Álgebra

Ignacio Cordón Castillo

Extensiones separables

Definición. ***Elemento separable***

Un elemento algebraico u sobre un cuerpo K se llama separable si $Irr(u, K)$ no tiene raíces múltiples.

Definición. ***Extensión separable***

Una extensión algebraica F/K se llama separable si todo elemento de F es separable sobre K.

Proposición 1. ***Torres separables***

Sea $E \supset F \supset K$ torre de cuerpos tal que E/K es extensión separable. Entonces E/F y F/K son extensiones separables.

F/K es separable, por tener menos elementos que E. E/F es separable porque $Irr(u, F)|Irr(u, K)$ y $Irr(u, K)$ no tiene raíces múltiples, luego $Irr(u, F)$ tampoco.

Pongamos un ejemplo de cuerpo normal no separable.

$$\mathbb{Z}_p(t^p)(t) \supset \mathbb{Z}_p(t^p)$$

con p primo y t trascendente sobre $\mathbb{Z}_p$

Tenemos que es extensión normal, por tenerse que $\mathbb{Z}_p(t^p)(t)$ es cuerpo de descomposición de $(X^p - t^p) = (X - t)^p$.

Y no es separable puesto que $4Irr(t, \mathbb{Z}_p) = (X - t)^p$ con raíces repetidas. Para demostrar esto último, supongamos $gr(Irr(t, \mathbb{Z}_p)) = m < p$. Entonces se tendría $(X - t)^m = \mathrm{f(t^p)\$}$, lo que negaría que t fuera transitivo sobre $\mathbb{Z}_p$

Definición. ***Grado separable***

Sea una torre de cuerpos

$$\bar{K} \supset F \supset K$$

donde $\bar{K}$ es una clausura algebraica de K

LLamamos ***grado separable*** *de F sobre K al conjunto:*

$$[F : K]_s = |\{\sigma : F/K \to \bar{K}/K \quad homomorfismo\}|$$

Proposición 2. ***Grado separable de una torre de cuerpos***

$$\bar{K} \supset E \supset F \supset K$$

donde $\bar{K}$ es una clausura algebraica de K. Entonces:

$$[E : K]_s = [E : F]_s [F : K]_s$$

Proposición 3. *Sea F/K* ***extensión finita****. Entonces $[F : K]_s$ divide a $[F : K]$.*

Proposición 4. ***Caracterización de separabilidad***

Sea E/K ***extensión finita****. La extensión E/K es separable si y sólo si $[E : K]_s = [E : K]$*

Por inducción sobre el grado de la extensión. Si $[E : K] = 1$ se cumple trivialmente.

Supuesto cierto para extensiones de hasta grado $n - 1$:

Si E/K es separable debe tenerse $E/K(u), K(u)/K$ separables y por hipótesis de inducción

$$[E:K] = [E:K(u)][K(u):K] = [E:K(u)]_s[K(u):K]_s = [E:K]_s$$

Supuesto $[E:K]_s = [E:K]$ entonces dado $u \in F \setminus K$,

$[E:K(u)][K(u):K] = [E:K(u)]_s[K(u):K]_s$ y por la proposición anterior $[E:K(u)]_s \leq [E:K(u)]$ y $[K(u):K]_s \leq [K(u):K]$ deberíamos tener la igualdad

Entonces $Irr(u,K)$ no podría tener raíces múltiples, porque en ese caso el grado de separabilidad sería menor que $[K(u):K]$ porque tendríamos menos formas de permutar las raíces para obtener homomorfismos $K(u)/K \to \bar{K}/K$ distintos.

Luego todo polinomio irreducible sobre K tiene raíces únicas.

Proposición 5. *Sea $E \supset F \supset K$ torre de cuerpos con E/K finita. Entonces $[E:K]_s = [E:K]$ si y solo si $[E:F]_s = [E:F]$ y $[F:K]_s = [F:K]$.*

Proposición 6. *Sea F/K extensión algebraica y $S \subset F$ tal que $F = K(S)$. Entonces la extensión F/K es separable sii todo elemento es separable sobre K*

Proposición 7.

1. *Sea $E \supset F \supset K$ torre de cuerpos con E/K **algebraica**. La extensión E/K es separable sii lo son las extensiones E/F y F/K*
2. *Sean E/K extensión algebraica separable y F/K extensión arbitraria. Etnocnes EF/F es separable.*
3. *Sean $E/K, F/K$ dos extensiones algebraicas separables. Entonces EF/K es separable.*

Corolario 1. ***La clausura normal de una extensión separable es separable***

Definición. *Definimos como clausura separable de K cuerpo, y lo notamos como K^{sep} al subcuerpo formado por todos los elementos de $\bar{K}$ separables sobre K forman un subcuerpo de $\bar{K}$*

Teorema 1. ***Teorema del elemento primitivo*** *Sea F/K extensión finita. La extensión es **simple** sii el conjunto de cuerpos intermedios $\{E : F \supset E \supset K\}$ es finito.*

Si una extensión F/K es finita y separable, entonces es simple.

Definición. ***Endomorfismo de Frobenius*** *Sea K un cuerpo de característica p. El homomorfismo $\phi : K \to K$ definido por $\phi(u) = u^p$ se llama endomorfismo de Frobenius del cuerpo K.*

Teorema 2. ***Caracterizaciones de cuerpos perfectos***

Para un cuerpo K son equivalentes:

1. *Todo polinomio $f \in K[X]$ irreducible tiene sólo raíces simples.*
2. *Toda extensión algebraica es separable.*
3. *Toda extensión finita es separable.*
4. *$car(K) = 0$ o $car(K) = p$ y el endomorfismo de Frobenius es sobreyectivo.*

En este caso el cuerpo se llama ***cuerpo perfecto***

Las implicaciones $1 \implies 2 \implies 3$ son claras. Para la implicación $3 \implies 1$, dado $f \in K[X]$ polinomio irreducible, con raíces $\alpha_1, \dots \alpha_n$ en una extensión algebraica, $K(\alpha_1, \dots \alpha_n)$ es finita, y 3 acaba.

Como ejemplos: cuerpos de característica 0, cuerpos finitos, cuerpos algebraicamente cerrados.

Derivada y raíces multiples

Definición. ***Multiplicidad de raíces***

Sea $f \in F[X]$ polinomio, $u \in F$ es raíz de f de multiplicidad k si $f = (X - u)^k f_1$ con $f_1(u) \neq 0$.

El elemento u es una raíz simple si $k = 1$ y es una raíz múltiple si $k > 1$.

Definición. ***Derivada de un polinomio en un cuerpo*** K

Dado $f = \sum_{i=0}^{n} a_i X^i$ definimos la derivada de f como:

$$f' = \sum_{i=0}^{n} i a_i X^{i-1}$$

Proposición 8. *1.* $(f+g)' = f' + g'$

2. $(fg)' = f'g + fg'$

3. $(f^m)' = m f^{m-1} f'$

Corolario 2. ***Condiciones para que las raíces sean simples***

1. *f irreducible, $f' \neq 0$. Entonces las raíces de f son simples.*
2. *$car(K) = 0$ y f irreducible sobre K. Entonces las raíces de f son simples.*
3. *$car(K) = p > 0$. El polinomio f irreducible tiene raíces múltiples sii $f(X) = g(X^p)$*

Definición. ***Polinomio separable***

Un polinomio $f \in K[X]$ se llama separable sobre K si sus factores irreducibles tienen solo raíces múltiples.