dejamos al lector.
(4) ($\Rightarrow$) Sea $f\in K[X_1,\dots,X_N]$ tq $f(t_1,\dots,t_N)=0$ con $\{t_1,\dots,t_N\}\subset T\cup\{t\}$.
Y sea $\boldsymbol{t'}=\{t_1,\dots,t_N\}-\{t\}$ (eventualmente $\boldsymbol{t'}=(t_1,\dots,t_N)$ si t no aparece).

Escribamos $f(\boldsymbol{t'},t)=f_n(\boldsymbol{t'})t^n+\cdots+f_0(\boldsymbol{t'})=0$

Si $n=0$, $f=0$ por ser T alg.indep.$/K$.
Si $n>0$, como t es trasc.$/K(T)$, $f_n(\boldsymbol{t'})=\cdots=f_0(\boldsymbol{t'})=0$.
Lo que implica $f_n=\cdots=f_0=0$ pues T alg.indep.$/K$.
Y por lo tanto $f=0$.

($\Leftarrow$) T alg.indep.$/K$ pues $T\cup\{t\}$ alg.indep.$/K$.
Solo falta probar que t es trasc.$/K(T)$:
Sup. $\exists\, f\in K(T)[X]$ tq $f(t)=0$. Entonces existe $\boldsymbol{t}=(t_1,\dots,t_N)\subset T$ tq

$$f = \frac{a_n(\boldsymbol{t})X^n + \cdots + a_0(\boldsymbol{t})}{a(\boldsymbol{t})} \quad \Rightarrow \quad 0 = f(t) = a_n(\boldsymbol{t})t^n + \cdots + a_0(\boldsymbol{t}).$$

Por lo tanto, notando $\boldsymbol{X} = (X_1, \ldots, X_n)$, el polinomio

$$g = a_n(\boldsymbol{X})X^n + \cdots + a_0(\boldsymbol{X}) = \sum_{\boldsymbol{j},k} b_{\boldsymbol{j},k}\boldsymbol{X}^{\boldsymbol{j}}X^k$$

se anula en $\{t_1, \ldots, t_n, t\} \subset T \cup \{t\}$ alg.indep./K.
Esto implica $g = 0$, es decir $b_{\boldsymbol{j},k} = 0$, $\forall\, \boldsymbol{j}, k$, y por lo tanto $f = 0$.
(5) ($\Rightarrow$) Sea $T' = T \setminus \{t\}$: $T' \cup \{t\}$ alg.indep./K $\Rightarrow$ t trasc./$K(T')$ por (4).

($\Leftarrow$) Por contrarrecíproca: Si T es alg.dep./K, existen $t_1, \ldots, t_N \in T$ y $f \in K[X_1, \ldots, X_N]$ no nulo tq $f(t_1, \ldots, t_N) = 0$.
Sea X_i alguno que aparece en el polinomio: ent. t_i es alg./$K(T \setminus \{t_i\})$.

■

14.1 Bases de trascendencia

Motivación

Sea E/K una extensión *trascendente*, y sea

$$\mathcal{T} := \big\{T \subset E \,:\, T \text{ es algebraicamente independiente sobre } K\big\}.$$

Se tiene

- $\mathcal{T} \neq \emptyset$ pues existe $t \in E$ trascendente/K.
- $\mathcal{T}$ está parcialmente ordenado por inclusión.
- Toda cadena en $\mathcal{T}$ tiene cota superior:

  Si $\{T_i\}_{i\in I}$ es una cadena en $\mathcal{T}$, entonces $\cup_{i\in I}T_i$ es cota superior pues es alg.ind./K, ya que si f anula a finitos $t_i \in \cup T_i$, están todos en algún T_k.

Luego por el Lema de Zorn, $\mathcal{T}$ tiene elementos maximales, es decir

$$\exists\, T \in \mathcal{T} \text{ tq si } T \subset S \in \mathcal{T}, \text{ entonces } T = S.$$

Definición 14.1.1 (Base de trascendencia)
Sea E/K una extensión de cuerpos. Se dice que $T \subset E$ es una base de trascendencia de E/K *si T es maximal con la propiedad de ser algebraicamente independiente sobre K.*

Observación 14.1.2

- *Una base de trascendencia, eventualmente vacía, existe por la motivación.*
- $T = \emptyset \iff E/K$ *algebraica.*

Proposición 14.1.3 (Caracterización de base de trascendencia)
Sea E/K *una extensión de cuerpos y sea* $T \subset E$. *Entonces*

$$T \text{ es base de trasc. de } E/K \iff T \text{ es alg.ind./}K \text{ y } E/K(T) \text{ es algebraica.}$$

Prueba.–
$(\Rightarrow)$ T es alg.ind./K por def.
Sup. $\exists\, t \in E \setminus K(T)$ tq t es trasc./$K(T)$.
Entonces $T \cup \{t\}$ es alg.ind./K.
Esto contradice la maximalidad de T.
O sea $E/K(T)$ es algebraica.

$(\Leftarrow)$ Qpq en esas condiciones T es maximal con la propiedad de ser alg.ind./K.
Sup. $T \subsetneq S \subset E$, y sea $\alpha \in S \setminus T$.
Entonces α es alg./$K(T)$, lo que implica $T \cup \{\alpha\}$ alg.dep./K.
O sea S es alg.dep/K.

■

Definición-Proposición 14.1.4 (Grado de trascendencia)
Sea E/K *una extensión de cuerpos. Entonces*

1. *E admite una base de trascendencia sobre K (eventualmente vacía si E/K alg.)*
2. *Más aún, todo conjunto $T' \subset E$ alg.ind./K se puede extender a una base de trascendencia T de E/K.*
3. *Dos bases de trasendencia de E/K tienen el mismo cardinal, que se llama* grado de trascendencia de E/K, *y se nota*

$$\mathrm{trdeg}(E/K) \quad o \quad \mathrm{trdeg}_K(E).$$

Prueba.–
Ya vimos (1) y (2) es igual que (1) empezando con $\mathcal{T} = \{S \text{ alg.ind./}K \text{ con } T' \subset S\}$.
(3) Sean S, T dos bases de trascendencia de E/K.

(a) Supongamos primero que $\#T < \infty$: hacemos inducción en $\#(T \setminus S)$.
– Si $T \setminus S = \emptyset$, es decir $T \subset S$, entonces $T = S$ por ser maximal.
– Si $\#(T \setminus S) \geq 1$, vamos a ir reemplazando elementos de S por elementos de T:
Existe $t \in T \setminus S$ y por lo tanto $S \cup \{t\}$ es alg.dep./K.
Entonces existe f pol. no nulo que involucra a t (pues S es alg.ind./K)
y a eltos $\boldsymbol{s}$ de S que incluyen por lo menos un elto $s \in S \setminus T$ (pues T es alg.ind./K)
tq $f(\boldsymbol{s}, t) = 0$.
Así s es alg./$K(S_1)$ donde $S_1 := (S \setminus \{s\}) \cup \{t\}$.
Probemos que S_1 es base de trascendencia de E/K, y así podemos seguir la recurrencia:
- S_1 es alg.ind./K pues $S \setminus \{s\}$ es alg.indep./K y t es trasc./$K(S \setminus \{s\})$,
ya que si fuera t alg./$K(S \setminus \{s\})$, como s es alg./$K(S_1)$, s sería alg./$K(S \setminus \{s\})$, contradicción.
Luego S_1 es alg.ind./K.
- Probemos que $E/K(S_1)$ es algebraica (así aplicamos la proposición 14.1.3):

$$\begin{array}{c} E \\ | \\ K(S_1)(s) \\ | \\ K(S_1) \end{array}$$

O sea S_1 es base de trascendencia de E/K y $\#(T - S_1) = \#(T - S) - 1$.
Por lo tanto, por HI, se concluye $\#(T) = \#(S_1) = \#(S)$.

(b) Sean ahora $\#(S) = \#(T) = \infty$.
Esto es por cuestiones de cardinalidad (lo mismo que para demostrar que las bases de e.v. tienen mismo cardinal).
$S = \{s_i\}_{i \in I}$ y $T = \{t_j\}_{j \in J}$.
Cada s_i es algebraico/$K(T)$: cada s_i es raíz de un polinomio f_i que involucra finitos t_j.
Sea $T' = \{t_j : t_j \text{ aparece en algún } f_i,\ i \in I\}$. Entonces $\#(T') \leq \aleph_0 \#(S) = \#(S)$.
Probemos que $T' = T$: pues si existe $t \in T \setminus T'$, entonces t no es necesario, es decir S es alg./$K(T \setminus \{t\})$ pero t alg./$K(S)$, así t alg./$K(T \setminus \{t\})$. Contradicción.
Se concluye $\#(T) \leq \#(S)$ y recíprocamente.

■

Ejemplo

$$\mathrm{trdeg}_K(K(X_1, \ldots, X_n)) = n.$$