Notas Extensiones Separables AM III

Cristo Daniel Alvarado

Diciembre de 2023

Índice general

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. $\mathrm{car}(F) = 0$, entonces $f'(X) \neq 0$.
2. $\mathrm{car}(F) = p > 0$, 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

$$f(X) = a_0 + a_1 x + \cdots + a_n x^n, \quad n \geq 1,\ a_n \neq 0 \tag{4.1}$$

De (1): Se tiene que

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

donde $n a_n \neq 0$ ya que $\mathrm{car}(F) = 0$. 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 $g(X) = b_0 + b_1 x + \cdots + b_m x^m$, donde $b_m \neq 0$. Entonces

$$\begin{aligned} f(X) =& g(X^p) \\ =& b_0 + b_1 X^p + \cdots + b_m X^{pm} \\ \Rightarrow f'(X) =& p b_1 X^{p-1} + \cdots + p m b_m X^{pm-1} \\ =& 0 \cdot X^{p-1} + \cdots + 0 \cdot X^{pm-1} \\ =& 0 \end{aligned}$$

$\Rightarrow$): Supongamos que $f'(X) = 0$, donde $f'(X) = \sum_{i=1}^{m} i a_i x^{i-1}$, entonces $i a_i = 0$, para todo $i = 1, \cdots, m$. Si $a_i \neq 0$ para algún i, entonces debe suceder que $i \cdot 1 = i = 0$, por lo cual $\mathrm{car}(F) = p \mid i$. Luego si $a_i \neq 0$, existe $m_i \in \mathbb{N}$ tal que $i = p m_i$. 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 capítlo 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 $f(X) = g(X^p)$.

Demostración:
Es inmediata de la proposición anterior. ■

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 irredicible 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 irredicible.

De (2): Supongamos que $\Psi(X)$ admite una raíz multiple, 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 tenera todas sus raíces simples.

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

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

Donde $a \in F$ es alguna constante. Ahora, para cada $i = 1, \cdots, m$ sea $\alpha_i \in \bar{F}$ una raíz del polinomio $X^{p^e} - \beta_i = 0$, esto es $\beta_i = \alpha^{p^e}$. 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 irredicible. Entonces todas las raíces de $f(X)$ tienen la misma multiplicidad. Si $\operatorname{car}(F) = 0$, la multiplicidad de estas raíces es 1, y si $\operatorname{car}(F) = p > 0$, 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 demostracion, 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 $f(X) = \operatorname{irr}(\alpha, F, X)$, 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 $\operatorname{car}(F) = 0$, 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 $\operatorname{car}(F) = 0$, se tiene que

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

y, si $\operatorname{car}(F) = p > 0$, 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 cerradora 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:
Sea $f(X) = \mathrm{irr}(\alpha, F, X)$. Tomemos $\alpha_1, \ldots, \alpha_m \in \bar(F)$ las raíces distintas de $f(X)$. Se tiene por definición que

$$m = [F(\alpha) : F]_S$$

Sea $\phi : F(\alpha) \to \bar(F)$ un F-homomorfismo. Sabemos que ϕ está completamente detemrinada por su acción sobre α, teniendo que $\phi(\alpha)$ es raíces de $f(X)$, esto es debe ser que $\phi(\alpha) = \alpha_i$, con $i \in [\![1, m]\!]$. luego, a lo más tenemos m F-homomorfismos de $F(\alpha)$ en $\bar{F}$, con lo cual se tiene el resultado. ■

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

$$[E : F]_s = [E : K]_s [K : F]_s \tag{4.5}$$

Demostración:
Es inmediata de un teorema anterior. ■

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 camop y $\bar{F}$ cerradura algebraica de F.

1. Si $\alpha \in \bar{F}$, entonces α es separable sobre F si y sólo si $f(X) = \mathrm{irr}(\alpha, F, X)$ 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 $\mathrm{car}(F) = p > 0$. Entonces existe un elemento $t \in \mathbb{N}^*$ tal que

$$[E : F] = p^t [E : F]_s \tag{4.6}$$

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

Demostración:

Sean $\alpha_1, \ldots, \alpha_n \in E$ tales que $E = F(\alpha_1, \ldots, \alpha_n)$. Consideraremos la torre de campos $F \subseteq F(\alpha_1) \subseteq \cdots \subseteq F(\alpha_1, \ldots, \alpha_{n-1}) \subseteq F(\alpha_1, \ldots, \alpha_n)$. Sea e^i es exponente de inseparabilidad de α_i sobre $F(\alpha_1, \ldots, \alpha_{i-1})$, con $i \in [\![2, n]\!]$ y e_1 el grado de inseparabilidad de α_1 sobre F. Entonces

$$\begin{aligned}
[E : F]_s =& [F(\alpha_1, \ldots, \alpha_n) : F(\alpha_1, \ldots, \alpha_{n-1})]_s \cdot \cdots \cdot [F(\alpha_1) : F]_s \\
=& \frac{1}{p^{e_n}} [F(\alpha_1, \ldots, \alpha_n) : F(\alpha_1, \ldots, \alpha_{n-1})] \cdot \cdots \cdot \frac{1}{p^{e_1}} [F(\alpha_1) : F] \\
\Rightarrow [E : F] =& p^{e_1 + e_2 + \cdots + e_n} [E : F]_s
\end{aligned}$$

tomando $t = e_1 + \cdots + e_n \in \mathbb{Z}_{\geq 0}$ se sigue el resultado. ■

Observación 4.2.2

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

Proposición 4.2.3

Sea E/F una extension de campos con $\mathrm{car}(F) = p > 0$ 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) $e = 0$.
   - IV) $F(\alpha) = F(\alpha^p)$.

Demostración:

De (1): Sea $f(X) = \mathrm{irr}(\alpha, F, X)$ y $\psi(x) \in F[X]$ tal que $\psi(X^{p^e}) = f(X)$, pero $f(X) \notin F[X^{p^{e+1}}]$. Sabemos que $\psi(X)$ es irreducible sobre F y que todas sus raíces son simples, donde

$$0 = f(\alpha) = \psi(\alpha^{p^e})$$

esto es, α^{p^e} es raíz de $\psi(X)$, por lo cual $\psi(X) = \mathrm{irr}(\alpha^{p^e}, F, X)$. Por tanto, α^{p^e} es separable sobre F.

De (2): Es claro que I) $\iff$ II) $\iff$ III). Probaremos que I) $\iff$ IV). Antes, notemos que

$$F \subseteq F(\alpha^p) \subseteq F(\alpha)$$

I)$\Rightarrow$ IV): Sea $f(X) = \mathrm{irr}(\alpha, F, X)$. Tenemos que $g(X) = X^p - \alpha^p \in F(\alpha^p)[X]$ y α es raíz de $g(X)$. Por lo cual $\mathrm{irr}(\alpha, F(\alpha^p), X) \mid g(X)$ y $\mathrm{irr}(\alpha, F(\alpha^p), X) \mid f(X)$ en $F(\alpha^p)[X]$.

Entonces, como todas las raíces de $f(X)$ son simples, las raíces de $h(X) = \mathrm{irr}(\alpha, F(\alpha^p), X)$ también lo son; además $h(X) \mid X^p - \alpha^p = (X - \alpha)^p \Rightarrow h(X) = (x - \alpha) \Rightarrow \alpha \in F(\alpha^p)$. Por tanto, $F(\alpha) = F(\alpha^p)$.

IV)$\Rightarrow$ I): Recíprocamente, supongamos que $F(\alpha) = F(\alpha^p)$ pero α no es separable sobre F. Siendo $f(X) = \mathrm{irr}(\alpha, F, X)$, tenemos que $f(X) \in F[X^p]$, esto es, existe $g(X) \in F[X]$ tal que $f(X) = g(X^p)$ donde $\deg(f) = p \cdot \deg(g) > \deg(g)$.

Notemos que $g(X)$ tiene por raíz a α^p, pues $g(\alpha^p) = f(\alpha) = 0$, de esta forma $\mathrm{irr}(\alpha^p, F, X) \mid g(X) \Rightarrow [F(\alpha^p) : F] = \deg(\mathrm{irr}(\alpha^p, F, X)) = \deg(g) < \deg(f) = [F(\alpha) : F]$, luego $F(\alpha^p) \subsetneq F(\alpha)$, lo cual es una contradicción. Por tanto, α es separable sobre F.

■

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:
$\Rightarrow)$: Suponga que E/F es separable. Sean $\alpha_1, \ldots, \alpha_n \in E$ tales que $F(\alpha_1, \ldots, \alpha_n) = E$. Consideremos la torre de campos:

$$F \subsetneq F(\alpha_1) \subsetneq \cdots \subsetneq F(\alpha_1, \ldots, \alpha_n) = E$$

para cada $i \in [\![2, n]\!]$, tenemos que α_i es separable y, por ende, lo es sobre $F(\alpha_1, \ldots, \alpha_{i-1})$. Luego,

$$\begin{aligned} [E:F]_s =& [F(\alpha_1, \ldots, \alpha_n) : F(\alpha_1, \ldots, \alpha_{n-1})]_s \cdot \cdots \cdot [F(\alpha_1) : F]_s \\ =& [F(\alpha_1, \ldots, \alpha_n) : F(\alpha_1, \ldots, \alpha_{n-1})] \cdot \cdots \cdot [F(\alpha_1) : F] \\ =& [E:F] \end{aligned}$$

$\Leftarrow)$: Sea $\alpha \in E$ arbitrario. Tenemos lo siguiente:

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

donde $[E:F(\alpha)]_s \leq [E:F(\alpha)]$ y $[F(\alpha):F]_s \leq [F(\alpha):F]$. Por la igualdad anterior debe suceder que

$$[F(\alpha):F] = [F(\alpha):F]$$

esto es, que α es separable sobre F. Como el α fue arbitrario, entonces se sigue que la extensión E/F es una extensión separable.

■

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.

$$K = \{\alpha \in E | \alpha \text{ es separable sobre } F\} \tag{4.7}$$

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. ■

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:

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

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 cerrradura separable de E/F. Entonces, la extensión F_S/F es normal.

Demostración:
Sea $\alpha \in F_S$ con $f(X) = \operatorname{irr}(\alpha, F, X)$, 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 $\operatorname{irr}(\beta, F, X) = f(X)$ 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. ■

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,

$$[F_S : F] = [E : F]_s \tag{4.8}$$

Demostración:
Tenemos dos casos:

- Si $\mathrm{car}(F) = 0$, 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 $\mathrm{car}(F) = p > 0$. 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 $f : E \to \bar{F}$ un F_s-homomorfismo. Sea $\alpha \in E$. Si $\alpha \in F_S$m entonces $f(\alpha) = \alpha$. Si $\alpha \notin F_S$, se tiene por defininción de F_S que α no es separable sobre F.

  Sea $f(X) = \mathrm{irr}(\alpha, F, X)$, 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, $f = \mathrm{id}_E$. 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 $f(X) = \mathrm{irr}(\alpha, K, X)$, 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 $f(X) = \mathrm{irr}(\alpha, F(a_0, a_1, \dots, a_{m-1}), X)$. Entonces

$$\begin{aligned}[F(a_0, a_1, \dots, a_{m-1}, \alpha) : F] &= [F(a_0, a_1, \dots, a_{m-1}, \alpha) : Fa_0, a_1, \dots, a_{m-1}]\,[F(a_0, a_1, \dots, a_{m-1}) : F] \\ &= [F(a_0, a_1, \dots, a_{m-1}, \alpha) : Fa_0, a_1, \dots, a_{m-1}]_s\,[F(a_0, a_1, \dots, a_{m-1}) : F]_s \\ &= [F(a_0, a_1, \dots, a_{m-1}, \alpha) : F]_s\end{aligned}$$

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): Sean E/F y K/F extensiones separables, dónde E/F es separable y, E y K subcampos de un campo común L. Como $K(E) = KE$, entonce basta ver que los elementos de E son separables sobre K, lo cual ya se tiene.

Entonces, KE/F es una extensión separable. ■

Corolario 4.2.1
Sean E/F y K/F extensiones separables, con E y K subcamopos de un campo común L. Entonces, KE/F es separable.

Demostración:
Es inmediato de la proposición teorema. ■

Definición 4.2.6
Sea F un campo. Se dice que F **es perfecto** si toda extensión algebraica de F es separable.

Observación 4.2.7
Todo campo de caracterísitica 0 es perfecto (ya que toda extensión algebraica de un campo con caracterísica 0 sigue teniendo característica 0, es decir que la extensión siempre va a ser separable).

Definición 4.2.7
Sea F campo de caracerística $p > 0$. Sea $n \in \mathbb{N}$. Se define la función $\phi_n : F \to F$, $\alpha \mapsto \alpha^{p^n}$.

Se tiene que ϕ_n es un homomorfismo, llamado **el homomorfismo de Fröbenius de grado** n. Para $n = 1$ se dice simplemente que ϕ_1 es el homomorfismo de Fröbenius, y se denota por ϕ.

Teorema 4.2.3
Sea F un campo de caracterísitca $p > 0$. Las siguientes condiciones son equivalentes:

1. F es perfecto.
2. Toda extensión finita de F es separable.
3. Todo polinomio irreducible sobre F es separable.
4. Todo polinomio sobre F es separable.

5. El homomorfismo de Fröbenius es un automorfismo de F.

Demostración:

(1) $\Rightarrow$ (2): Es inmediato.

(2) $\Rightarrow$ (3): Sea $f(X) \in F[X] \backslash F$ irreducible y sea $\alpha \in \bar{F}$ una raíz de $f(X)$. Por hipótesis, $F(\alpha)$ es una extensión separable de F, luego α es separable sobre F. Como $f(X)$ es asociado con $\operatorname{irr}(\alpha, F, X)$, entonces f es separable sobre F.

(3) $\iff$ (4): Es inmediato.

(4) $\Rightarrow$ (5): Es claro que $\phi : F \to F$ es un monorfismo. Sea $\alpha \in F$ y considérese $f(X) = X^p - \alpha \in F[X]$. Sea $\beta \in \bar{F}$ una raíz de $f(X)$ y sea $g(X) = \operatorname{irr}(\beta, F, X)$, el cual es separable y divide a $f(X)$. Pero $f(X) = X^p - \alpha^p = (X - \alpha)^p$, así β es la única raíz de $f(X)$, por lo que también lo es de $g(X)$. Por tanto, $g(X) = X - \beta \in F[X]$.

Luego, $\beta \in F$. Así pues, ϕ es suprayectiva, luego es un automorfismo de F.

(5) $\Rightarrow$ (1): Sea E/F una extensión algebraica. Sean $\alpha \in E$ y $f(X) = \operatorname{irr}(\alpha, F, X)$, cuyas raíces tienen multiplicidad p^e, con $e \in \mathbb{Z}_{\geq 0}$, siendo e el exponente de inseparabilidad de α. Suponiendo que $e \geq 1$, entonces α es raíz múltiple de $f(X)$, por lo que existe $g(x) \in F[X]$ tal que $f(X) = g(X^p)$. Sea

$$g(X) = b_0 + b_1 X + \cdots + b_m X^m$$

Por hipótesis, para todo $i \in \{0, \ldots, m\}$ existe $c_i \in F$ tal que $b_i = c_i^p$. Pero, esto implica que

$$f(X) = c_0^p + c_0^p X^p + \cdots c_m^p X^{mp} = (c_0 + c_1 X + \cdots + c_m X^m)^p$$

lo cual contradice el hecho de que $f(X)$ sea irredicible. Por tanto, $e = 0$, luego α es separable sobre sobre F y, en consecuencia, E/F es una extensión separable. ■

Teorema 4.2.4
Todo campo finito es perfecto.

Demostración:

Considerando el homomorfismo de Fröbenius $\phi : F \to F$, se tiene que ϕ es inyectivo, por lo cual $\left|\phi(F)\right| = \left|F\right|$. Pero, como F es finito, entonces $\phi(F) = F$, luego ϕ es automorfismo de F. Así pues, F es perfecto. ■

Definición 4.2.8
Sea E/F una extensión de campos y α inseparable sobre F. Entonces $f(X) = \operatorname{irr}(\alpha, F, X)$ es de la forma $f(X) = (X - \alpha_1)^{p^e} \cdot \ldots \cdot (X - \alpha_m)^{p^e}$ con $e \geq 1$, Se dice que α es **puramente inseparable sobre** F si y sólo si existe $t \in \mathbb{Z}_{\geq 0}$ tal que $\alpha^{p^t} \in F$.

4.3. Extesiones puramente inseparables

Definición 4.3.1
Sea E/F una extensión de campos con $\operatorname{car}(F) = p > 0$ y $\alpha \in E$. Decimos que α **es puramente inseparable** si existe $t \in \mathbb{Z}$, $t \geq 0$ tal que $\alpha^{p^t} \in F$. La extensión E/F **es p.i.** si todo elemento de E es p.i. sobre F.

Observación 4.3.1
Si E/F es una extensión de campos, entonces todos los elementos de F son p.i. (separables) sobre F.

Proposición 4.3.1
Sea E/F una extensión de campos con $\mathrm{car}(F) = p > 0$. Sea

$$K := \{\alpha \in E | \alpha \text{ es puramente inseparable sobre } F\}$$

(por la observación anterior, $K \neq \emptyset$). Entonces, K es subcampo de E que contiene a F.

Demostración:
Es claro que $K \neq \emptyset$ y $F \subseteq K \subseteq E$. Sean $\alpha, \beta \in K$, y $t_1, t_2 \in \mathbb{Z}_{\geq 0}$ tales que

$$\alpha^{p_1^t}, \beta^{p_2^t} \in F$$

Sea $t = \max\{t_1, t_2\}$. Por lo cual $\alpha^{p^t}, \beta^{p^t} \in F$, así

$$(\alpha - \beta)^{p^t} = \alpha^{p^t} - \beta^{p^t} \in F$$
$$(\alpha\beta)^{p^t} = \alpha^{p^t}\beta^{p^t} \in F$$
$$\left(\alpha^{-1}\right)^{p^t} = \left(\alpha^{p^t}\right)^{-1} \in F \text{ donde } \alpha \neq 0$$

por lo cual K es campo intermedio de la extensión E/F. ■

Proposición 4.3.2
Sea E/F una extensión algebraica, con $\mathrm{car}(F) = p > 0$. Sea $S \subseteq E$ tal que $E = F(S)$. Entonces, las siguientes condiciones son equivalentes:

1. E/F es puramente inseparable.
2. Todo elemento de S es puramente inseparable sobre F.
3. Los elementos de E que son puramente inseparables y separables sobre F son exactamente los de F.
4. Si $\phi : E \to \bar{F}$ es un F-homomorfismo, entonces $\phi(\alpha) = \alpha$, para todo $\alpha \in E$.

Demostración:
(1) $\Rightarrow$ (2): Es inmediato.

(2) $\Rightarrow$ (3): Sea $\alpha \in E$ tal que es puramente inseparable sobre F y separable sobre F, y $e \in \mathbb{Z}_{\geq 0}$ el exponente de inseparablilidad de α sobre F.

Tenemos que α^{p^e} es separable sobre F (por una proposición anterior). Por otro lado, sea $t \in \mathbb{Z}_{\geq 0}$ tal que $\alpha^{p^e} \in F$. Podemos suponer que $t \geq e$. Luego, α es raíz del polinomio $g(X) = X^{p^t} - \alpha^{p^t} = (X - \alpha)^{p^t}$, por lo cual $f(X) | g(X)$, donde $f(X) = \mathrm{irr}(\alpha, F, X)$.

Así $f(x) = (X - \alpha)^{p^t}$. Como α es separable sobre F, se tiene que $e = 0$, es decir que $f(X) = X - \alpha \in F[X]$, en particular, $\alpha \in F$.

(3) $\Rightarrow$ (4): Sea $\phi : E \to \bar{F}$ un F-homomorfismo arbitrario, y $\alpha \in E$, con $e \in \mathbb{Z}_{\geq 0}$ su exponente de inseparabilidad. Sabemos que α^{p^e} es separable sobre F. Por hipótesis, $\alpha^{p^e} \in F$. Por lo cual

$$\phi(\alpha^{p^e}) = \alpha^{p^e}$$
$$\Rightarrow (\phi(\alpha) - \alpha)^{p^e} = \left(\phi\alpha^{p^e}\right) - \alpha^{p^e} = 0$$
$$\Rightarrow \phi(\alpha) = \alpha$$

(4) $\Rightarrow$ (1): sea $\alpha \in E$ arbitrario. Probaremos que existe $t \in \mathbb{Z}_{\geq 0}$ tal que $\alpha^{p^t} \in F$. Sea $\beta \in \bar{F}$ un F-conjugado de α. Sabemos que existe un F-isomorfismo $\psi : F(\alpha) \to F(\beta)$ tal que $\psi(\alpha) = \beta$. Extendemos ψ a un F-homomorfismo $\phi : E \to \bar{F}$. Por hipótesis, se tiene que $\phi(\gamma) = \gamma$, para todo $\gamma \in E$, en particular $\beta = \psi(\alpha) = \phi(\alpha) = \alpha$. Luego, si $e \in \mathbb{Z}_{\geq 0}$ es el exponente de inseparabilidad de α, entonces

$$\begin{aligned} f(X) =& \operatorname{irr}(\alpha, F, X) \\ =& (X - \alpha)^{p^e} \\ =& X^{p^e} - \alpha^{p^e} \in F[X] \end{aligned}$$

por tanto $\alpha^{p^e} \in F$. Luego α es p.i. sobre F. ■

Definición 4.3.2
Si E/F es una extensión algebraica con $\operatorname{car}(F) = p > 0$, entonces la **cerradura puramente inseparable** de la extensión E/F o de E en F, es el campo intermedio de todos los elementos $\alpha \in R$ tal que son puramente inseparables sobre F.

Observación 4.3.2
Si E/F es finita, entonces E/F es p.i. $\iff$ $[E : F]_S = 1$.

Observación 4.3.3
Sea E/F una extensión algebraica la cual es p.i. y separable. Entonces, tenemos que $E = F$.

Teorema 4.3.1
La clase de extensiones p.i. forman una clase distinguida.

Demostración:
(a): Sea $F \subseteq K \subseteq E$ una torre de campos con $\operatorname{car}(F) = p > 0$. Supóngase que E/F es puramente inseparable. Sea $\alpha \in E$, entonces existe $t \in \mathbb{R}_{\geq 0}$ tal que $\alpha^{p^t} \in F \subseteq K$, por tanto E/K es puramente inseparable.

Por otro lado, es claro que todos los elementos de K son p.i. sobre F, por lo cual K/F es puramente inseparable.

Recíprocamente, suponga que E/K y K/F son p.i. Sea $\alpha \in E$,entonces existe $r \in \mathbb{Z}_{\geq 0}$ tal que $\alpha^{p^r} \in K$. Pero para este elemento existe $s \in \mathbb{Z}_{\geq 0}$ tal que $(\alpha^{p^r})^{p^s} \in F$, es decir $\alpha^{p^{r+s}} \in F$. Por tanto, E/F es puramente inseparable.

(b): Sean E/F y K/F extensiones de campos con $\operatorname{car}(F) = p > 0$, donde E y K son subcampos de un campo común L. Supóngase que la extensión E/F es p.i. Probaremos que la extensión EK/K es p.i.

Tenemos que $EK = K(E)$. Si $\alpha \in E$, entonces existe $t \in \mathbb{Z}_{\geq 0}$ tal que $\alpha^{p^t} \in F \subseteq K$. Por tanto, EK/K es p.i.

Por (a) y (b), se sigue que la clase de extensiones p.i. es una clase distinguida. ■

Corolario 4.3.1
Sean E/F y K/F extensiones de campos tales que $\operatorname{car}(F) = p > 0$, donde K y E son subcampos de un campo común L. Si E/F y K/F son p.i., entonces EK/F es p.i.

Demostración:
Es inmediato del teorema anterior. ■

Sea E/F una extensión algebraica con $\mathrm{car}(F) = p > 0$, y sean F_i y F_s las cerraduras p.i. y separables, respectivamente. Entonces tenemos el siguiente diagrama:

donde $F_i \cap F_s = F$.

Proposición 4.3.3
En las condiciones de las notaciones anteriores, tenemos lo siguiente

1. E/F_s es p.i.
2. E/F_i es separable si y sólo si $E = F_iF_s$.

Demostración:
De (1): Sea $\alpha \in E$, y $e \in \mathbb{Z}_{\geq 0}$ su expontente de inseparabilidad sobre F. Sabemos que α^{p^e} es separable sobre F, por lo cual $\alpha \in F_s$. De esta forma, E/F_s es puramente inseparable.

De (2):

$\Rightarrow$): Supóngase que E/F_i es separable, entonces E/F_iF_s es separable y p.i., por lo cual $E = F_iF_s$.

$\Leftarrow$): Es inmediata. ■

Proposición 4.3.4
Sea F un campo cualquiera tal que $\mathrm{car}(F) = p > 0$. Sea $\bar(F)$ su cerradura algebraica y F_i la cerradura p.i. de F en $\bar{F}$. Tenemos lo siguiente

1. El campo F_i es perfecto.
2. $F_i \cap F_s = F$ y $F_iF_s = \bar{F}$, dónde F_s es la cerradura separable de F en $\bar{F}$.
3. Si K es un campo perfecto tal que $F \subseteq K$, con $K \subseteq \bar{F}$, entonces $F_i \subseteq K$.

Demostración:
De (1): Probemos que $F_i^p = F_i$, donde

$$F_i^p = \{\alpha^p | \alpha \in F_i\}$$

ya se tiene que $F_i^p \subseteq F_i$. Sea $\alpha \in F_i$, y $\beta \in \bar{F}$ tal que $\alpha = \beta^p$. Luego, existe $t \in \mathbb{Z}_{\geq 0}$ tal que $\beta^{p^{t+1}} = \alpha^{p^t} \in F$, por lo cual $\beta \in F_i$. Asi $\alpha = \beta^p \in F_i$.

Por tanto, $F_i = F_i^p$. Luego, F_i es un campo perfecto.

De (2): Ya sabemos que $F_i \cap F_s = F$. Para la otra igualdad, como F_i es un campo perfecto, entonces la extensión $\bar{F}/F_i$ es separable, lo cual implica que $F_iF_s = \bar{F}$.

De (3): Sea K un campo intermedio de la extensión $\bar{F}/F$ el cual es perfecto. Probemos que $F_i \subseteq K$. Sea $\alpha \in F_i$. Consideremos la extensión $K(\alpha)/K$, esta extensión es separable; por otro lado, existe un elemento $t \in \mathbb{Z}_{\geq 0}$ tal que $\alpha^{p^t} \in F \subseteq K$, luego la extensión $K(\alpha)/K$ es p.i., así $K(\alpha) = K$ lo cual implica que $\alpha \in K$.

Por ende, $F_i \subseteq K$. ■

Corolario 4.3.2
Sea F un campo con $\mathrm{car}(F) = p > 0$. Entonces, la intersección de cualquier familia de subcampos

de $\bar{F}$ que contienen a F es un campo perfecto.

Demostración:

Es inmediata. ■

Definición 4.3.3
Sea E/F una extensión finita arbitraria. Se define **el grado de inseparabilidad de la extensión** E/F como:

$$[E:F]_i := \frac{[E:F]}{[E:F]_s}$$

Notemos que si $\mathrm{car}(F) = 0$, entonces $[E:F]_i = 1$. Si $\mathrm{car}(F) = p > 0$, entonces $[E:F]_i = p^t$, para algún $t \in \mathbb{Z}_{\geq 0}$.

Observación 4.3.4
Sea E/F una extensión finita. Si K es un campo intermedio de la extensión E/F, entonces

$$[E:F]_i = [E:K]_i \cdot [K:F]_i$$

Si E/F es una extensión finita con $\mathrm{car}(F) = p > 0$, entonces E/F es p.i. si y sólo si $[E:F] = [E:F]_i$.

Observación 4.3.5
Sea E/F una extensión finita con $\mathrm{car}(F) = p > 0$. Si $p \nmid [E:F]$ entonces $[E:F]_i = 1$, es decir la extensión E/F es separable.

Proposición 4.3.5
Sea F un campo, $\alpha_1, ..., \alpha_n, \beta \in \bar{F}$ tales que $\alpha_1, ..., \alpha_n$ son separables sobre F. Si F es infinito entonces, existe $\theta \in F(\alpha_1, ..., \alpha_n, \beta)$ tal que:

$$F(\alpha_1, ..., \alpha_n, \beta) = F(\theta)$$

Demostración:

Procederemos por inducción sobre n. Para $n = 1$, suponemos que tenemos la extensión $F(\alpha_1, \beta)/F$ donde α_1 es separable sobre F y β simplemente es algebraico sobre F. Denotemos por $f(X) = \mathrm{irr}\,(\alpha_1, F, X)$ y $g(X) = \mathrm{irr}\,(\beta, F, X)$, con $m = \deg f$ y $k = \deg g$.

Sean $\delta_1, ..., \delta_m$ y $\beta_1, ..., \beta_r$ las raíces distintas de $f(X)$ y $g(X)$, respectivamente, donde $r \leq k$. Consideremos las ecuaciones lineales siguientes:

$$\delta_1 X + \beta_1 = \delta_i X + \beta_j$$

con $i \in [\![2, m]\!]$ y $j \in [\![1, r]\!]$. Si δ_1 fuera la única raíz de $f(X)$, esto es $m = 1$, entonces $f(X) = X - \delta_1 \in F[X]$, luego $\alpha_1 = \delta_1 = \in F$. Por ende, $F(\alpha_1, \beta) = F(\beta)$. Así, basta tomar $\theta = \beta$.

Supongamos que δ_1 no es la única raíz de $f(X)$, es decir que $m \geq 2$. Hacemos $\delta_1 = \alpha_1$ y $\beta_1 = \beta$. Se tiene que las ecuaciones anteriores están bien determinadas.

Elegimos un elemento $a \in F$ tal que

$$a\delta_1 + \beta_1 \neq a\delta_i + \beta_j$$
$$\Rightarrow a\alpha_1 + \beta \neq a\delta_i + \beta_j$$

para todo $i \in [\![1, m]\!]$ y para todo $j \in [\![1, r]\!]$. Tal elemento existe ya que F es infinito. Definimos

$$\theta = a\delta_1 + \beta \in F(\alpha_1, \beta)$$

probemos que $F(\alpha_1, \beta) = F(\theta)$. Por lo de arriba se sigue que $F(\theta) \subseteq F(\alpha_1, \beta)$. Basta probar que $\alpha_1, \beta \in F(\theta)$. Para ello, consideremos el polinomio $h(X) = g(\theta - aX) \in F(\theta)[X]$.

Notemos que $h(\alpha_1) = g(a\alpha_1 + \beta_1 - a\alpha_1) = g(\beta) = 0$ y,

$$\begin{aligned} h(\delta_i) &= g(\theta - a\delta_i) \\ &= g((a\delta_1 + \beta_1) - a\delta_i) \\ &\neq 0, \quad \forall i \in [\![2, m]\!] \end{aligned}$$

pues, $(a\delta_1 + \beta_1) - a\delta \neq \beta_j$ para todo $j \in [\![1, m]\!]$, es decir que nunca puede ser alguna raíz de g. Así pues, h y f tienen solamente una raíz en común, a saber, α_1, donde $h(X), f(X) \in F(\theta)[X]$.

Sea $d(X) \in F(\theta)[X]$ el máximo común divisor de $h(X)$ y $f(X)$ (el cual existe pues este anillo es dominio euclideano), donde

$$d(X) = l(X)h(X) + t(X)f(X)$$

siendo $l(X), t(X) \in F(\theta)[X]$. Notemos de la ecuación anterior que

$$d(\alpha_1) = 0$$

y, toda raíz de $d(X)$ es raíz de $f(X)$ y $h(X)$ (pues es el M.C.D.) pero, como $f(X)$ y $h(X)$ tienen a α_1 como única raíz, entonces $d(X)$ solo tiene como raíz a α_1. Por ende,

$$d(X) = X - \alpha_1$$

(el coeficiente lider es 1 ya que $f(X)$ es separable y $d(X) \mid f(X)$). Por tanto,

$$X - \alpha_1 = l(X)h(X) + t(X)f(X) \in F(\theta)[X]$$

por tanto, $\alpha_1 \in F(\theta)$. En particular, como $a \in F$ entonces $a\alpha \in F(\theta)$, luego

$$\beta = (a\alpha + \beta) - a\alpha = \theta - a\alpha \in F(\theta)$$

por tanto, $\alpha_1, \beta \in F(\theta)$. Finalmente se tiene que

$$F(\theta) = F(\alpha_1, \beta)$$

De aquí que la proposición se cumple para $n = 1$. Suponga que se cumple para algún $n \in \mathbb{N}$, probaremos que se cumple para $n + 1$. En efecto, sean $\alpha_1, ..., \alpha_{n+1} \in \bar{F}$ separables sobre F y $\beta \in \bar{F}$ algebraico.

Por hipótesis de inducción, existe $\theta_1 \in F(\alpha_1, ..., \alpha_n, \beta)$ tal que

$$F(\theta_1) = F(\alpha_1, ..., \alpha_n, \beta)$$

y, por el caso $n = 1$ existe $\theta \in F(\alpha_1, ..., \alpha_{n+1}, \beta)$ tal que

$$F(\theta) = F(\alpha_{n+1}, \theta_1)$$

luego,

$$\begin{aligned} F(\theta) &= F(\alpha_{n+1}, \theta_1) \\ &= F(\theta_1)(\alpha_{n+1}) \\ &= F(\alpha_1, ..., \alpha_n, \beta)(\alpha_{n+1}) \\ &= F(\alpha_1, ..., \alpha_{n+1}, \beta) \\ \Rightarrow F(\theta) &= F(\alpha_1, ..., \alpha_{n+1}, \beta) \end{aligned}$$

lo que prueba el caso $n + 1$. ■

Corolario 4.3.3
Sea F un campo perfecto. Entonces, toda extensión E/F finita es simple.

Demostración:
Es inmediata. ■

Corolario 4.3.4
Si F es un campo de característica cero, entonces toda extensión E/F finita es simple.

Demostración:
Todo campo de característica cero es perfecto. ■

Ejemplo 4.3.1
Toda extensión $E/\mathbb{Q}$ finita es simple. En particular, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. En este caso, $\alpha_1 = \sqrt{2}$ y $\beta = \sqrt{3}$ (en realidad da igual cual elijamos ya que cualquiera de estos dos elementos son separables sobre $\mathbb{Q}$ por ser este de característica cero). Así,

$$\alpha_1 = \delta_1 = \sqrt{2} \quad \text{y} \quad \delta_2 = -\sqrt{2}$$

además,

$$\beta = \beta_1 = \sqrt{3} \quad \text{y} \quad \beta_2 = -\sqrt{3}$$

uno de los posibles $a \in \mathbb{Q}$ que nos sirven es $a = 1$, ya que las ecuaciones que tenemos son:

$$\begin{cases} \sqrt{2}X + \sqrt{3} & = -\sqrt{2}X + \sqrt{3} \\ \sqrt{2}X + \sqrt{3} & = -\sqrt{2}X - \sqrt{3} \end{cases}$$

siendo $X = a = 1$ el que hace que no se cumpla la ecuación. Luego es por ello que tomamos $\theta = 1 \cdot \sqrt{2} + \sqrt{3} = \sqrt{2} + \sqrt{3}$.

Lema 4.3.1
Para $n \in \mathbb{N}$:

$$n = \sum_{d|n \text{ y } d \geq 1} \varphi(d)$$

donde φ es la función de Euler.

Demostración:
Ejercicio. ■

Lema 4.3.2
Sea G un grupo abeliano finito y multiplicativo tal que la ecuación $X^m = e$ tiene a lo más m soluciones en G. Entonces, G es grupo cíclico.

Demostración:
Ejercicio. ■

Proposición 4.3.6
Si F es un campo, entonces F^* es un grupo multiplicativo y cada subgrupo finito de F^* es cíclico.

Demostración:

Se sigue del lema anterior. ■

Teorema 4.3.2 (Teorema del elemento primitivo)
Toda extensión finita y separable de campos es simple.

Demostración:

Sea E/F una extensión finita y separable. Si F es un campo infinito, tenemos que E/F es f.g. con elementos separables y F finito. Por tanto, E/F es simple.

Si F es finito, E también es finito. Más aún,

$$|E| = n|F|$$

entonces, E^* es grupo multiplicativo abeliano y finito. Luego por una proposición anterior, es cíclico (visto como grup multiplicativo). Sea $\theta \in E^*$ tal que

$$\begin{aligned} E^* &= \langle\theta\rangle \\ &= \left\{\theta^t \middle| t \in \mathbb{N}\right\} \end{aligned}$$

luego, $E = F(\theta)$. Así, la extensión E/F es simple.

■

Observación 4.3.6
El θ de la proposición anterior es llamado **elemento primitivo**.