Álgebra III - 2do C. 2020 - Clase 18 - 6/11/2020

13 Extensiones algebraicas arbitrarias

13.1 Recuerdo extensiones separables

- E/K es *separable* si $\forall\, \alpha \in E$, se tiene que α es separable $/K$.

  Es decir, equivalentemente

  - $f(\alpha, K)$ tiene solo raíces simples en $\overline{K}$ $\ (\operatorname{mcd}(f, f') = 1)$
  - α es raíz de un polinomio no nulo con raíces simples
  - $[K(\alpha) : K] = \#\{\sigma : K(\alpha) \underset{K}{\hookrightarrow} \overline{K}\} = \#\operatorname{Hom}(K(\alpha)/K, \overline{K}/K)$

- E/K es *separable finita* $\iff$ $[E : K] = \#\operatorname{Hom}(E/K, \overline{K}/K)$

  Y en ese caso E/K es simple: existe $\theta \in E$ (separable $/K$) tq $E = K(\theta)$.

- Sea $f \in K[X]$ *irreducible* de grado n.

  Entonces si $\operatorname{car}(K) = 0$ o $\operatorname{car}(K) = p \nmid n$, f es separable.

- O sea si queremos extensiones *algebraicas* con elementos no separables, tenemos que buscar extensiones algebraicas de K con $\operatorname{car}(K) = p$ con p primo.

  Pero si E es cuerpo finito, entonces $\operatorname{car}(K) = p$ para algún p y $E/\mathbb{F}_p$ es una extensión separable pues

  $$E/\mathbb{F}_p = \mathbb{F}_p(X^{p^n} - X)$$

  para algún $n \in \mathbb{N}$, donde $X^{p^n} - X$ es separable.

  Por lo tanto E es separable también sobre cualquiera de sus subextensiones.

  Pasa lo mismo si $E/\mathbb{F}_p$ es algebraica pues cada elemento $\alpha \in E$ es separable $/K$.

Conclusión:

Las extensiones algebraicas de K con $\operatorname{car}(K) = 0$ o K cuerpo finito son todas separables

---

13.2 Ejemplos de extensiones algebraicas no separables

- Ejemplo de extensión algebraica no separable:

  Sea $K = \mathbb{F}_p(t)$ con t trascendente $/\mathbb{F}_p$,

  y sea $E = K(\sqrt[p]{t})$.

  Entonces E/K es algebraica

  pero E/K no es separable pues

  $f(\sqrt[p]{t}, K) = X^p - t = (X - \sqrt[p]{t})^p$.

  Notar que $[E : K] = p$ pero $\mathrm{Hom}(E/K, \overline{K}/K) = \{\mathrm{id}_E\}$.

- Ejemplo de extensión finita no separable y no simple:

  Recordemos que E/K simple $\Leftrightarrow$ E/K tiene finitas subextensiones.

  Sean t, u variables independientes sobre $\mathbb{F}_p$.

  Sea $K = \mathbb{F}_p(t, u)$ y $E = K(\sqrt[p]{t}, \sqrt[p]{u})$.

  Sean las subextensiones

  $F := K(\sqrt[p]{t})$ y $L := K(\sqrt[p]{u})$

  ¿Cómo es $X^p - u$ en $F[X]$?

  Por lo tanto $[E : K] =$

  Probemos que E/K tiene infinitas subextensiones:

  ¿Candidatos?

  Sea $\alpha_k := \sqrt[p]{t} + t^k \sqrt[p]{u} \ \in E$.

  Entonces

  - $\alpha_k \notin K$:

  - $K(\alpha_k) \neq E$ pues $\mathrm{gr}(f(\alpha_k, K)) \leq p$:

    $$\alpha_k^p =$$

  - $K(\alpha_k) \neq K(\alpha_j)$ para $k \neq j$:

13.3 Caracterización de extensiones algebraicas separables

Sea K cuerpo infinito con $\operatorname{car}(K) = p$. ¿Cuándo E/K algebraica es separable?

Definición 13.3.1 (Cuerpo perfecto)
Se dice que K es un cuerpo perfecto *si*

- $\operatorname{car}(K) = 0$, *o*
- $\operatorname{car}(K) = p$ *y se cumple una de las dos equivalencias siguientes*
  - $K^p = K$, *(donde notamos que $K^p = \{a^p : a \in K\} \subset K$ es un cuerpo pues $\operatorname{car}(K) = p$.)*
  - *el morfismo de Frobenius $\Phi_p : a \mapsto a^p$ es un automorfismo de K.*

Ejemplo
Un cuerpo K con $\operatorname{car}(K) = p$ algebraico sobre $\mathbb{F}_p$ es perfecto.

Observación 13.3.2 (Extensiones algebraicas de cpos perfectos son separables)
Sea K un cuerpo perfecto y sea E/K algebraica, entonces E/K es separable.

Prueba.–
Alcanza hacerla para $\operatorname{car}(K) = p$ porque ya sabemos que si $\operatorname{car}(K) = 0$, E/K es separable.
Supongamos que $f = X^n + a_1X^{n_1} + \cdots + a_{k-1}X^{n_{k-1}} + a_k \in K[X]$ candidato a irreducible es no separable, donde $a_j \neq 0$, $\forall\, j$.
Entonces $f' = 0$, i.e. $p \mid n, p \mid n_1, \ldots, p \mid n_{k-1}$, o sea

$$f = X^{pm} + a_1X^{pm_1} + \cdots + a_{k-1}X^{pm_{k-1}} + a_k = (X^m + b_1X^{m_1} + \cdots + b_{k-1}X^{m_{k-1}} + b_k)^p$$

para $b_j \in K$ tal que $a_j = b_j^p$ dado que K es perfecto.
O sea f no puede ser irreducible.

■

Pero esto es pedir un poco mucho. Hay una condición un poco más debil que ser perfecto q garantiza separabilidad, al menos de una E/K dada.

Proposición 13.3.3 (Extensiones algebraicas separables)
Sea K cuerpo con $\operatorname{car}(K) = p$. Entonces

1. *E/K separable $\Longrightarrow$ $E = KE^p$*
2. *E/K finita y $E = KE^p$ $\Longrightarrow$ E/K separable.*

Observación 13.3.4 (Extensiones algebraicas de cpos perfectos son perfectas)
Sea K tq $K = K^p$ y E/K es algebraica. Entonces $E = E^p$.
Esto vale pues por un lado $K = K^p \subset E^p$, o sea E^p es extensión de K,
y al ser E separable$/K$, lo que implica separable$/E^p$,
se tiene que dado $\alpha \in E$, $\alpha^p \in E^p$:

$$f(\alpha, E^p) \mid X^p - \alpha^p = (X-\alpha)^p \underset{\alpha\ sep/K}{\Longrightarrow} f(\alpha, E^p) = X - \alpha \quad \Longrightarrow \quad \alpha \in E^p.$$

■

Prueba de la proposición 13.3.3.–
(1) Qpq $\alpha \in E \ \Rightarrow \ \alpha \in KE^p$ (donde $K \subset KE^p \subset E$)
Pero $\alpha \in E \ \Rightarrow \ \alpha^p \in E^p$:
α es raíz de $X^p - \alpha^p = (X-\alpha)^p \in E^p[X] \subset KE^p[X]$,
y α separable$/K \ \Rightarrow \ \alpha$ separable$/KE^p$.
Por lo tanto $f(\alpha, KE^p) \mid (X-\alpha)^p \ \Rightarrow \ f(\alpha, KE^p) = X - \alpha$,
O sea $\alpha \in K\,E^p$.

(2) Sea E/K finita y supongamos que $E = KE^p$ pero es no separable $/K$.
Lleguemos a un absurdo.
O sea existe $\alpha \in E$ no separable$/K$:

$$f(\alpha, K) = X^{pm} + a_{m-1}X^{p(m-1)} + \cdots + a_1 X^p + a_0 \ \in \ K[X]$$

donde al menos $a_0 \neq 0$. Esto implica que $\{1, \alpha^p, \ldots, (\alpha^{m-1})^p, (\alpha^m)^p\}$ es ld$/K$.
Probemos que si $E = KE^p$, esto implica que $\{1, \alpha, \ldots, \alpha^m\}$ son ld$/K$, con lo cual f no es irreducible.

Probaremos en realidad que si $E = KE^p$, entonces

$$\{\alpha_1, \ldots, \alpha_d\} \text{ base de } E/K \quad \Longrightarrow \quad \{\alpha_1^p, \ldots, \alpha_d^p\} \text{ base de } E/K:$$

Sea $\alpha \in E$: $\alpha = a_1\alpha_1 + \cdots + a_d\alpha_d$ con $a_1, \ldots, a_d \in K$.
Entonces $\alpha^p = a_1^p\alpha_1^p + \cdots + a_d^p\alpha_d^p$.
O sea KE^p está generado sobre K por $\{\alpha_1^p, \ldots, \alpha_d^p\}$.
Pero $E = KE^p$, o sea E está generado sobre K por $\{\alpha_1^p, \ldots, \alpha_d^p\}$,
y por lo tanto $\{\alpha_1^p, \ldots, \alpha_d^p\}$ es base por tener la buena dimensión.

■

13.4 Polinomios irreducibles en característica p

Proposición 13.4.1 (Polinomios irreducibles en característica p)
Sea K con $\operatorname{car}(K) = p$ y $f \in K[X]$ irreducible.
Entonces existe $e \geq 0$ y $g \in K[X]$ irreducible *y* separable *tal que*

$$f(X) \;=\; g(X^{p^e})$$

Prueba.–
Sea $e \in \mathbb{N}_0$ tq p^e es la máxima potencia de p que divide a todos los exponentes de f (de monomios que aparecen con coeficiente no nulo obviamente). O sea

$$f = X^{p^e m_d} + a_{d-1}X^{p^e m_{d-1}} + \cdots + a_1 X^{p^e m_1} + a_0 \quad \in K[X]$$

donde $a_{d-1}, \ldots, a_0$ no nulos, $m_d > m_{d-1} > \cdots > m_1 > 0$ y $p \nmid m_i$ para algún i, $0 \leq i \leq d$.
Sea

$$g(X) = X^{m_d} + a_{d-1}X^{m_{d-1}} + \cdots + a_1 X^{m_1} + a_0 \quad \in K[X].$$

Entonces

- $f(X) = g(X^{p^e})$
- g es irreducible pues si no lo fuera,

$$g = h_1 h_2 \;\Rightarrow\; f(X) = g(X^{p^e}) = h_1(X^{p^e})h_2(X^{p^e}) \;\text{ reducible}$$

- g es separable pues $g' = m_d X^{m_d - 1} + m_{d-1}a_{d-1}X^{m_{d-1}-1} + \cdots + m_1 a_1 X^{m_1 - 1} \neq 0$ dado que $p \nmid m_i$ para algún i.

■

Corolario 13.4.2 (Factorización de polinomios irreducibles en característica p)
Sea K con $\operatorname{car}(K) = p$ y $f \in K[X]$ irreducible.
Entonces existe $e \geq 0$ tal que

$$f \;=\; \big((X - \alpha_1)\cdots(X - \alpha_r)\big)^{p^e} \quad \textit{con } \alpha_i \in \overline{K} \;\; \textit{distintos entre sí.}$$

En particular todas las raíces de f en $\overline{K}$ tienen la misma multiplicidad, que es una potencia de p.

Prueba.–
Sea $g=(X-\beta_1)\cdots(X-\beta_r)$, con $\beta_1,\dots,\beta_r\in\overline{K}$ distintos (por ser separable) tal que $f(X)=g(X^{p^e})$. Entonces,

$$\begin{aligned} f &= (X^{p^e}-\beta_1)\cdots(X^{p^e}-\beta_r) = (X^{p^e}-\alpha_1^{p^e})\cdots(X^{p^e}-\alpha_r^{p^e}) \\ &= (X-\alpha_1)^{p^e}\cdots(X-\alpha_r)^{p^e} = \big((X-\alpha_1)\cdots(X-\alpha_r)\big)^{p^e} \end{aligned}$$

donde para $1\le i\le r$, $\alpha_i\in\overline{K}$ es tal que $\alpha_i^{p^e}=\beta_i$ son todos distintos.

■

Observación 13.4.3 (Casos extremos)

- $e=0 \iff f$ *separable (o sea* α *raíz de* f *es* separable*).*
- $r=1 \iff f=(X-\alpha)^{p^e}$ *(o sea* α *es* puramente inseparable*).*

13.5 Extensiones puramente inseparables

Definición 13.5.1 (Elementos y extensiones puramente inseparables)
Sea K *un cuerpo con* $\mathrm{car}(K)=p$*. Entonces*

- *Se dice que* $\alpha\in\overline{K}$ *es* puramente inseparable (p.i) *sobre* K *si* α *es la única raíz de* $f(\alpha,K)$*, o sea* $f(\alpha,K)=(X-\alpha)^{p^e}$ *para algún* $e\in\mathbb{N}_0$*.*
- *Sea* E/K *algebraica. Se dice que* E/K *es* puramente inseparable (p.i) *si* $\forall\,\alpha\in E$*,* α *es puramente inseparable sobre* K*.*

Observación 13.5.2

- *Sea* $\alpha\in\overline{K}$*. Entonces* α *es sep. y p.i. sobre* K *a la vez* $\Leftrightarrow$ $\alpha\in K$,

  pues α sep. $\Leftrightarrow$ $f(\alpha,K)=(X-\alpha_1)\cdots(X-\alpha_r)$

  y α p.i. $\Leftrightarrow$ $f(\alpha,K)=(X-\alpha)^{p^e}$.

  Lo que implica α sep. y p.i. sobre K a la vez $\Leftrightarrow$ $f(\alpha,K)=X-\alpha\in K[X]$
- E/K *sep. y p.i. a la vez* $\Leftrightarrow$ $E=K$*.*

- $\alpha \in \overline{K}$ *p.i.* $/K \iff \exists\, k \in \mathbb{N}_0$ *tq* $\alpha^{p^k} \in K$

  ($(\Rightarrow)$ α p.i. $/K \Rightarrow f(\alpha, K) = (X-\alpha)^{p^e} = X^{p^e} - \alpha^{p^e}$, o sea $\alpha^{p^e} \in K$.

  $(\Leftarrow)$ $\alpha^{p^k} \in K \Rightarrow f(\alpha, K) \mid X^{p^k} - \alpha^{p^k} = (X-\alpha)^{p^k}$,

  y por la pinta de los irreducibles de $K[X]$, eso fuerza a que $f(\alpha, K) = (X-\alpha)^{p^e}$ para algún $e \leq k \in \mathbb{N}_0$.)

- α *p.i.* $/K \Rightarrow f(\alpha, K) = (X-\alpha)^{p^e}$ *donde* $e := \min\{k : \alpha^{p^k} \in K\}$.

Proposición 13.5.3 (Elementos y extensiones p.i. y Hom)
Sea K *un cuerpo con* $\mathrm{car}(K) = p$. *Entonces*

1. *Sea* $\alpha \in \overline{K}$. *Entonces,* α *es p.i.* $/K \iff \mathrm{Hom}(K(\alpha)/K, \overline{K}/K) = \{\mathrm{id}_{K(\alpha)}\}$.
2. *Sea* E/K *alg. Entonces,* E/K *es p.i.* $\iff \mathrm{Hom}(E/K, \overline{K}/K) = \{\mathrm{id}_E\}$.

Prueba.–

1.

2. $(\Rightarrow)$ Sea $\alpha \in E$, $\sigma \in \mathrm{Hom}(E/K, \overline{K}/K) \rightsquigarrow \sigma|_{K(\alpha)} \in \mathrm{Hom}(K(\alpha)/K, \overline{K}/K)$.

   Como α es p.i. $/K$, $\sigma|_{K(\alpha)} = \mathrm{id}_{K(\alpha)}$, i.e. $\sigma(\alpha) = \alpha$.

   $(\Leftarrow)$ Sea $\alpha \in E$ y $\psi \in \mathrm{Hom}(K(\alpha)/K, \overline{K}/K)$.

   Entonces ψ es la restricción de algún $\sigma \in \mathrm{Hom}(E/K, \overline{K}/K) = \{\mathrm{id}_E\}$.

   Por lo tanto, $\psi = \mathrm{id}_{K(\alpha)}$, o sea α es p.i. $/K$.

$\blacksquare$

Corolario 13.5.4
Sea $\alpha \in \overline{K}$. *Entonces,* α *p.i.* $/K \iff K(\alpha)/K$ *p.i.*

$\blacksquare$