

Notas Extensiones Separables AM III

Cristo Daniel Alvarado

Diciembre de 2023

Índice general

4. Extensiones Separables	2
4.1. Resultados preeliminares	2
4.2. Extensiones separables	4

Capítulo 4

Extensiones Separables

4.1. Resultados preeliminares

Para enunciar lo que es una extensión separable, se necesitarán demostrar algunos resultados preeliminares para enunciarlo de forma adecuada.

Proposición 4.1.1

Sea F un campo y $f(X) \in F[X]$ un polinomio no constante. Si

1. $\text{car}(F) = 0$, entonces $f'(X) = 0$.
 2. $\text{car}(F) = p > 0$, entonces $f'(X) = 0$ si y sólo si $\exists g(X) \in F[X]$ tal que $f(X) = g(X^p)$.
-

Demostración:

En ambos casos, para la demostración se requiere de usar el polinomio $f'(X)$. Expresamos

$$f(X) = a_0 + a_1x + \cdots + a_nx^n, \quad n \geq 1, a_n \neq 0 \quad (4.1)$$

De (1): Se tiene que

$$f'(X) = \cdots + na_nx^{n-1}$$

donde $na_n \neq 0$ ya que $\text{car}(F) = 0$. Por tanto, $f'(X) \neq 0$.

De (2): Se probará el si, sólo si.

\Leftarrow): Supongamos que $\exists g(X) \in F[X]$ tal que $f(X) = g(X^p)$. Expresamos a $g(X) = b_0 + b_1x + \cdots + b_mx^m$, donde $b_m \neq 0$. Entonces

$$\begin{aligned} f(X) &= g(X^p) \\ &= b_0 + b_1X^p + \cdots + b_mX^{pm} \\ \Rightarrow f'(X) &= pb_1X^{p-1} + \cdots + pm b_mX^{pm-1} \\ &= 0 \cdot X^{p-1} + \cdots + 0 \cdot X^{pm-1} \\ &= 0 \end{aligned}$$

\Rightarrow): Supongamos que $f'(X) = 0$, donde $f'(X) = \sum_{i=1}^m ia_i x^{i-1}$, entonces $ia_i = 0$, para todo $i = 1, \dots, m$. Si $a_i \neq 0$ para algún i , entonces debe suceder que $i \cdot 1 = i = 0$, por lo cual $\text{car}(F) = p \mid i$. Luego si $a_i \neq 0$, existe $m_i \in \mathbb{N}$ tal que $i = pm_i$. Escribiendo a $f(X)$ con todos sus términos no cero, se tiene que

$$\begin{aligned} f(X) &= a_0 + a_{pm_1}X^{pm_1} + \cdots + a_{pm_n}X^{pm_n} \\ &= a_0 + a_{pm_1}(X^p)^{m_1} + \cdots + a_{pm_n}(X^p)^{m_n} \\ &= g(X^p) \end{aligned}$$

donde $g(X) = a_0 + a_{pm_1}X + \cdots + a_{pm_n}X^{m_n}$, siendo $a_{pm_n} \neq 0$, pues $f(X) \neq 0$ □

De este teorema anterior y de un teorema del capítulo pasado, se deduce de forma inmediata el siguiente corolario:

Corolario 4.1.1

Sea F un campo y $f(X) \in F[X]$ un polinomio irreducible. Si

1. $\text{car}(F) = 0$, entonces todas las raíces de $f(X)$ son simples.
 2. $\text{car}(F) = p > 0$, entonces $f(X)$ tiene una raíz simple si y sólo si, $\exists g(X) \in F[X]$ tal que $f(X) = g(X^p)$.
-

El siguiente teorema tiene como objetivo caracterizar las extensiones separables, enunciando un resultado importante para su definición.

Teorema 4.1.1

Sea F un campo con $\text{car}(F) = p > 0$. Sea $f(X) \in F[X]$ un polinomio irreducible, y $e \in \mathbb{N}^*$ tal que $f(X) \in F[x^{p^e}]$, pero $f(X) \notin F[x^{p^{e+1}}]$. Sea $\Psi(X) \in F[X]$ el polinomio tal que $f(X) = \Psi(X^{p^e})$. Entonces

1. $\Psi(X)$ es un polinomio irreducible en $F[X]$.
 2. Todas las raíces de $\Psi(X)$ son simples.
 3. Todas las raíces de $f(X)$ tienen la misma multiplicidad, a saber, p^e .
 4. Si $m = \deg(\Psi)$, entonces $\deg(f) = p^e m$.
-

Demostración:

De (1): Supongamos que $\Psi(X)$ es descomponible, entonces existen $g(X), h(X) \in F[X]$ con grados ≥ 1 tales que

$$\begin{aligned}\Psi(X) &= g(X)h(X) \\ \Rightarrow f(X) &= g(X^p)h(X^p) \\ &= g_1(X)h_1(X)\end{aligned}$$

donde $g_1(X) = g(X^p)$ y $h_1(X) = h(X^p)$ con grados ≥ 1 , lo cual implicaría que $f(X)$ es reducible. Luego $\Psi(X)$ tiene que ser irreducible.

De (2): Supongamos que $\Psi(X)$ admite una raíz múltiple, entonces $\exists g(X) \in F[X]$ tal que $\Psi(X) = g(X^p)$. Así

$$\begin{aligned}f(X) &= \Psi(X^{p^e}) \\ &= g(X^{p^{e+1}}) \\ &\in F[x^{p^{e+1}}]\end{aligned}$$

lo cual es una contradicción. Por lo tanto $\Psi(X)$ debe tener todas sus raíces simples.

De (3): Sea $m = \deg(\Psi)$. Sean $\beta_1, \dots, \beta_m \in \bar{F}$ todas las raíces de $\Psi(X)$ en alguna cerradura algebraica de F . Se tiene entonces que

$$\begin{aligned}\Psi(X) &= a(x - \beta_1) \cdots (x - \beta_m) \\ \Rightarrow f(X) &= \Psi(X^{p^e}) \\ &= a(x^{p^e} - \beta_1) \cdots (x^{p^e} - \beta_m)\end{aligned}$$

Donde $a \in F$ es alguna constante. Ahora, para cada $i = 1, \dots, m$ sea $\alpha_i \in \bar{F}$ una raíz del polinomio $X^{p^e} - \beta_i = 0$, esto es $\beta_i = \alpha_i^{p^e}$. Notemos que si $i \neq j$, debe suceder que $\alpha_i \neq \alpha_j$. Por tanto

asd

De (4): Es inmediata. □

Se deduce de forma inmediata el siguiente corolario.

Corolario 4.1.2

Sea F campo y $f(X) \in F[X]$ un polinomio irreducible. Entonces todas las raíces de $f(X)$ tienen la misma multiplicidad. Si $\text{car}(F) = 0$, la multiplicidad de estas raíces es 1, y si $\text{car}(F) = p > 0$, tienen multiplicidad p^e , para algún $e \in \mathbb{N}^*$ (este e se obtiene del teorema anterior).

4.2. Extensiones separables

Ahora estamos en las condiciones de enunciar la definición de separabilidad.

Definición 4.2.1

De acuerdo con las notaciones del teorema anterior y de su demostración, tenemos que el número $\deg(\Psi)$ es llamado **el grado de separabilidad de f** , y al entero no negativo e es llamado **el grado de inseparabilidad de f** .

En otras palabras, podemos ver que el grado de separabilidad de f es el número de raíces distintas de f .

Definición 4.2.2

Sea F un campo y \bar{F} una cerradura algebraica de F . Si $\alpha \in \bar{F}$ y $f(X) = \text{irr}(\alpha, F, X)$, entonces se define **el grado de separabilidad de α** , como el grado de separabilidad de f , y al exponente e de inseparabilidad de f , será el **exponente de inseparabilidad de α** .

En el caso en que $\text{car}(F) = 0$, el exponente y grado de inseparabilidad de f y α no tienen sentido en estar definidos, pues en ambos casos su valor siempre será de 1.

En cualquier caso, si $\alpha \in \bar{F}$ se denota al grado de separabilidad de α como

$$[F(\alpha) : F]_s \tag{4.2}$$

En el caso de que $\text{car}(F) = 0$, se tiene que

$$[F(\alpha) : F]_s = [F(\alpha) : F] = \deg(\text{irr}(\alpha, F, X)) \tag{4.3}$$

y, si $\text{car}(F) = p > 0$, entonces

$$[F(\alpha) : F]_s = \frac{[F(\alpha) : F]}{p^e} \tag{4.4}$$

Proposición 4.2.1

Sea F un campo, \bar{F} una cerradura algebraica de F y $\alpha \in \bar{F}$. Entonces, $[F(\alpha) : F]_s = N$, donde $N \in \mathbb{N}$ es el número de F -homomorfismos de $F(\alpha)$ en \bar{F} .

Demostración:

□

Definición 4.2.3

Sea E/F una extensión algebraica. Se define el **grado de separabilidad de E sobre F** como la cardinalidad del conjunto de F -homomorfismos que van de E en \bar{F} , donde \bar{F} es una cerradura algebraica de F que contiene a E . Tal cardinal es denotado por $[E : F]_s$.

De resultados de capítulo anterior, se deduce de forma inmediata el siguiente teorema.

Teorema 4.2.1

Sea E/F una extensión finita y K un campo intermedio de la extensión E/F . Entonces

$$[E : F]_s = [E : K]_s [K : F]_s \quad (4.5)$$

Definición 4.2.4

Sea F un campo y $\alpha \in \bar{F}$. Decimos que α **es separable sobre F** si $[F(\alpha) : F]_s = [F(\alpha) : F]$. Si E/F es una extensión algebraica, entonces se dice que E/F **es separable** o E **es separable sobre F** , si todo elemento de E es separable sobre F .

Veremos ahora algunas caracterizaciones de las extensiones separables.

Observación 4.2.1

Sea F campo y \bar{F} cerradura algebraica de F .

1. Si $\alpha \in \bar{F}$, entonces α es separable sobre F si y sólo si $f(X) = \text{irr}(\alpha, F, X)$ es tal que todas sus raíces son simples. Cuando esto ocurra decimos que $f(X)$ **es separable sobre F** .
2. Si $g(X) \in F[X]$, decimos que $g(X)$ **es separable sobre F** si todos sus factores irreducibles son separables sobre F .

Proposición 4.2.2

Sea E/F una extensión finita con $\text{car}(F) = p > 0$. Entonces existe un elemento $t \in \mathbb{N}^*$ tal que

$$[E : F] = p^t [E : F]_s \quad (4.6)$$

En particular, si $p \nmid [E : F]$, entonces $[E : F] = [E : F]_s$.

Observación 4.2.2

Si E/F es una extensión finita y $\text{car}(F) = 0$, entonces $[E : F] = [E : F]_s$.

Proposición 4.2.3

Sea E/F una extensión de campos con $\text{car}(F) = p > 0$ y $\alpha \in E$ algebraico sobre F . Sea e el exponente de inseparabilidad de α sobre F . Entonces

1. α^{p^e} es separable sobre F .
2. Las siguientes condiciones son equivalentes:
 - I) α es separable sobre F .
 - II) $[F(\alpha) : F]_s = [F(\alpha) : F]$.
 - III) $e = 0$.

$$\text{IV) } F(\alpha) = F(\alpha^p).$$

Demostración:

De

□

Proposición 4.2.4

Sea E/F una extensión finita. Entonces E/F es separable si y sólo si $[E : F]_s = [E : F]$.

Demostración:

□

Observación 4.2.3

Sea $F \subseteq K \subseteq E$ una torre de campos y $\alpha \in E$ separable sobre F . Entonces α es separable sobre K . Más generalmente, sean E/F y K/F extensiones de campos y $\alpha \in E$ separable sobre F . Si α es elemento de un campo L extensión de K , entonces α es separable sobre K .

Proposición 4.2.5

Sea E/F una extensión de campos y $S \subseteq E$ tal que $E = F(S)$. Sea.

$$K = \{\alpha \in E \mid \alpha \text{ es separable sobre } F\} \quad (4.7)$$

Entonces

1. K es un subcampo intermedio de la extensión E/F .
 2. E/F es separable si y sólo si α es separable sobre F , para todo $\alpha \in S$.
-

Demostración:

De (1): Probaremos que K es campo y que $F \subseteq K \subseteq E$. En efecto, sea $\alpha \in F$, se tiene que α es algebraico sobre F , con polinomio irreducible $f(X) = X - \alpha$, el cual tiene todas sus raíces distintas, por lo cual α es separable sobre F . Entonces $F \subseteq K \subseteq E$. Sean ahora $\alpha, \beta \in K \neq \emptyset$, pues $F \subseteq K$. Consideremos el campo intermedio de la extensión E/F , $F(\alpha, \beta)$. Se tiene entonces la torre de campos

$$F \subseteq F(\alpha) \subseteq F(\alpha, \beta) \subseteq E$$

Como β es separable sobre F , lo es sobre $F(\alpha)$, luego como el grado de separabilidad es multiplicativo, se tiene que

$$\begin{aligned} [F(\alpha, \beta) : F]_s &= [F(\alpha, \beta) : F(\alpha)]_s [F(\alpha) : F]_s \\ &= [F(\alpha, \beta) : F(\alpha)] [F(\alpha) : F] \\ &= [F(\alpha, \beta) : F] \end{aligned}$$

por lo cual, la extensión $F(\alpha, \beta)/F$ es separable, luego los elementos $\alpha - \beta, \alpha\beta, \alpha^{-1} \in F(\alpha, \beta)$ son separables sobre F . Por tanto, K es campo y por lo anterior, es subcampo intermedio de la extensión E/F .

De (2): Veamos que

\Rightarrow): Es inmediata, pues si E/F es separable todo elemento de E es separable sobre F . En particular todo elemento de S es separable sobre F .

\Leftarrow): Supongamos que α es separable sobre F , para todo $\alpha \in S$. Por (1) se tiene que $S \subseteq K$ y $F \subseteq K$, pero como K es subcampo de E , se tiene que $F(S) \subseteq K$, por lo cual $F(S) = E = K$. Así, todos los elementos de E son separables sobre F , es decir E/F es una extensión separable. \square

Definición 4.2.5

El campo K de la definición (4.7) es llamado **la cerradura separable** o de la extensión E/F o simplemente de E/F , o de F en E .

Si consideramos la extensión \bar{F}/F , entonces la cerradura separable de F en \bar{F} simplemente se dice es la **cerradura separable de F** .

Observación 4.2.4

Si E/F es una extensión algebraica de tal manera que $E \subseteq \bar{F}$, entonces la cerradura separable de F en E , K , es la intersección de la cerradura separable de F con E .

Observación 4.2.5

En la literatura no existe notación establecida para referirse a la cerradura normal. En este momento nosotros acordaremos la siguiente. Sobre la extensión E/F , se denotará a la cerradura separable de F en E por:

$$F_{S,E/F} \quad \text{o} \quad F_{S,F}^E$$

Cuando la extensión es \bar{F}/F será

$$F_S$$

y a veces a la cerradura algebraica se le denota por $\bar{F} = F^a$.

Proposición 4.2.6

Sea E/F una extensión normal & F_S la cerradura separable de E/F . Entonces, la extensión F_S/F es normal.

Demostración:

Sea $\alpha \in F_S$ con $f(X) = \text{irr}(\alpha, F, X)$, y $\beta \in \bar{F}$ tal que α y β son F -conjugados, es decir que ambos son raíces del polinomio $f(X)$. Como la extensión E/F es normal, entonces $\beta \in E$, donde $\text{irr}(\beta, F, X) = f(X)$ es separable sobre F , pues α es separable sobre F , es decir, β es separable sobre F . Luego $\beta \in F_S$. Por tanto, la extensión F_S/F es normal. \square

Observación 4.2.6

Si F es campo, la extensión \bar{F}/F es normal, por lo cual las extensiones \bar{F}/F_S y F_S/F son ambas normales (siendo F_S la cerradura separable de F).

Proposición 4.2.7

Sea E/F una extensión finita. y F_S la cerradura separable de F en E . Entonces,

$$[F_S : F] = [E : F]_s \quad (4.8)$$

Demostración:

Tenemos dos casos:

- Si $\text{car}(F) = 0$, entonces la extensión E/F es separable y por tanto $F_S = E$. Por tanto

$$\begin{aligned} [F_S : F] &= [E : F] \\ &= [E : F]_s \end{aligned}$$

- Si $\text{car}(F) = p > 0$. Tenemos que

$$\begin{aligned} [E : F]_S &= [E : F_S]_S [F_S : F]_S \\ &= [E : F_S]_S [F_S : F] \end{aligned}$$

Para probar el resultado, basta con probar que $[E : F_S]_S = 1$. Recordemos que $[E : F_S]_S$ es el cardinal de F_S -homomorfismos de E en $\bar{F} = \bar{F}_S$. Sea entonces $f : E \rightarrow \bar{F}$ un F_S -homomorfismo. Sea $\alpha \in E$. Si $\alpha \in F_S$ entonces $f(\alpha) = \alpha$. Si $\alpha \notin F_S$, se tiene por definición de F_S que α no es separable sobre F .

Sea $f(X) = \text{irr}(\alpha, F, X)$, y tomemos $e \in \mathbb{N}^*$ su exponente de inseparabilidad. Por un resultado anterior sucede que α^{p^e} es separable sobre F , es decir $\alpha^{p^e} \in F_S$. Luego,

$$\begin{aligned} f(\alpha^{p^e}) &= \alpha^{p^e} \\ \Rightarrow (\alpha - f(\alpha))^{p^e} &= \alpha^{p^e} - f(\alpha)^{p^e} \\ &= 0 \\ \Rightarrow f(\alpha) - \alpha &= 0 \\ \Rightarrow f(\alpha) &= \alpha \end{aligned}$$

Es decir, $f = \text{id}_E$. Por tanto $[E : F_S] = 1$. Así por la ecuación anterior

$$[E : F]_S [F_S : F]$$

□

Teorema 4.2.2

La clase de extensiones separables es una clase distinguida.

Demostración:

De (a): Sea $F \subseteq K \subseteq E$ una torre de campos. Probaremos que E/F es separable si, y sólo si E/K y K/F son separables.

\Rightarrow): Supongamos que E/F es separable. Sabemos ya que E/K es separable. Pero, por otro lado, es claro que la extensión K/F es separable.

\Leftarrow): Supongamos que las extensiones E/K y K/F son separables. Sea $\alpha \in E$ arbitrario y tomemos $f(X) = \text{irr}(\alpha, K, X)$, digamos

$$f(X) = a_0 + a_1X + \cdots + a_{m-1}X^{m-1} + X^m \in K[X]$$

Tenemos que $f(X)$ es separable sobre K , es decir todas las raíces de $f(X)$ son simples. Consideremos la torre de campos:

$$F \subseteq F(a_0, a_1, \dots, a_{m-1}) \subseteq F(a_0, a_1, \dots, a_{m-1}, \alpha)$$

donde $F(a_0, a_1, \dots, a_{m-1})/F$ es finita y separable, al igual que $F(a_0, a_1, \dots, a_{m-1}, \alpha)/F(a_0, a_1, \dots, a_{m-1})$. Notemos que $f(X) = \text{irr}(\alpha, F(a_0, a_1, \dots, a_{m-1}), X)$. Entonces

$$\begin{aligned} [F(a_0, a_1, \dots, a_{m-1}, \alpha) : F] &= [F(a_0, a_1, \dots, a_{m-1}, \alpha) : F(a_0, a_1, \dots, a_{m-1})] [F(a_0, a_1, \dots, a_{m-1}) : F] \\ &= [F(a_0, a_1, \dots, a_{m-1}, \alpha) : F(a_0, a_1, \dots, a_{m-1})]_s [F(a_0, a_1, \dots, a_{m-1}) : F]_s \\ &= [F(a_0, a_1, \dots, a_{m-1}, \alpha) : F]_s \end{aligned}$$

es decir, $F(a_0, a_1, \dots, a_{m-1}, \alpha)/F$ es una extensión separable, en particular se tiene que α es separable sobre F . Por ser el α arbitrario en E , se sigue que E/F es una extensión separable.

De (b):

□