

## EXTENSIONES DE CAMPOS.

**Def.** Sea  $F/K$  una extensión de campos.<sup>1)</sup> El grado de la extensión  $F/K$ , denotada por  $[F:K]$ , es la dimensión de  $F$  como esp. vect. sobre  $K$ . Es decir:

$$[F:K] = \dim_K F$$

**Def.** Decimos que  $F/K$  es una extensión finita, si  $[F:K] < \infty$ . En caso contrario, decimos que es una extensión infinita, y lo escribimos como  $[F:K] = \infty$ .

### Teorema.

Sea  $K \subseteq F \subseteq E$  una torre de campos (también llamada cadena de campos). Entonces:

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

**Dem:**

Sea  $\{\alpha_i\}_{i \in I}$  y  $\{\beta_j\}_{j \in J}$  base de  $F$  sobre  $K$  y base de  $E$  sobre  $F$ , respectivamente.

$\begin{matrix} E \\ | \\ F \\ | \\ K \end{matrix} \quad \{B_j\}$  Afirmamos que  $\{\alpha_i \beta_j\}_{(i,j) \in I \times J}$  es base de  $E$  sobre  $K$ . Claramente  $\alpha_i \beta_j \in E, \forall (i,j) \in I \times J$ . Notemos que necesariamente:

$$|\{\alpha_i \mid i \in I\}| = |I|, \quad |\{\beta_j \mid j \in J\}| = |J|$$

Por ser bases. Sea  $\alpha \in E$ , entonces  $\alpha$  se expresa de manera única como combinación lineal de la base de los  $\beta_j$  sobre  $F$ :

$$\alpha = \sum_{j \in J} b_j \beta_j \quad (b_j \in F \text{ y } b_j = 0 \nabla j \in J).$$

Por otro lado, cada  $b_j \in F$  se expresa de manera única como una combinación lineal de la base  $\{\alpha_i\}_{i \in I}$  sobre  $K$ :

$$b_j = \sum_{i \in I} a_{ij} \alpha_i \quad (a_{ij} \in K \text{ y } a_{ij} = 0 \nabla i \in I), \quad \forall j \in J.$$

$$\Rightarrow \alpha = \sum_{j \in J} \left( \sum_{i \in I} a_{ij} \alpha_i \right) \beta_j$$

$$= \sum_{(i,j) \in I \times J} a_{ij} (\alpha_i \beta_j), \quad \text{donde } a_{ij} \in K, \quad \forall (i,j) \in I \times J \text{ y } a_{ij} = 0 \nabla (i,j) \in I \times J.$$

Luego  $E = \sum_{(i,j) \in I \times J} \{ \alpha_i \beta_j \mid (i,j) \in I \times J \}$  (i.e. generan a  $E$  sobre  $K$ ). Probemos que  $\{\alpha_i \beta_j\}_{(i,j) \in I \times J}$  es l.i. sobre  $K$ . Sea

$$\begin{aligned} \sum_{(i,j) \in I \times J} \alpha_i \beta_j &= 0 \\ \Rightarrow \sum_{j \in J} \left( \sum_{i \in I} \alpha_i \beta_i \right) \beta_j &= 0 \end{aligned}$$

Como  $\{\beta_j\}_{j \in J}$  es base de  $E$  sobre  $F$ , ent.  $\sum_{i \in I} \alpha_i \beta_i = 0, \forall j \in J$ , pero  $\{\alpha_i\}_{i \in I}$  es base de  $F$  sobre  $K \Rightarrow \alpha_i = 0, \forall (i,j) \in I \times J$ .

Por tanto  $\{\alpha_i \beta_j\}_{(i,j) \in I \times J}$  es l.i. sobre  $K$ . Así  $\{\alpha_i \beta_j\}_{(i,j) \in I \times J}$  es base de  $E$  sobre  $K$ , y:

$$\begin{aligned} |\{\alpha_i \beta_j \mid (i,j) \in I \times J\}| &= |I \times J| = |I| |J| \\ \Rightarrow [E : K] &= [E : F] [F : K] \end{aligned}$$

□

## EJEMPLOS

1) Si  $p, q \in \mathbb{N}$  números primos distintos. Podemos suponer que  $p < q$ . Definimos

$$\begin{aligned} F &= \mathbb{Q}(\sqrt{p}) \\ &= \{a + b\sqrt{p} \mid a, b \in \mathbb{Q}\} \end{aligned}$$

Sabemos que  $F$  es una extensión de  $\mathbb{Q}$ . Además  $[F : \mathbb{Q}] = 2$  pues  $\{1, \sqrt{p}\}$  es base de  $F$  sobre  $\mathbb{Q}$ .

De manera similar, definimos

$$\begin{aligned} E &= F(\sqrt{q}) \\ &= \{a + b\sqrt{q} \mid a, b \in F\} \end{aligned}$$

Afirmamos que  $E$  es campo. Notamos que  $E \subseteq \mathbb{R}$  y  $F \subseteq \mathbb{R}$ , por donde  $F$  es subcampo de  $\mathbb{R}$ . Para ello, notemos que  $\forall \alpha, \beta \in F$ ,

$$\alpha + \beta \sqrt{q} = 0 \Leftrightarrow \alpha = \beta = 0$$

En efecto, si  $\alpha + \beta \sqrt{q} = 0$  entonces si  $\beta \neq 0 \Rightarrow \sqrt{q} \in F \Rightarrow \sqrt{q} = a + b\sqrt{p}$  con  $a, b \in \mathbb{Q}$

$$\Rightarrow q = a^2 + 2ab\sqrt{p} + b^2 p$$

$\Rightarrow ab = 0$ . Si  $a = 0 \circ b = 0$ , llegamos a un absurdo. Por tanto  $B = 0 \Rightarrow \alpha = 0$ . Luego, cada elemento de  $E$  se expresa de manera única en la forma  $\alpha + B\sqrt{q}$  donde  $q, B \in F$ .

Sean  $x, y \in E$ , con  $x = \alpha + B\sqrt{q}$  y  $y = r + \delta\sqrt{q}$  ( $\alpha, B, r, \delta \in F$ ). Entonces:

$$x - y = \alpha - r + (B - \delta)\sqrt{q}$$

donde  $\alpha - r, B - \delta \in F$ , así  $x - y \in E$ . Y:

$$xy = (\alpha r + qB\delta) + (\alpha\delta + \beta r)\sqrt{q}$$

Con  $\alpha r + qB\delta, \alpha\delta + \beta r \in F$ . Así  $xy \in E$ . Y:

$$x^{-1} = \frac{1}{\alpha + B\sqrt{q}} = \frac{\alpha - B\sqrt{q}}{\alpha^2 - B^2 q} = \left(\frac{\alpha}{\alpha^2 - B^2 q}\right) + \left(\frac{-B}{\alpha^2 - B^2 q}\right)\sqrt{q} \in E$$

Si  $x \neq 0$ , pues cada entrada está en  $F$ .  $\therefore x - y, xy, x^{-1} \in E$ , así  $E$  es subcampo de  $\mathbb{R}$ . Por lo tanto:

$$[E : F] = 2, \text{ con base } \{1, \sqrt{q}\}$$

$$\Rightarrow [E : \mathbb{Q}] = 4 \text{ con base } \{1, \sqrt{p}, \sqrt{q}, \sqrt{pq}\}$$

## Proposición.

Sea  $p_1, \dots, p_n \in \mathbb{N}$  primos distintos s.t.  $p_i < p_{i+1}$ ,  $\forall i \in [1, n-1]$ . Definimos por recursión  $E_0 = \mathbb{Q}$

y

$$\begin{aligned} E_i &= E_{i-1}(p_i), \forall i \in [1, n] \\ &= \{ \alpha + B\sqrt{p_i} \mid \alpha, B \in E_{i-1} \}, \forall i \in [1, n] \end{aligned}$$

Entonces  $E_0 \subseteq E_1 \subseteq \dots \subseteq E_n$  es una torre de campos tal que la extensión  $E_i/E_{i-1}$  con una base  $\{1, \sqrt{p_i}\}, \forall i \in [1, n]$ . En particular.

$$[E_n : E_0] = 2^n$$

## Dem.

La demostración será por inducción sobre  $n$ .

**Notación.** Los campos  $E_i$  de la prop. ant. se denotan como:

$$E_i = Q(\sqrt{p_1}, \dots, \sqrt{p_i}), \forall i \in [1, n].$$

Así que, la torre de campos que se tiene es:

$$\mathbb{Q} \subseteq Q(\sqrt{p_1}) \subseteq Q(\sqrt{p_1}, \sqrt{p_2}) \subseteq \dots \subseteq Q(\sqrt{p_1}, \dots, \sqrt{p_n})$$

donde  $\sqrt{p_i} \notin Q(\sqrt{p_1}, \dots, \sqrt{p_{i-1}})$ ,  $\forall i \in [2, n]$ .

## CONSTRUCCIONES.

Sea  $E$  un campo y  $S \subseteq E$  arbitrario. Entonces, tenemos que el conjunto de subcampos (o subanillos) de  $E$  que contienen a  $S$  es no vacío. Sea  $\mathcal{F}$  dicho conjunto, i.e

$$\mathcal{F} = \{T \subseteq E \mid T \text{ es subcampo (resp. subanillo) de } E \text{ y } S \subseteq T \text{ NO TRIVIALES}\}^{2)}$$

Sabemos que  $\bigcap_{T \in \mathcal{F}} T$  es subcampo (resp. subanillo de  $E$ ) el cual lo denotaremos como  $(S)$  (resp  $[S]$ ).

Tenemos que  $(S)$  (resp.  $[S]$ ) es el mínimo subcampo (resp. subanillo) de  $E$  que contiene a  $S$ .  
 $(S)$  es llamado el **subcampo**

(resp. **subanillo**) generado por  $S$ . Al conjunto  $S$  se le llama un **conjunto de generadores del subcampo** ( $S$ ) (resp. **subanillo**  $[S]$ ).

S:  $S = \emptyset$  entonces  $(S) = (\emptyset)$  es el llamado el **Campo primo** de  $E$ , y denotado por  $P_E$ , es decir, si  $K$  es subcampo de  $E \Rightarrow P_E \subseteq K$ .

Por lo general, siempre supondremos que  $S \neq \emptyset$ . Si,  $S \subseteq E$  y  $K$  es subcampo de  $E$ , entonces denotamos por  $K(S)$  (resp.  $K([S])$ ) a  $(K \cup S)$  (resp.  $[K \cup S]$ ). Si  $K$  y  $L$  son subcampos de  $E$  entonces  $(L \cup K)$  (resp.  $[L \cup K]$ ) es denotado por  $KL = LK$  (resp.  $K[L] = L[K]$ ). Pero  $K(L) = L(K)$ .  $KL$  es llamado el **complejo** de  $K$  y  $L$ .

S:  $S$  es un subconjunto finito de  $E$ , con  $S = \{u_1, \dots, u_n\}$ , entonces escribimos

$$K(u_1, \dots, u_n) = K/\{u_1, \dots, u_n\}) \quad (\text{resp. } K(u_1, \dots, u_n) = K(\{u_1, \dots, u_n\}))$$

$S; E/K$  es una extensión de campos, entonces decimos que  $E/K$  es finitamente generado. (f.g)

S. existen  $u_1, \dots, u_n \in E$  m  $E = K(u_1, \dots, u_n)$ .

### Teorema.

S.  $u \in E$  un campo,  $K$  subcampo de  $E$ ,  $S \subseteq E$  ( $S \neq \emptyset$ ), y  $u, u_1, \dots, u_n \in E$ . Ent.

i)  $K(u) = \{f(u) \mid f(x) \in K(x)\}$ .

ii)  $K(u_1, \dots, u_n) = \{f(u_1, \dots, u_n) \mid f(x_1, \dots, x_n) \in K(x_1, \dots, x_n)\}$ .

iii)  $K(S) = \{f(v_1, \dots, v_m) \mid f(x_1, \dots, x_m) \in K(x_1, \dots, x_m), v_i \in S, \forall i \in [1, m]; m \in \mathbb{N}\}$ .

iv)  $K(u) = \left\{ \frac{f(u)}{g(u)} \mid f(x), g(x) \in K(x), g(u) \neq 0 \right\}$ .

v)  $K(u_1, \dots, u_n) = \left\{ \frac{f(u_1, \dots, u_n)}{g(u_1, \dots, u_n)} \mid f(x_1, \dots, x_n), g(x_1, \dots, x_n) \in K(x_1, \dots, x_n), g(u_1, \dots, u_n) \neq 0 \right\}$ .

vi)  $K(S) = \left\{ \frac{f(v_1, \dots, v_m)}{g(v_1, \dots, v_m)} \mid f(x_1, \dots, x_m), g(x_1, \dots, x_m) \in K(x_1, \dots, x_m), v_i \in S, \forall i \in [1, m], g(v_1, \dots, v_m) \neq 0 \right. \\ \left. ; m \in \mathbb{N} \right\}$ .

Dem:<sup>3)</sup>

**Obs)** Sean  $E$ ,  $K$  campos, y  $f: E \rightarrow K$  un homomorfismo. Ent.  $f$  es el homomorfismo trivial o  $f$  es monomorfismo. En el segundo caso,  $f(1_E) = 1_K$  y luego,  $f(\alpha^{-1}) = f(\alpha)^{-1}$ ,  $\forall \alpha \in E$ .

**Def.** Sea  $E/F$  una extensión de campos y  $\alpha \in E$ . Se dice que  $\alpha$  es algebraico sobre  $F$ , si existe un polinomio  $h(x) \in F[x] \setminus \{0\}$  m  $h(\alpha) = 0$ .

### EJEMPLOS.

1) Sea  $E/F$  una extensión de campos y  $\alpha \in E$ . Entonces  $\alpha$  es algebraico sobre  $F$  ya que  $\exists f(x) = x - \alpha \in F[x]$  m  $f(\alpha) = \alpha - \alpha = 0$ . Ent.

$$F \subseteq \{\alpha \in E \mid \alpha \text{ es algebraico sobre } F\}$$

2) Sea  $p \in \mathbb{N}$  número primo. En la extensión  $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$ ,  $\alpha = \sqrt{p}$  es algebraico sobre  $\mathbb{Q}$ , pues  $x^2 - p \in \mathbb{Q}[x]$  y  $\alpha$  es raíz de ese polinomio.

3) En la extensión  $\mathbb{Q}/\mathbb{Q}$ ,  $\pi$  no es algebraico sobre  $\mathbb{Q}$ , pero en  $\mathbb{C}/\mathbb{R}$  sí lo es.

4) Sea  $F \subseteq K \subseteq E$  una extensión de campos. Entonces si  $\alpha \in E$  es algebraico sobre  $F$ , también lo es sobre  $K$ , pues  $F[x] \subseteq K[x]$ .

**Def.** Si  $E/F$  es una extensión de campos y  $\alpha \in E$  no es algebraico sobre  $F$ , se dice que  $\alpha$  es trascendente sobre  $F$ .

### Teorema.

Sea  $E/F$  una extensión de campos y  $\alpha \in E$ . Las sig. cond. son equivalentes:

i)  $\alpha$  es algebraico sobre  $F$ .

ii)  $F(\alpha) = F[\alpha]$ .

iii)  $F(\alpha)/F$  es una extensión finita.

### Dem.

(ii)  $\Rightarrow$  (iii):

Se construyó el polinomio en  $F[x]$  mónico y de mínimo grado  $m$   $f(\alpha) = 0$ . Si  $n = \text{grad}(f(x)) \Rightarrow \{1, \alpha, \dots, \alpha^{n-1}\}$  es base de  $F(\alpha)$  sobre  $F$ , i.e.

$B \in F(\alpha) \Rightarrow \beta = g(\alpha), g(x) \in F[x]$  y:

$$g(x) = q(x)f(x) + r(x)$$

donde  $r(x) = 0$  o  $\text{grad}(r(x)) < \text{grad}(f(x))$ . Luego  $\beta = g(\alpha) = r(\alpha) \Rightarrow \beta \in F(1, \alpha, \dots, \alpha^{n-1})$ .

Probemos que  $\{1, \alpha, \dots, \alpha^{n-1}\}$  es l.d. sobre  $F$ . Supóngase que  $\{1, \alpha, \dots, \alpha^{n-1}\}$  es l.d. sobre  $F$ .

Entonces  $\exists d_0, d_1, \dots, d_{n-1} \in F$  no todos cero m

$$d_0 \cdot 1 + d_1 \alpha + \dots + d_{n-1} \alpha^{n-1} = 0$$

$\Rightarrow f(x) = d_0 + d_1 x + \dots + d_{n-1} x^{n-1} \in F[x] \setminus \{0\}$  y  $f_0(\alpha) = 0$ , lo cual contradice la minimalidad del grado de  $f(x)$ . Por tanto  $\{1, \alpha, \dots, \alpha^{n-1}\}$  es base de  $F(\alpha)/F$ . En particular,  $F(\alpha)/F$  es una extensión finita.

(iii)  $\Rightarrow$  (i):

Sea  $n = [F(\alpha) : F] < \infty$ . Consideremos el conjunto formado por  $\{1, \alpha, \dots, \alpha^n\}$ . Notemos que

podemos suponer que  $\alpha \notin F$ . Si  $\exists m, k \in \mathbb{Z}$  con  $0 \leq k < m \leq n$  m  $\alpha^k = \alpha^m \Rightarrow \alpha^{m-k} = 1$ , con  $0 < m-k < n \Rightarrow \alpha$  es raíz del pol.  $g(x) = x^{m-k} - 1 \in F[x] \Rightarrow \alpha$  algebraico sobre  $F$ .

De aquí que, podemos suponer que  $|\{1, \alpha, \dots, \alpha^n\}| = n+1$ . Luego  $\{1, \alpha, \dots, \alpha^n\}$  es l.d. sobre  $F$ , pues  $[F(\alpha) : F] = n$ , luego  $\exists \lambda(x) \in F[x] \setminus \{0\}$  m  $\text{grad}(\lambda(x)) \leq n$  m

$$\lambda(\alpha) = 0$$

por tanto,  $\alpha$  es algebraico sobre  $F$ .

□

Obs) Sea  $E/F$  una extensión de campos y  $\alpha \in E$  algebraico sobre  $F$ . Sea  $f(x) \in F[x]$  el

polinomio mónico de mínimo grado m  $f(\alpha)$  es raíz. Ent.

i)  $f(x)$  es el único pol. mónico de mínimo grado tal que  $f(\alpha) = 0$ . Si hubiera otro de

mismo grado, digamos  $f_1(x) \in F[x]$  m  $f_1(x) \neq f(x)$  y  $f_1(\alpha) = 0$ , ent.

$$f_1(x) - f(x) \neq 0$$

$\text{grad}(f_1(x) - f(x)) < \text{grad}(f(x))$  y  $f_1(\alpha) - f(\alpha) = 0 \neq 0$ . Por tanto el  $f(x)$  es único.

ii)  $f(x)$  es un polinomio irreducible en  $F[x]$ .

iii)  $F[x]/\langle f(x) \rangle$  es un campo isomorfo a  $F[\alpha] = F(\alpha)$ . Es decir:

$$F[x]/\langle f(x) \rangle \xrightarrow{\sim} F(\alpha) = F(\alpha)$$

$$h(x) + \langle f(x) \rangle \mapsto h(\alpha)$$

iv) Si  $n = \text{grad}(f(x))$ , entonces

$$[F(\alpha) : F] = n = \text{grad}(f(x)).$$

v)  $\{1, \alpha, \dots, \alpha^{n-1}\}$  es base de  $F(\alpha)$  sobre  $F$ .

El polinomio  $f(x)$  es llamado el **irreducible de  $\alpha$  sobre  $F$** , y denotado por:

$$f(x) = \text{irr}(\alpha, F) \text{ ó}$$

$$f = \text{irr}(\alpha, F, x)$$

$$\begin{aligned} \text{vii)} \quad \langle f(x) \rangle &= \{ q(x)f(x) \mid q(x) \in F[x] \} \\ &= \{ g(x) \in F[x] \mid g(\alpha) = 0 \} \\ &= \{ g(x) \in F[x] \mid f(x) \mid g(x) \} \end{aligned}$$

**Def.** Sea  $E/F$  una extensión de campos. La extensión  $E/F$  es **algebraico**, si todo  $\alpha \in E$  es algebraico sobre  $F$ . En caso cont. decimos que la extensión es **trascendente**.

### Proposición.

Sea  $E/F$  una extensión de campos,  $S \subseteq E$  no vacío y  $K = \{ \alpha \in E \mid \alpha \text{ es algebraico sobre } F \}$ .

Entonces:

i)  $K$  es subcampo de  $E$  que es extensión de  $F$ .

ii) Si  $S \subseteq K$ ,  $E = F(S)$ , entonces  $E/F$  es algebraica.

**Dem.**

De (i): Ya sabemos que  $F \subseteq K \subseteq E$ . Sean  $\alpha, \beta \in K$ , por tanto  $F(\alpha)/F$  es una exten-  
sión finita, donde  $\beta$  es algebraico sobre  $F(\alpha)$ , luego

$$F(\alpha)/F \quad \& \quad F(\alpha, \beta)/F(\alpha)$$

son extensiones finitas, donde  $F(\alpha, \beta) = F(\alpha)(\beta)$  y los grados son multiplicativos, lue-  
go:

$$[F(\alpha, \beta) : F] < \infty$$

donde  $r \in F(\alpha, \beta)$  siendo  $r \in \{\alpha - \beta, \alpha\beta, \alpha^{-1}\}$  (cuando  $\alpha \neq 0$ ). Como

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

es una torre de campos con  $[F(\alpha, \beta) : F] < \infty \Rightarrow [F(r) : F] < \infty \Rightarrow r$  es algebraico sobre  
 $F \Rightarrow \alpha - \beta, \alpha\beta, \alpha^{-1} \in K$ .

Por tanto,  $K$  es subcampo de  $E$ , y campo intermedio de la extensión  $E/F$ .

De (ii): Tenemos que  $S \subseteq K$ , por lo cual

$$\underline{E} = F(S) \subseteq K$$

y  $K \subseteq E \Rightarrow K = E$ . Por tanto  $E/F$  es una extensión algebraica.

□

**EJEMPLOS.**

1) Sean  $E/F$  una extensión de campos y  $\alpha \in E$  m  $\alpha$  es algebraico sobre  $F$ . Entonces  $\frac{F(\alpha)}{F}$   
es algebraica.

2) Sean  $p_1, \dots, p_n \in \mathbb{N}$  primos dist. entre si, i.e.  $p_1 < p_2 < \dots < p_n$ . Entonces  $\frac{\mathbb{Q}(p_1, \dots, p_n)}{\alpha}$   
es una extensión algebraica de grado  $2^n$ .

3) Sean  $F(x)$  el campo de funciones racionales con coef. en  $F$  en la indeterminada  $x$ . Es decir:

$$F(x) = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in F[x], g(x) \neq 0 \right\}$$

entonces  $\frac{F(x)}{F}$  es una extensión de campos la cual es trascendente sobre  $F$ , ya que  $x \in$

$F(x)$  es trascendente sobre  $F$  (por ser  $x$  una indeterminada).

**Def.** Sea  $E/F$  una extensión de campos,  $\alpha \in E$  &  $K = \{B \in E \mid B \text{ es algebraico sobre } F\}$ .

i) Si  $\alpha \in E$  es algebraico sobre  $F$ , el grado de  $\alpha$  sobre  $F$ , es el grado de  $\text{irr}(\alpha, F)$ ,

$$\text{i.e. } [F(\alpha) : F].$$

ii) El campo intermedio  $K$  de la extensión  $E/F$  es llamado la Cerradura algebraica de  $F$  en  $E$ , o la Cerradura algebraica de la extensión  $E/F$ , y es denotado por  $\bar{F}_E$ ,  $\bar{F}_{E/F}$  o  $\bar{F}$  (si no hay confusión).

### Proposición.

Sea  $E/F$  una extensión de campos.  $E/F$  es extensión finita  $\Leftrightarrow E/F$  es algebraica y f.g.

### Dem.

$\Rightarrow$ ) Supongamos que  $E/F$  es finita. Se tienen dos casos:

i)  $[E : F] = 1$ , ent. por un ejercicio  $E = F = F(1)$ , i.e.  $E/F$  es algebraica y finitamente generada.

ii)  $[E : F] > 1$ . Antes, notemos que si  $K \subseteq E$  es un campo intermedio de la extensión, se debe tener que:

$$[E : F] = [E : K][K : F] < \infty$$

i.e.  $[K : F], [E : K] < \infty$ . En particular, si  $\alpha \in E$  y  $K = F(\alpha)$ , ent.  $[F(\alpha) : F], [E : F(\alpha)] < \infty$ . Como  $[E : F] > 1$  ent.  $E \neq F$ . Sea  $u_1 \in E \setminus F$ . Se tiene ent. la sig. torre de campos:

$$F \subsetneq F(u_1) \subseteq E$$

Si  $F(u_1) = E$ , habremos terminado. Si  $F(u_1) \neq E$  ent.  $\exists u_2 \in E \setminus F(u_1)$  m

$$F \subsetneq F(u_1) \subsetneq F(u_1, u_2) \subseteq E$$

Si  $F(u_1, u_2) = E$ , ent. habremos terminado. Si  $F(u_1, u_2) \neq E$ , continuaremos el proceso, el cual debe concluir en una cantidad finita de pasos, ya que la extensión  $E/F$  es finita.

Es decir, existirán  $u_1, \dots, u_m \in E$  m

$$F \subsetneq F(u_1) \subsetneq F(u_1, u_2) \subsetneq \dots \subsetneq F(u_1, \dots, u_m) = E$$

donde

$$2^{m-1} \leq [E : F(u_1, \dots, u_m)] \cdot [F(u_1, \dots, u_m) : F(u_1, \dots, u_{m-1})] \cdot \dots \cdot [F(u_1) : F] = [E : F] < \infty$$

Por lo tanto,  $E/F$  es algebraica y f.g. con  $E = F(u_1, \dots, u_m)$ .

$\Leftarrow$ ) Supongamos que  $E/F$  es algebraica y f.g. Sean  $u_1, \dots, u_m \in E$  m

$$E = F(u_1, \dots, u_m)$$

$u_1 \in E$  es algebraico sobre  $F$ , i.e.  $[F(u_1) : F] < \infty$ .  $u_2 \in E$  es algebraico sobre  $F$ , luego

sobre  $F(u_1) \Rightarrow [F(u_1, u_2) : F(u_1)] < \infty$ . Continuando con el proceso, tenemos que cada  $u_i$  ( $i \in [2, m]$ ) es algebraico sobre  $F(u_1, \dots, u_{i-1})$ , i.e.

$$[F(u_1, \dots, u_i) : F(u_1, \dots, u_{i-1})] < \infty, \forall i \in [2, m]$$

Por tanto:

$$[E : F] = [E : F(u_1, \dots, u_{m-1})] \cdot [F(u_1, \dots, u_{m-1}) : F(u_1, \dots, u_{m-2})] \cdot \dots \cdot [F(u_1) : F] < \infty$$

□

### Proposición.

Sea  $E/F$  una extensión de campos y  $\bar{F}$  la cerradura algebraica de  $F$  en  $E$ ,  $\alpha \in E$  algebraico sobre  $\bar{F}$ . Ent.  $\alpha \in \bar{F}$ . (i.e  $\bar{F} = \bar{\bar{F}}$ ).

### Dem.

Probaremos el resultado de una forma más general. Probaremos que si  $K$  es un campo intermedio de la extensión  $E/F$  tal que  $K/F$  es algebraica, ent.  $\alpha$  algebraico sobre  $K$   $\Rightarrow \alpha$  algebraico sobre  $F$ , es decir  $\bar{K} \subseteq \bar{F}$ .

En efecto, sea  $\alpha \in \bar{K}$  y  $g(x) = \text{irr}(\alpha, K, x)$ , digamos

$$g(x) = a_0 + a_1 x + \dots + a_n x^n$$

donde  $a_i \in K$ ,  $\forall i \in [0, n]$ . En part.  $g(x) \in F(a_0, \dots, a_n)[x]$ , i.e  $\alpha$  es algebraico en

$F(a_0, \dots, a_n)$ . Entonces  $[F(a_0, \dots, a_m, \alpha) : F(a_0, \dots, a_m)] < \infty$ . Pero  $F(a_0, \dots, a_m)$  es extensión algebraica y f.g. de  $F$ . En efecto, est.g. Veamos que es algebraica, ya que  $\{a_0, \dots, a_m\} \subseteq \bar{F}$ , por tanto  $F(a_0, \dots, a_m)/F$  es algebraica.

En part. es finito. Luego son finitas:

$$[F(a_0, \dots, a_m, \alpha) : F(a_0, \dots, a_m)] \text{ y } [F(a_0, \dots, a_m) : F] < \infty$$

$$\Rightarrow [F(a_0, \dots, a_m, \alpha) : F] < \infty$$

Por tanto  $F(a_0, \dots, a_m, \alpha)/F$  es finito  $\Rightarrow$  es algebraica. Luego  $\alpha \in \bar{K}$  es algebraico sobre  $F$

$$\Rightarrow \alpha \in \bar{F}$$

□

Sean  $E/K$  y  $F/K$  dos extensiones de campos, con  $E$  y  $F$  subcampos de un campo común  $L$ . Consideremos el compuesto de  $E$  y  $F$ ,  $EF$ , el cual es subcampo de  $L$ . Ent. la

extensión  $EF/F$  (resp.  $E/F$ ) es llamada el **transladado de la extensión  $E/K$** .

(resp.  $F/K$ ) en  $F$  (resp. en  $E$ ).

K es llamado el **campo base de la extensión**.

**Def.** Sean  $\mathcal{C}$  una clase de extensiones de campos. Decimos que  $\mathcal{C}$  es una **clase distinguida**, si cumple las sig. prop.

a) Sean  $K \subseteq F \subseteq E$  una torre de campos. Entonces,

$$E/K \in \mathcal{C} \Leftrightarrow E/F \in \mathcal{C} \text{ y } F/K \in \mathcal{C}$$

b) Sean  $E/K$  y  $F/K$  dos extensiones de campos, con  $E$  y  $F$  subcampos de un campo común  $L$ . Entonces

$$E/K \in \mathcal{C} \Rightarrow EF/F \in \mathcal{C}$$

c) Sean  $E/K$  y  $F/K$  dos extensiones de campos, con  $E$  y  $F$  subcampos de un campo común  $L$ . Entonces

$$E/K \in \mathcal{C} \text{ & } F/K \in \mathcal{C} \Rightarrow EF/K \in \mathcal{C}$$

Obs) Notemos que (a) & (b)  $\Rightarrow$  (c).

Teorema.

La clase de extensiones algebraicas es una clase distinguida.

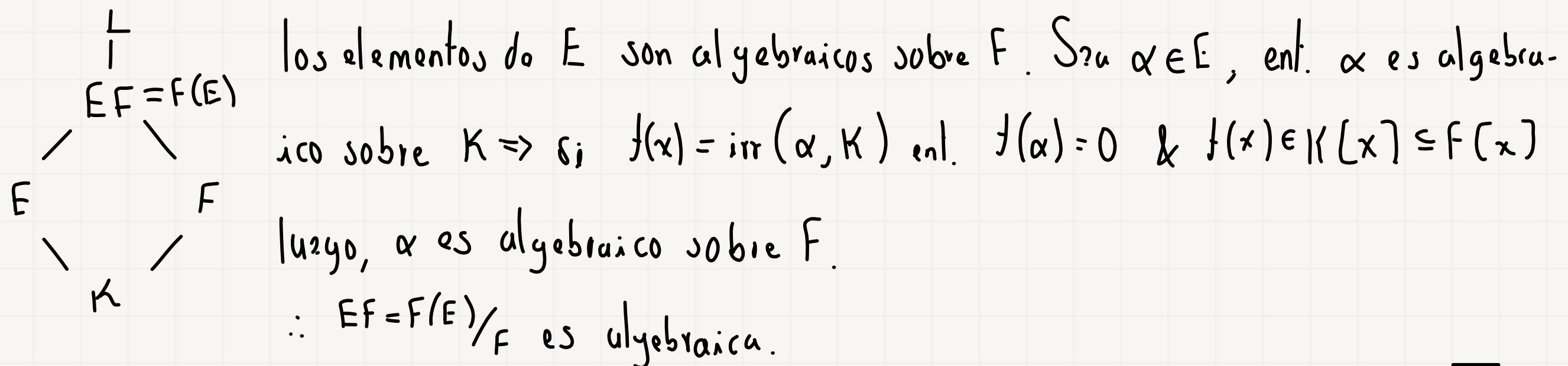
Dem.

D<sup>e</sup>. a): Sea  $K \subseteq F \subseteq E$  una torre de campos.

$\Rightarrow$  Suponemos que  $E/F$  &  $F/K$  son extensiones algebraicas. Sea  $\alpha \in E$ . Ent. tenemos que  $\alpha$  es algebraico sobre  $F$  con  $F/K$  algebraica. Por la prop. ant.  $\alpha$  es algebraico sobre  $K$ .  $\therefore E/K$  es algebraica.

$\Leftarrow$  Supongamos  $E/K$  algebraica. Es claro que  $F/K$  es algebraica. Pero también, si  $\alpha \in E$ , ent.  $f(x) = \text{irr}(\alpha, K) \in K[x] \subseteq F[x]$  con  $f(\alpha) = 0 \Rightarrow \alpha$  algebraico sobre  $F \Rightarrow E/F$  es algebraica.

D<sup>e</sup> b): Consideremos el diagrama, donde  $E/K$  es algebraica. Basta probar que todos



Teorema.

La clase de extensiones finitas forma una clase distinguida.

Dem.

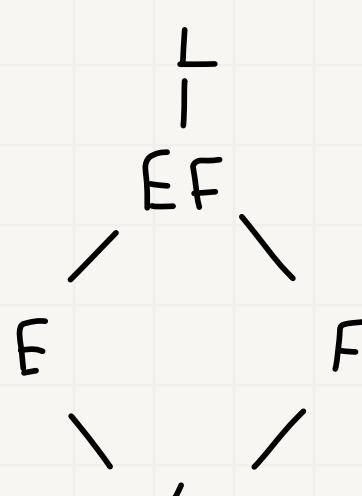
D<sup>e</sup> c): Es inmediato ya que los grados son multiplicativos, i.e si  $K \subseteq F \subseteq E$  es una torre de campos, ent.

$$[E : K] = [E : F] \cdot [F : K] \text{ donde}$$

$$[E : K] < \infty \Leftrightarrow [E : F], [F : K] < \infty$$

D<sub>2</sub> b): Consideremos el diagrama, donde  $E/K$  es finita, luego  $E/K$  es algebraica y f.g.

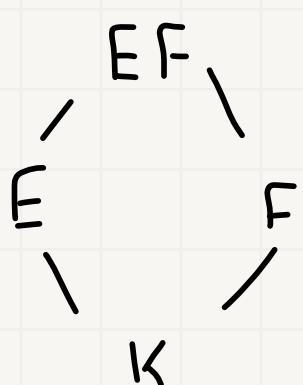
Luego  $EF/F$  es algebraica. Probemos que es f.g. Sean  $u_1, \dots, u_m \in E$  m



$E = K(u_1, \dots, u_m)$

$\Rightarrow EF = K(u_1, \dots, u_m)F = F(u_1, \dots, u_m)$ , i.e.  $EF/F$  es f.g. Por tanto, de lo ant. se deduce que  $EF/F$  es finita. □

Obs) Considerando el sig. diagrama, tenemos que si  $E/K$  es f.g. su traslado  $E^f/F$  también es f.g.



Por otro lado, si  $K \subseteq F \subseteq E$  es una torre de campos donde  $E/F$ ,  $F/K$  son f.g. entonces  $E/K$  es f.g.

Recíprocamente, si  $E/K$  es f.g.,  $E/F$  también lo es. En cierta forma, las extensiones f.g. forman una clase distinguida.

## EJEMPLOS.

1) Sean  $p, q \in \mathbb{N}$ ,  $p < q$  primos. Sabemos que  $\mathbb{Q}(\sqrt{p}, \sqrt{q})/\mathbb{Q}$  es una extensión finita de grado 4, con base  $\{1, \sqrt{p}, \sqrt{q}, \sqrt{pq}\}$ . Afirmamos que  $\exists \alpha \in \mathbb{Q}(\sqrt{p}, \sqrt{q})$  m

$$\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{p}, \sqrt{q})$$

es decir,  $\mathbb{Q}(\sqrt{p}, \sqrt{q})/\mathbb{Q}$  es una extensión simple. En efecto, sea  $\alpha = \sqrt{p} + \sqrt{q}$ . Tenemos que  $\alpha \in \mathbb{Q}(\sqrt{p}, \sqrt{q}) \setminus \mathbb{Q}$ . Luego, se tiene la torre de campos:

$$\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{p}, \sqrt{q})$$

donde  $[(\mathbb{Q}(\alpha):\mathbb{Q})] / [(\mathbb{Q}(\sqrt{p}, \sqrt{q}):\mathbb{Q}] = 4 \Rightarrow [\mathbb{Q}(\alpha):\mathbb{Q}] = 2 \text{ ó } 4$ . Notemos que  $\alpha^2 \in \mathbb{Q}(\alpha)$ , i.e.  $p+q+2\sqrt{pq} \in \mathbb{Q}(\alpha) \Rightarrow \sqrt{pq} \in \mathbb{Q}$  &  $\sqrt{p} + \sqrt{q} \in \mathbb{Q}(\alpha)$ . Pero  $\{1, \sqrt{p} + \sqrt{q}, \sqrt{pq}\}$  es l.i. sobre  $\mathbb{Q}$  ya que, en caso contrario,  $\exists a, b, c \in \mathbb{Q}$  no todos cero  $\cap$

$$a + b\sqrt{p} + b\sqrt{q} + c\sqrt{pq} = 0$$

pero  $\{1, \sqrt{p}, \sqrt{q}, \sqrt{pq}\}$  es l.i. sobre  $\mathbb{Q}$ . Así pues,  $[\mathbb{Q}(\alpha):\mathbb{Q}] \geq 3 \Rightarrow [\mathbb{Q}(\alpha):\mathbb{Q}] = 4 \Rightarrow \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ . Como  $\alpha = \sqrt{p} + \sqrt{q}$

$$\Rightarrow (\alpha - \sqrt{p})^2 = q$$

$$\Rightarrow \alpha^2 - 2\sqrt{p}\alpha + p = q$$

$$\Rightarrow \alpha^2 + p - q = 2\sqrt{p}\alpha$$

$$\Rightarrow \alpha^4 + p^2 + q^2 + 2\alpha^2p - 2\alpha^2q - 2pq = 4p\alpha^2$$

$$\Rightarrow \alpha^4 - 2(p+q)\alpha^2 + (q-p)^2 = 0$$

$$\Rightarrow f(x) = x^4 - 2(p+q)x^2 + (q-p)^2 = \text{irr}(\alpha, \mathbb{Q})$$

**Def.** Sean  $E/K$  y  $F/K$  dos extensiones de campos. Y sea  $\ell: E \rightarrow F$  un homomorfismo. Si  $\ell|_K = \text{id}_K$ , i.e.  $\ell(a) = a, \forall a \in K$ . Entonces decimos que  $\ell$  es un  $K$ -homomorfismo.

Si  $\ell$  es isomorfismo se dice que  $\ell$  es  $K$ -isomorfismo. Si  $E = F$  se dice que  $\ell$  es  $K$ -automorfismo.

Sean  $A$  y  $B$  dos anillos y  $\ell: A \rightarrow B$  un isomorfismo. Sea  $x$  una indeterminada en  $A$  y  $B$ . Entonces  $\ell$  se puede extender, de manera natural, a un isomorfismo  $\tilde{\ell}: A[x]$  sobre  $B[x]$  es decir:

$$A[x] \xrightarrow{\sim} B[x]$$

$$f(x) = a_0 + a_1x + \dots + a_nx^n \mapsto f^{\ell}(x) = \ell(a_0) + \ell(a_1)x + \dots + \ell(a_n)x^n \in B[x]$$

Seguimos denotando por  $\ell$  a dicha extensión. Si  $I$  es un ideal de  $A[x]$  ent. sa-

bemos que  $\ell(I)$  es un ideal de  $B[x]$ . Luego,  $\ell$  induce un isomorfismo

$$\bar{\ell} : A(x)/_I \xrightarrow{\sim} B(x)/_{\ell(I)}$$

$$I + f(x) \mapsto \ell(I) + f^{\ell}(x)$$

Finalmente, si  $A$  y  $B$  son campos, ent. cualquier ideal  $\bar{I}$  de  $A(x)$  es de la forma  $\langle h(x) \rangle = \bar{I}$ , y  $\ell(\bar{I}) = \langle h^{\ell}(x) \rangle$ , así:

$$A(x)/_{\langle h(x) \rangle} \xrightarrow{\sim} B(x)/_{\langle h^{\ell}(x) \rangle}$$

$$\langle h(x) \rangle + f(x) \mapsto \langle h^{\ell}(x) \rangle + f^{\ell}(x)$$

Y, por otro lado,  $\ell$  se extiende a un isomorfismo

$$A(x) \xrightarrow{\sim} B(x)$$

$$\frac{f(x)}{g(x)} \mapsto \frac{f^{\ell}(x)}{g^{\ell}(x)}$$

### Teorema.

Seun  $E/F$  y  $L/K$  extensiones de campos,  $\ell: F \rightarrow K$  un isomorfismo,  $u \in E$  y  $v \in L$  m una de las dos cond. so ha de cumplir:

i)  $u$  es trascendente sobre  $F$  y  $v$  es trascendente sobre  $K$ .

ii)  $u$  es raiz de un polinomio irreducible  $f(x) \in F[x]$  y  $v$  es raiz del polinomio irreducible  $f^{\ell}(x) \in K[x]$ .

Ent.  $\ell$  se extiende a un isomorfismo de  $F(u)$  sobre  $K(v)$ , con  $\ell(u) = v$ .

### Dem.

Suponemos que se cumple (i). Tenemos que si  $x$  es una indeterminada para  $F$  y  $K$ , ent.

$$\psi: F(x) \rightarrow F(u)$$

$$\frac{g(x)}{h(x)} \mapsto \frac{g(u)}{h(u)}$$

es un isomorfismo, luego entonces tenemos la composición de funciones

$$F(u) \xrightarrow{\psi^{-1}} F(x) \xrightarrow{\tau} K(x) \xrightarrow{\sigma} K(v), \text{ con } \tilde{\ell} = \psi^{-1} \circ \tau \circ \sigma$$

$$\frac{g(u)}{h(u)} \mapsto \frac{g(x)}{h(x)} \mapsto \frac{g^u(x)}{h^u(x)} \mapsto \frac{g^u(v)}{h^u(v)}$$

dónde  $r$  se construye de forma análoga a  $\psi$ . Ent. por ser todos isomorfismos, es isomorfismo y

$$u \mapsto x \mapsto x \mapsto v, i.e. \tilde{\varphi}(u) = v$$

En part.  $\forall a \in F$

$$a = \frac{a|_u}{1|_u} \mapsto \frac{a}{1} \mapsto \frac{a(a)}{1} \mapsto \frac{a(a)|_v}{1|_v} = \varphi(a), i.e. \tilde{\varphi}(a) = \varphi(a)$$

As: pues, dicha composición es el isomorfismo  $\tilde{\varphi} : F(u) \rightarrow K(v)$ . Por lo ant.

$$\tilde{\varphi}|_F = \varphi$$

y así,  $\tilde{\varphi}$  es una extensión de  $\varphi$  en  $\tilde{\varphi}(u) = v$ .

Ahora, suponemos que se cumple (ii), ent. tenemos lo sig.

$$F(u) \xrightarrow{\sim} \frac{F(x)}{\langle \text{irr}(u, F) \rangle} = \frac{F(x)}{\langle f(x) \rangle}$$

$$g(u) \mapsto \langle f(x) \rangle + g(x).$$

Pero,

$$\frac{F(x)}{\langle f(x) \rangle} \xrightarrow{\sim} \frac{K(x)}{\langle f^u(x) \rangle} = \frac{K(x)}{\langle \text{irr}(v, K) \rangle} \xrightarrow{\sim} K(v)$$

$$\langle f(x) \rangle + g(x) \mapsto \langle f^u(x) \rangle + g^u(x) \mapsto g^u(v)$$

i.e. dicha composición  $\tilde{\varphi} : F(u) \rightarrow K(v)$ ,  $g(u) \mapsto g^u(v)$  es un isomorfismo.

O que mapea  $u$  en  $v$  y  $\tilde{\varphi}|_F = \varphi$ , pues:

$$\tilde{\varphi}(u) = \tilde{\varphi}(x|_u) = x^u|_v = \varphi(1)x|_v = 1 \cdot v = v$$

y,  $\forall a \in F$ :

$$\tilde{\varphi}(a) = \tilde{\varphi}(a|_u) = a^u|_v = \varphi(a)|_v = \varphi(a)$$

□

## Corolario.

Sean  $E/K$  y  $F/K$  extensiones de campo,  $u \in E$  y  $v \in F$  algebraicos sobre  $K$ . Ent. los sig.

Son equivalentes:

i)  $u$  &  $v$  tienen el mismo polinomio irreducible sobre  $K$ .

ii) Existe un  $K$ -isomorfismo de  $K(u)$  sobre  $K(v)$  que mapea  $u$  en  $v$ .

Dem.

$K(u) \xrightarrow{\sim} K(v)$  (i)  $\Rightarrow$  (ii). Suponemos que  $f(x) = \text{irr}(u, K) = \text{irr}(v, K)$ . Si:  
$$\begin{array}{ccc} K & \xrightarrow{id} & K \\ \downarrow & & \downarrow \\ K & \longrightarrow & K \end{array}$$
a  $\varphi: K \rightarrow K$  la fun. identidad. Aplicando el t. ant. en (ii) tenemos que  $\varphi = id_K$  se extiende a un isomorfismo  $K(u) \xrightarrow{\sim} K(v)$  que mapea  $u \mapsto v$ , siendo este un  $K$ -isomorfismo.

(ii)  $\Rightarrow$  (i). Sea  $\varphi: K(u) \xrightarrow{\sim} K(v)$  un  $K$ -isomorfismo m  $\varphi(u) = v$ . Tomamos  $f(x) = \text{irr}(u, K)(x)$ , irreducible de  $K(x)$ , luego  $v = \varphi(u)$  es raiz de  $f^{\varphi}(x)$ . Pero  $f^{\varphi}$  es irreducible en  $K(x)$  y  $\varphi$  es  $K$ -isomorfismo, luego  
$$f^{\varphi}(x) = f(x)$$
  
 $\therefore \text{irr}(v, K, x) = f(x)$ .

□

Corolario.

Sea  $E/F$  una extensión de campos y  $x \in E$  trascendente sobre  $F$ . Si  $x$  es una indeterminada para  $F$ , ent. existe un  $F$ -isomorfismo  $F(u)$  en  $F(x)$  que mapea  $u$  en  $x$ .

Dem.

Es inmediato del teorema ant.

□

Def. Sea  $E/F$  una extensión de campos,  $u, v \in E$  tales que son raíces de un mismo pol. irreducible de  $F(x)$ . Entonces, decimos que  $u$  y  $v$  son  $F$ -conjugados.

## Teorema.

Sea  $F$  un campo y  $f(x) \in F[x]$  de grado  $\geq 1$ . Ent. existe una extensión simple  $E(u)/F$  m  $f(u) = 0$ .

## Dem.

Como  $f(x)$  es de grado  $\geq 1$  y  $F[x]$  es  $D\mathcal{F}(u)$ , elegimos un factor polinomio irreducible de  $f(x)$  con el cual probaremos la existencia de la extensión simple  $E(u)/F$  donde  $u$  es raíz de dicho factor irreducible, y por lo tanto  $f(u) = 0$ .

S: se desea, podemos suponer que  $f(x)$  el pol. irreducible de  $F[x]$  de grado  $\geq 1$ . Luego,  $\langle f(x) \rangle$  es un ideal maximal de  $F[x] \Rightarrow E := F[x]/\langle f(x) \rangle$  es un campo.

Sea  $\varphi: F[x] \rightarrow E$  el epimorfismo canónico. Ent.  $\varphi|_F: F \rightarrow E = F[x]/\langle f(x) \rangle = E$  es un monomorfismo. Luego:

$$F \cong \varphi(F) = \{\varphi(a) \mid a \in F\} = \{a + \langle f(x) \rangle \mid a \in F\} \stackrel{(1)}{=} F + \langle f(x) \rangle \stackrel{(2)}{=} \langle f(x) \rangle$$

Denotemos por  $\bar{I} = \langle f(x) \rangle$ . As; que, tenemos el diagrama:

$$\begin{array}{ccc} E & = & F[x]/\langle f(x) \rangle \\ & | & \\ F & \xrightarrow{\varphi|_F} & \varphi(F) \stackrel{(1)}{=} \bar{I} \end{array}$$

Si polinomio  $f(x) \in F[x]$  lo expresamos en la forma:

$$f(x) = a_0 + a_1 x + \dots + a_n x^n$$

Bajo el isomorfismo  $\varphi|_F$ , el polinomio  $f(x)$  visto en  $\varphi(F)[y]$  es:

$$f^{\varphi}(y) = (a_0 + \bar{I}) + (a_1 + \bar{I})y + \dots + (a_n + \bar{I})y^n$$

Sea  $u = x + \bar{I} \in E$ . Ent.

$$\begin{aligned} f^{\varphi}(u) &= f^{\varphi}(x + \bar{I}) \\ &= (a_0 + \bar{I}) + (a_1 + \bar{I})(x + \bar{I}) + \dots + (a_n + \bar{I})(x^n + \bar{I}) \\ &= (a_0 + a_1 x + \dots + a_n x^n) + \bar{I} \\ &= f(x) + \langle f(x) \rangle \\ &= 0 \end{aligned}$$

•  $u$  es raíz de  $f^{\ell}(y)$ . Además,  $\ell(f)(u) = E$ . En efecto, ya se sabe que  $\ell(f)(u) \subseteq E$ .

Sea  $\alpha \in E$ . Expresamos  $\alpha$  como:

$$\alpha = g(x) + I, \text{ donde } g(x) \in F[x]$$

y  $g(x) = b_0 + b_1 x + \dots + b_m x^m$ . Luego:

$$\begin{aligned} \alpha &= (b_0 + b_1 x + \dots + b_m x^m) + I \\ &= (b_0 + I) + (b_1 + I)(x + I) + \dots + (b_m + I)(x^m + I) \\ &= (b_0 + I) + (b_1 + I)u + \dots + (b_m + I)u^m \\ &\in \ell(F)(u) \end{aligned}$$

Por tanto,  $E \subseteq \ell(F)(u) \Rightarrow E = \ell(F)(u)$ . Luego, la extensión  $E/\ell(F)$  es simple generada por  $u$  sobre  $F$ , con  $f^{\ell}(u) = 0$ .

□

**Def.** Sea  $E$  un campo. Decimos que  $E$  es algebraicamente cerrado si todo pol. de  $E(x)$  de grad.  $> 1$  tiene una raíz en  $E$ .

Si  $E$  es algebraicamente cerrado y  $f(x) \in E(x)^{E}$ , ent. existe  $\lambda \in E$  y  $u_1, \dots, u_n \in E$  m

$$f(x) = \lambda(x - u_1) \cdot \dots \cdot (x - u_n).$$

Más generalmente, si  $E/F$  es una extensión de campos con  $E$  algebraicamente cerrado y  $f(x) \in F(x) \setminus F$ , ent. existen  $\lambda \in F$  y  $u_1, \dots, u_n \in E$  m

$$f(x) = \lambda(x - u_1) \cdot \dots \cdot (x - u_n)$$

### Teorema.

Sea  $E$  un campo. Ent. las sig. son equivalentes

- i)  $E$  es algebraicamente cerrado.
- ii)  $F/E$  extensión algebraica  $\Rightarrow F = E$ .

iii)  $F/E$  extensión finita  $\Rightarrow F = E$ .

iv) Todo polinomio en  $E(x)$  de grado  $\geq 1$  irreducible es de grado 1.

v) Todo polinomio en  $E(x)$  de grado  $\geq 1$  es un producto de polinomios lineales.

Dem.

i)  $\Rightarrow$  ii): Sea  $F/E$  una extensión algebraica. Sea  $\alpha \in F$ . Entonces  $\alpha$  es algebraico sobre  $E$ , sea  $f(x) = \text{irr}(\alpha, E, x)$ .

Como  $E$  es algebraicamente cerrado,  $\exists \alpha_1, \dots, \alpha_n \in E$  tal que

$$f(x) = (x - \alpha_1) \cdot \dots \cdot (x - \alpha_n)$$

Pero  $f(\alpha) = 0 \Rightarrow \alpha \in \{\alpha_1, \dots, \alpha_n\} \subseteq E$ . Luego  $F \subseteq E$ .  
 $\therefore F = E$ .

ii)  $\Rightarrow$  iii): Es inmediata.

iii)  $\Rightarrow$  iv): Sea  $g(x) \in E[x]$  irreducible con  $n = \deg(g(x)) \geq 1$ . Por el t. ant.  $\exists$  una extensión simple  $E^{(\alpha)}/E$  en la que  $g(\alpha) = 0 \Rightarrow E^{(\alpha)}/E$  es finita y:

$$\begin{aligned} [E(\alpha):E] &= \text{grad}(\text{irr}(\alpha, E, x)) \\ &= n \end{aligned}$$

Pero, por hip.  $E(\alpha) = E \Rightarrow n = 1 \Rightarrow \text{grad}(g(x)) = 1$ .

iv)  $\Rightarrow$  v): Es inmediato, pues  $E(x)$  es DFU.

v)  $\Rightarrow$  i): Es inmediato. □

Corolario.

El campo  $E$  es algebraicamente cerrado  $\Leftrightarrow$   $\forall L/E$  extensión de campos  $\& x \in L/E$  implica  $x$  trascendente sobre  $E$ .

Dem.

Es inmediato. □

## Teorema (Art. n).

Sea  $F$  un campo. Entonces existe una extensión  $F/F$  en  $E$  es un campo algebraicamente cerrado.

Dem.

Para cada polinomio  $H(x) \in F[x]$  de grado  $\geq 1$  le asociamos una indeterminada  $x_f$  en el conjunto de todos los indeterminados  $X_f$  están en correspondencia biunívoca con los polinomios  $f(x) \in F[x]$  de grado  $\geq 1$ .

$$f \mapsto x_f$$

denotamos por  $S = \{x_f \mid f(x) \in F[x], \text{grado}(f(x)) \geq 1\}$ . Construimos el anillo  $F[s]$ .

Sea  $I$  el ideal de  $F[s]$  generado por todos los pol. de la forma  $f(x_f)$ , i.e:

$$I = \langle f(x_f) \mid x_f \in S \rangle$$

Tomemos que  $I \neq F[s]$ . En efecto, si  $I = F[s] \Rightarrow 1 \in I$

$$\Rightarrow 1 = g_1 f_1(x_{f_1}) + \dots + g_m f_m(x_{f_m})$$

donde  $g_i \in F[s]$ ,  $f_i$  son pol. con coef. en  $F$  con grado  $\geq 1$ . Para comodidad:

$$x_i := x_{f_i}, \forall i \in [1, m]$$

Así que, asumimos que en la ec. ant.  $x_1, \dots, x_m, x_{m+1}, \dots, x_N$  es la totalidad de indeterminadas que aparecen en la ec. ant.  $F[s]$  decir:

$$(= g_1(x_1, \dots, x_N) f_1(x_1) + \dots + g_m(x_1, \dots, x_N) f_m(x_m))$$

Por el t. ant. elegimos raíces  $\alpha_1, \dots, \alpha_m$  de los pol.  $f_1, \dots, f_m$ , resp. / evaluamos en la ec. ant. tomando  $x_i = \alpha_i, \forall i \in [1, m]$ ,  $x_i = 0, \forall i \in [m+1, N]$

$$\therefore () = 1$$

Por lo tanto  $I \neq F[s]$ . Sea  $M$  un ideal maximal de  $F[s]$  en  $I \subseteq M$ .

$$\Rightarrow E := F[s]/M \text{ es campo.}$$

Sea  $\varphi: F[s] \rightarrow E$ , el homomorfismo ranónico. Notemos que  $\varphi(1) = 1$ . Luego  $\varphi|_F$ :

$F \rightarrow E_1$  es monomorfismo, i.e.  $\ell|_F : F \rightarrow \ell(F)$  es isomorfismo, o seu  $\ell(F)$  es subcampo de  $E_1$ , isomorfo a  $F$ .

$$\begin{array}{c} E_1 = F[x]/M \\ | \\ F \xrightarrow{\sim} \ell(F) \stackrel{\text{"}}{=} F \end{array}$$

Si  $f(x) \in F[x]$  con  $\deg(f(x)) \geq 1$ , digumos

$$\begin{aligned} f(x) &= a_0 + a_1 x + \dots + a_k x^k, \quad a_k \neq 0, \\ \Rightarrow f^M(x) &= (a_0 + M) + (a_1 + M)x + \dots + (a_k + M)x^k \\ \Rightarrow f^M(x_f + M) &= (a_0 + a_1 x_f + \dots + a_k x_f^k) + M \\ &= f(x_f) + M \\ &= 0 \end{aligned}$$

$$\Rightarrow \exists \alpha_f \in F, \text{ s.t. } f(\alpha_f) = 0.$$

Resumiendo, se tiene que  $E_1/F$  es una extensión d. ceros en todo polinomio en  $F[x]$  de grado  $\geq 1$  tiene una raíz en  $E_1$ .

Demuera inductivamente, construimos una torre de campos  $F \subseteq E_1 \subseteq \dots \subseteq E_n \subseteq E_{n+1} \subseteq \dots$  tal que todo polinomio en  $E_n$  de grado  $\geq 1$  tenga una raíz en  $E_{n+1}$ ,  $\forall n \geq 1$ .

Definimos:

$$E := \bigcup_{n \in \mathbb{N}} E_n$$

Tenemos que  $E/F$  es una extensión de campos con  $E$  algebraicamente cerrado ya que si  $f(x) \in E[x]$  de grado  $\geq 1$ , con  $f(x) = b_0 + b_1 x + \dots + b_k x^k$  ( $b_k \neq 0$ ) ent.

$b_0, b_1, \dots, b_k \in E \Rightarrow \exists N \in \mathbb{N}$  s.t.  $b_0, b_1, \dots, b_k \in E_N \Rightarrow f(x) \in E_N[x]$ . Luego  $f(x)$  tiene una raíz en  $E_{N+1} \subseteq E$ .

□

Corolario.

**S7o.**  $F$  un campo. Entonces existe una extensión  $E/F$  algebraica con  $E$  un campo algebraicamente cerrado.

**Dem.**

Sea  $L/F$  una extensión donde  $L$  es algebraicamente cerrado (T. de Artin). Sea  $E$  la cerradura algebraica de  $F$  en  $L$ . Así que  $E/F$  es algebraica ya que

$$E = \{ \alpha \in L \mid \alpha \text{ es algebraico sobre } F \}$$

Afirmamos que  $E$  es algebraicamente cerrado. En efecto, sea  $f(x) \in E[x]$  y  $\text{gr}(f(x)) > 1$ . Laugo,  $f(x) \in L[x]$ , por lo cual  $\exists \alpha \in L$  s.t.  $f(\alpha) = 0$ .

Ent.  $\alpha$  es algebraico sobre  $E$ , como  $E/F$  es algebraica ent.  $\alpha$  es algebraico sobre  $F \Rightarrow \alpha \in E$ . Por lo tanto,  $E$  es algebraicamente cerrado con  $E/F$  algebraica.  $\square$

**Daf.** Sea  $F$  un campo y  $E/F$  una extensión de campos. Decimos que el campo  $E$  es una **cerradura algebraica de  $F$** , si  $E$  es algebraicamente cerrado y  $E/F$  es algebraica.

**Obs)** Notemos que todo campo  $E$  algebraicamente cerrado es infinito. En efecto, si el campo  $E$  fuera finito, con  $E = \{\alpha_1, \dots, \alpha_n\}$ . Ent. el polinomio

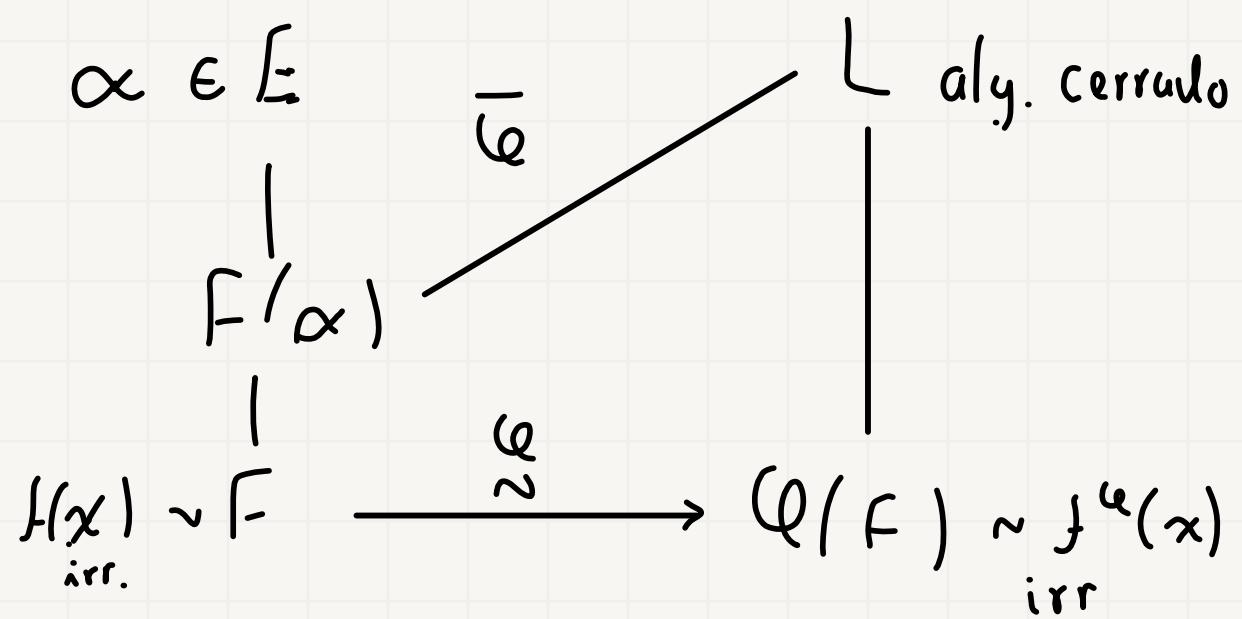
$$f(x) = (x - \alpha_1) \cdot (x - \alpha_2) \cdots (x - \alpha_n) + 1 \in E[x]$$

no tiene raíces en  $E$ .

**Teorema.**

Sea  $E/F$  una extensión de campos,  $L$  un campo algebraicamente cerrado,  $\alpha \in E$  algebraico sobre  $F$ ,  $f(x) \in F[x]$  irreducible s.t.  $f(\alpha) = 0$ ,  $\alpha: F \rightarrow L$  un homomorfismo y  $\beta_1, \dots, \beta_t \in L$  las raíces distintas del polinomio  $f^*(x) \in L[x]$  donde  $t \leq \text{grad}(f(x))$ . Ent. se admite exactamente  $t$  extensiones a homomorfismos de  $f(\alpha)$  en  $L$ .

**Dem.**



i) Definimos  $\bar{\varphi}_i: F(\alpha) \rightarrow L$  dada como si...  
 que:  $\forall r \in F(\alpha)$  con  $r = g(\alpha)$  donde  $g$   
 $(x) \in F(x)$ , ent.  
 $\varphi_i(r) := g^u(B_i)$   
 donde  $i \in \{l, r\}$ .

Tenemos que  $\bar{\varphi}_i$  está bien def. pues si  $r \in F(\alpha) = F[\alpha]$  con  $g(\alpha) = r = g_i(\alpha)$   
 donde  $g(x), g_i(x) \in F(x)$ , al tomar  $h(x) = g(x) - g_i(x) \in F(x)$ , ent.

$$h(\alpha) = g(\alpha) - g_i(\alpha)$$

$$= r - r$$

$$= 0$$

$$\Rightarrow f(x) \mid h(x)$$

pues  $\exists \lambda \in F$  m  $f(x) = \lambda_{\text{irr}}(\alpha, F, x)$ , luego  $\exists \lambda(x) \in F(x)$  m  
 $h(x) = \lambda(x) f(x)$ , i.e

$$g(x) - g_i(x) = f(x) \lambda(x), \text{ luego}$$

$$y^u(x) - y_i^u(x) = f^u(x) \lambda^u(x)$$

$$\Rightarrow g^u(B_i) - g_i^u(B_i) = f^u(B_i) \lambda^u(B_i) = 0$$

$$\Rightarrow g^u(B_i) = g_i^u(B_i).$$

Así,  $\bar{\varphi}_i$  está bien def. Es decir probar que  $\bar{\varphi}_i: F(\alpha) \rightarrow L$  es un homomorfismo. Y que

$\forall u \in F$ ,  $u = K(\alpha)$ , donde  $K(x) \in F(x)$ ,  $K(x) = u$ .

$$\Rightarrow \bar{\varphi}_i(u) = K^u(B_i) = \varphi(u)$$

así que  $\bar{\varphi}_i: F(\alpha) \rightarrow L$  es un homomorfismo extensión de  $\varphi$ . Notemos que

$$\bar{\varphi}_i \neq \bar{\varphi}_j \text{ si } i \neq j$$

Pues  $\bar{\varphi}_i(\alpha) = B_i \neq B_j = \bar{\varphi}_j(\alpha)$ , ya que

$$\alpha = g(\alpha) = x|_\alpha$$

$$\Rightarrow \bar{\varphi}_j(\alpha) = g^{\varphi}(\beta_j) \\ = 1 \cdot \beta_j \\ = \beta_j$$

de aquí que  $\varphi$  admite al menos  $f$ -extensiones a homomorfismos de  $F(\alpha)$  en  $L$ . Sea  $\psi: F(\alpha) \rightarrow L$  un homomorfismo cualquiera extensión de  $\varphi$ . Notemos que:

$$\begin{aligned} f^{\varphi}(\psi(\alpha)) &= \varphi(a_0) + \varphi(a_1)x + \dots + \varphi(a_n)x^n |_{\psi(\alpha)} \\ &= \psi(a_0) + \psi(a_1)\psi(\alpha) + \dots + \psi(a_n)\psi(\alpha^n) \\ &= \psi(a_0 + a_1\alpha + \dots + a_n\alpha^n) \\ &= \psi(f(\alpha)) \\ &= \psi(0) \\ &= 0 \end{aligned}$$

Por tanto,  $\psi(\alpha)$  es raíz de  $f(x) \Rightarrow \exists j \in [1, f] \cap \psi(\alpha) = \beta_j \Rightarrow \forall r \in F(\alpha)$  (on  $r = g(\alpha) / g(x) \in F(x)$ ):

$$\begin{aligned} \psi(r) &= g^{\varphi}(\psi(\alpha)) \\ &= g^{\varphi}(\beta_j) \\ &= \bar{\varphi}_j(r) \\ \therefore \psi &= \bar{\varphi}_j \end{aligned}$$

□

### Teorema.

Sea  $E/F$  una extensión algebraica,  $L$  un campo algebraicamente cerrado y  $\varphi: F \rightarrow L$  un homomorfismo (no trivial). Ent.

i)  $\varphi$  admite una extensión  $\bar{\varphi}$  a un homomorfismo de  $E$  en  $L$ .

ii) Si además  $E$  es algebraicamente cerrado y  $L/\varphi(F)$  es algebraica, ent.  $\bar{\varphi}$  es un isomorfismo de  $E$  en  $L$ .

Dem.

De (i): Sea  $\mathcal{F} = \{(K, \sigma) \mid K \text{ es un campo intermedio de la extensión } E/F \text{ y } \sigma \text{ es un homomorfismo de } K \text{ en } L \text{ con } \sigma|_F = \varphi\}$

$\mathcal{F}$  es no vacía, pues  $(F, \varphi) \in \mathcal{F}$ . Definimos en  $\mathcal{F}$  la sig. relación:  $(K_1, \sigma_1), (K_2, \sigma_2) \in \mathcal{F}$ , decimos que

$$(K_1, \sigma_1) \leq (K_2, \sigma_2) \iff K_1 \subseteq K_2 \text{ y } \sigma_2|_{K_1} = \sigma_1$$

$\leq$  es un preorden en  $\mathcal{F}$ , así  $(\mathcal{F}, \leq)$  es un conjunto parcialmente ordenado. Sea  $\beta$  una cadena de  $\mathcal{F}$ . Definimos

$$M := \bigcup_{(K, \sigma) \in \beta} K$$

por ser  $\beta$  cadena,  $M$  es subcampo de  $E$  (es inmediato). Definimos  $\sigma_M : M \rightarrow L$  como sigue. Para cada  $\alpha \in M$ , se define

$$\sigma_M(\alpha) = \sigma_K(\alpha) \text{ si } (K, \sigma_K) \in \beta \text{ y } \alpha \in K.$$

$\sigma_M(\alpha)$  no depende de  $K$ . Si  $(K_1, \sigma_1), (K_2, \sigma_2) \in \beta$ , ent.  $(K_1, \sigma_1) \leq (K_2, \sigma_2)$  y

$$\sigma_2(\alpha) = \sigma_2|_{K_1}(\alpha) = \sigma_1(\alpha) = \sigma_M(\alpha)$$

Además,  $\sigma_M$  es homomorfismo de  $M$  en  $L$ , con  $\sigma_M|_F = \varphi \Rightarrow (M, \sigma_M) \in \mathcal{F}$  y  $(M, \sigma_M)$  es cota superior de todos los elementos de  $\beta$ . Por el lema de Zorn,  $\mathcal{F}$  tiene elementos máximos.

Sea  $(K_0, \sigma_0) \in \mathcal{F}$  maximal. Afirmamos que  $K_0 = E$ . Si  $K_0 \subsetneq E$  ent.  $\exists \alpha \in E \setminus K_0$ , luego  $\sigma_0$  tiene una extensión  $\psi$  a un homomorfismo  $K_0(\alpha)$  en  $L$ . Notemos que  $\psi|_F = \sigma_0|_F = \varphi$ . Luego  $(K_0(\alpha), \psi) \in \mathcal{F}$  con  $(K_0, \sigma_0) < (K_0(\alpha), \psi)$ .

Por tanto,  $K_0 = E$  y  $\sigma_0 : E \rightarrow L$  es una extensión de  $\varphi$ .

De (ii): Bajo las hip. se tiene que  $E$  y  $L$  son cerraduras algebraicas de  $F$  y  $\bar{\mathbb{Q}}(F)$ , resp.

Probemos que  $\bar{\mathbb{Q}}(E) = L$ . Claro que  $\bar{\mathbb{Q}}(E) \subseteq L$ .

Notar que bajo isomorfismo,  $\bar{\mathbb{Q}}(E)$  es un campo alg. cerrado con  $L/\bar{\mathbb{Q}}(E)$  ext. algebraica  $\Rightarrow L = \bar{\mathbb{Q}}(E)$ . □

### Corolario.

Sea  $E/F$  ext. algebraica y  $\bar{F}$  una cerradura algebraica de  $F$  que contiene a  $E$ . Cada homomorfismo de  $F$  en  $\bar{F}$  se extiende a un homomorfismo de  $E$  en  $\bar{F}$  y este último se puede extender a un automorfismo de  $\bar{F}$ .

Dem:

Es inmediata. □

### Corolario.

Sea  $F$  un campo y  $E_1$  y  $E_2$  dos cerraduras algebraicas de  $F$ . Ent. existe un  $F$ -isomorfismo de  $E_1$  en  $E_2$ .

Dem:

Es inmediata. □

### Proposición.

Sea  $E/F$  una extensión algebraica con  $F$  campo infinito. Entonces,  $|E| = |F|$ .

Dem.

Sea

$$S = \{f(x) \in F[x] \mid \text{grad}(f(x)) \geq 1 \text{ y } f(x) \text{ es monico}\}$$

$\forall n \in \mathbb{N}$ , definimos

$$\begin{aligned} S_n &= \{f(x) \in F[x] \mid \text{grad}(f(x)) = n \text{ y } f(x) \text{ es monico}\} \\ &\Rightarrow S = \bigcup_{n=1}^{\infty} S_n \end{aligned}$$

Como  $S_n \cap S_m = \emptyset$ ,  $\forall m, n \in \mathbb{N}, m \neq n$ :

$$\Rightarrow |S| = \lambda_0 \cdot |S_n|$$

Notemos que,  $\forall f(x) = a_0 + \dots + x_n \in S_n$ . Luego existe una biyección

$$F \times \underbrace{\dots \times F}_{n-\text{veces}} \rightarrow S_n$$

$$(a_0, \dots, a_{n-1}) \mapsto a_0 + a_1 x + \dots + a_{n-1} x^{n-1} + x^n$$

Luego

$$\begin{aligned} |S_n| &= |F \times \dots \times F| \\ &= |F|^n, \text{ pues } |F| \geq n!. \\ \therefore |S| &= |F|^n \end{aligned}$$

Para cada  $f(x) \in S$ , denotamos por  $K_f = \{\alpha \in E \mid f(\alpha) = 0\}$  (posiblemente,  $K_f = \emptyset$ ), pero  $|K_f| \leq \text{grad}(f(x))$ . Luego:

$$\begin{aligned} E &= \bigcup_{f \in S} K_f \\ \Rightarrow |E| &\leq |E| = \left| \bigcup_{f \in S} K_f \right| \leq \sum_{f \in S} |K_f| \leq n! \cdot |S| = |S| = |F|^n \\ \therefore |E| &= |F|^n \end{aligned}$$

□

Sea  $F$  un campo y  $\{f_i(x)\}_{i \in I}$  una familia de pol. en  $F[x]$ . Sea  $\bar{F}$  una cerradura algebraica de  $F$ .

Para cada  $i \in I$ , sea

$$S_i = \{\alpha \in \bar{F} \mid f_i(\alpha) = 0\}$$

Denotamos por  $S = \bigcup_{i \in I} S_i \subseteq \bar{F}$  (todos los  $f_i(x)$  se suponen no constantes). Ent. el campo  $F(S)$  es llamado el **Campo de descomposición** de la familia de pol. de  $\{f_i(x)\}_{i \in I}$  sobre  $F$ .

**Proposición.**

Bajo las notaciones ant., todo  $\varphi$  homomorfismo de  $F$  en  $\bar{F}$  se extiende a un isomorfismo de  $F(S)$  en  $\varphi(F)(S')$  donde  $S'$  es el conjunto de raíces en  $\bar{F}$  de la familia  $\{\varphi(f_i)(x)\}_{i \in I}$ .

**Dem.**

Extendemos  $\varphi$  a un automorfismo  $\bar{\varphi}$  de  $\bar{F}$  y, denotemos por  $\bar{\varphi} = \varphi|_{F(S)}$ . Probemos

que  $\bar{\varphi}(F(S)) = F(S)$ . Para ello, tomemos  $i \in I$ . Si  $\alpha \in S_i$ , i.e.  $f_i(\alpha) = 0$ , ent.

$0 = \bar{\varphi}(0) = \bar{\varphi}(f_i(\alpha)) = f_i^{\bar{\varphi}}(\bar{\varphi}(\alpha)) = f_i^{\varphi}(\bar{\varphi}(\alpha))$ , i.e.  $\bar{\varphi}(\alpha)$  es raíz de  $f_i^{\varphi}$ . Luego

$\bar{\varphi}(S_i) \subseteq S_i'$ , donde  $S_i'$  es el conjunto de raíces de  $f_i^{\varphi}(x)$  en  $\bar{F}$  con  $|S_i'| = |S_i|$

$$\Rightarrow \bar{\varphi}(S_i) = S_i'$$

$$\Rightarrow \bar{\varphi}(F(S)) = \bar{\varphi}(F(\bigcup_{i \in I} S_i))$$

$$= \varphi(F)\left(\bigcup_{i \in I} \bar{\varphi}(S_i)\right)$$

$$= \varphi(F)(S')$$

$$= \varphi(F)(S')$$

□

### Corolario.

Si  $\varphi: F \rightarrow \bar{F}$  es el encaje canónico, ent.  $\varphi$  se extiende a un automorfismo de  $F(S)$ .

### Teorema.

Sea  $F$  un campo y  $\{f_i(x)\}_{i \in I}$  una familia de pol. en  $F[x]$ . Cualesquier dos campos de descomposición de la familia  $\{f_i(x)\}_{i \in I}$  son  $F$ -isomorfos.

### Dem.

## Teatrmo.

S<sub>2</sub>, E/F una extensión algebraica y  $\bar{F}$  una cerradura algebraica de F en  $E \subseteq \bar{F}$ .

Ent. las sig. cond. son equiv.

i) Todo F-homomorfismo de E en  $\bar{F}$  es un F-automorfismo de E.

ii) Si  $f(x) \in F[x]$  irreducible y  $\alpha \in E$  &  $\beta \in \bar{F}$  en  $f(\alpha) = 0 = f(\beta)$ , ent.  $\beta \in E$ .

iii) Si  $\alpha, \beta \in \bar{F}$  son F-conjugados con  $\alpha \in E$ , ent.  $\beta \in E$ .

iv) E es el campo de descomposición de una familia de pol. de  $F[x]$  sobre F.

## Dcm.

i)  $\Rightarrow$  ii):

Sea  $f(x) \in F[x]$  irreducible,  $\alpha, \beta \in \bar{F}$  en  $f(\alpha) = 0 = f(\beta)$ . Supongamos que  $\alpha \in E$ . Si  $\alpha = \beta$  claramente  $\beta \in E$ . Supongamos  $\alpha \neq \beta$ , ent.  $\text{grado}(f(x)) \geq 2$ .

Notemos que  $\exists \lambda \in F \text{ Kos}$  en  $\text{irr}(\alpha, F, x) = \lambda f(x)$ , i.e.  $\alpha$  y  $\beta$  son F-conjugados. Ent. existe un F-isomorfismo  $\Psi: F(\alpha) \rightarrow F(\beta)$  en  $\Psi(\alpha) = \beta$ . Extendemos  $\Psi$  a un  $\bar{F}$ -homomorfismo  $\varphi: E \rightarrow \bar{F}$ . Por hip.  $\varphi(E) = E$

$$\Rightarrow \beta = \varphi(\alpha) \in \varphi(E) = E$$

ii)  $\Rightarrow$  iii):

Es inmediato.

iii)  $\Rightarrow$  iv):

Para cada  $\alpha \in E$ , sea  $f_\alpha(x) = \text{irr}(\alpha, F, x)$  y sea:

$$S_\alpha := \{ \beta \in \bar{F} \mid f_\alpha(\beta) = 0 \}$$

Por hip.  $S_\alpha \subseteq E, \forall \alpha \in E$ .

$$\Rightarrow S := \bigcup_{\alpha \in E} S_\alpha \subseteq E$$

Más aún,  $S = E$ . En part.  $E = F(S)$ , i.e. E es el campo de descomposición de la familia  $\{f_\alpha(x)\}_{\alpha \in E}$ .

iv)  $\Rightarrow$  i):

Sea  $\varphi: E \rightarrow \bar{F}$  un  $F$ -homomorfismo. Por hip.  $\exists$  una familia de pol.  $\{f_i(x)\}_{i \in \mathbb{Z}}$  en  $E$  es el campo de descomposición de esta familia.

Ent.

$$\begin{aligned}\varphi(F) &= \varphi(F)(\varphi(s)) \\ &= F(\varphi(\bigcup_{i \in \mathbb{Z}} S_i)) \\ &= F(\bigcup_{i \in \mathbb{Z}} \varphi(S_i)) \\ &= F(\bigcup_{i \in \mathbb{Z}} S_i) \\ &= F(S) \\ &= F\end{aligned}$$

dónde  $S = \bigcup_{i \in \mathbb{Z}} S_i$ ,  $S_i = \{\beta \in \bar{F} \mid f_i(\beta) = 0\}$ . Luego  $\varphi$  es  $F$ -automorfismo.

□

D.o.). Sean  $E/F$  una extensión algebraica. Decimos que  $E/F$  es normal, si se cumple la cond.

i) (y por tanto i)-iv)) del t. ant.

### Proposición

Sean  $E/F$  una extensión finita. Ent.  $E/F$  es normal  $\Leftrightarrow E$  es el campo de descomposición de un polinomio sobre  $F$ .

### Dem.

$\Leftarrow$ ) Es inmediato.

$\Rightarrow$ ) Supongamos que  $E/F$  es normal y finita. Sean  $\alpha_1, \dots, \alpha_n \in E$  en  $E = F(\alpha_1, \dots, \alpha_n)$  (con  $n \alpha_1, \dots, \alpha_n$  algebraicos sobre  $F$ ). Para cada  $i = 1, \dots, n$ , Sean

$$S_i = \{\beta \in \bar{F} \mid \alpha_i \text{ y } \beta \text{ son } F\text{-conjugados}\}$$

dónde  $\bar{F}$  es una cerradura algebraica de  $F$  en  $E \subseteq \bar{F}$ . Puesto que  $E/F$  es normal, ent.

$S_i \subseteq E, \forall i \in [1, n]$ , luego

$$S = \bigcup_{i=1}^n S_i \subseteq E$$

$$\Rightarrow E = F(\alpha_1, \dots, \alpha_n) \subseteq F(S) \subseteq E$$

$$\therefore E = F(S)$$

Sea  $f(x) = \prod_{i=1}^n \text{irr}(\alpha_i, F, x)$ .

$$\Rightarrow T := \{B \in \bar{F} \mid f(B) = 0\} = S$$

$$\therefore E = F(S) = F(T)$$

i.e  $E$  es el campo de descomposición de un polinomio.

□

### Proposición.

i) Sean  $F \subseteq K \subseteq E$  una torre de campos. Si  $E/F$  es normal, ent.  $E/K$  también lo es.

ii) Sean  $E/F$  y  $K/F$  extensiones de campos en  $E$  y  $K$  son subcampos de un campo común  $L$ .

Si  $E/F$  es normal  $\Rightarrow KE/K$  también lo es.

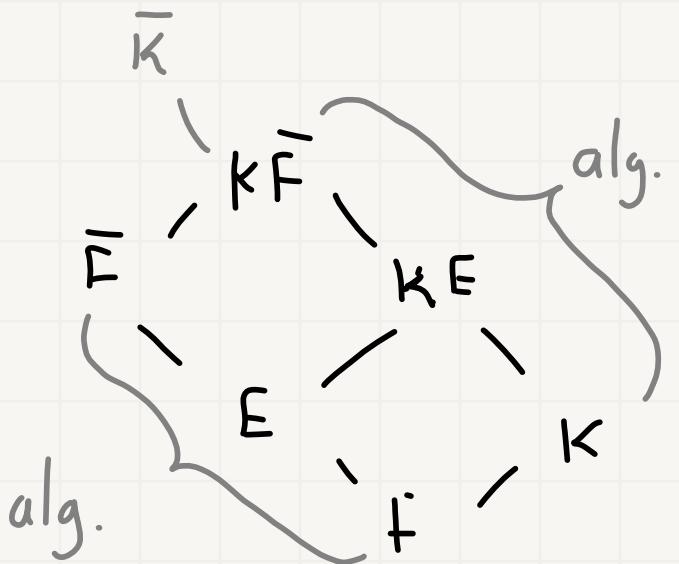
### Dem.

De (i): Sean  $\alpha, \beta \in \bar{K}$  lí-ron;ugados donde  $\bar{K}$  es una cerradura algebraica de  $E \subseteq \bar{K}$  y  $\alpha \in E$ . Probaremos que  $\beta \in E$ . Sean  $g(x) = \text{irr}(\alpha, K, x)$  y  $f(x) = \text{irr}(\alpha, F, x)$ . Tenemos que  $f(\alpha) = 0 = f(\beta)$ . Además como  $f(x) \in F[x] \subseteq K(x)$ , ent.  $g(x) | f(x) \Rightarrow \alpha$  y  $\beta$  son raíces de  $f(x)$ , i.e  $\alpha$  y  $\beta$  son  $F$ -conjugados con  $\alpha \in E$  y al ser  $E/F$  normal  $\Rightarrow \beta \in E$ .

De (ii): Sea  $\{f_i(x)\}_{i \in I}$  una familia de pol. en  $F(x)$  tal que  $E = F(S)$  donde

$$S = \bigcup_{i \in I} S_i$$

&  $S_i = \{B \in \bar{F} \mid f_i(B) = 0\}, \forall i \in I$ , para  $\bar{F}$  una cerradura algebraica de  $F$  que contiene a  $E$ . Tenemos que  $KE/k$  es una ext. algebraica y  $\{f_i(x)\}_{i \in I}$  es una fam. de pol. en  $K(x)$  la cual s. aliste que, considerando el diagrama, donde  $\bar{K}$  es una cerradura algebraica de  $K$  que contiene a  $KE$ .



Así que  $S_i \subseteq \bar{F}, \forall i \in I$ .

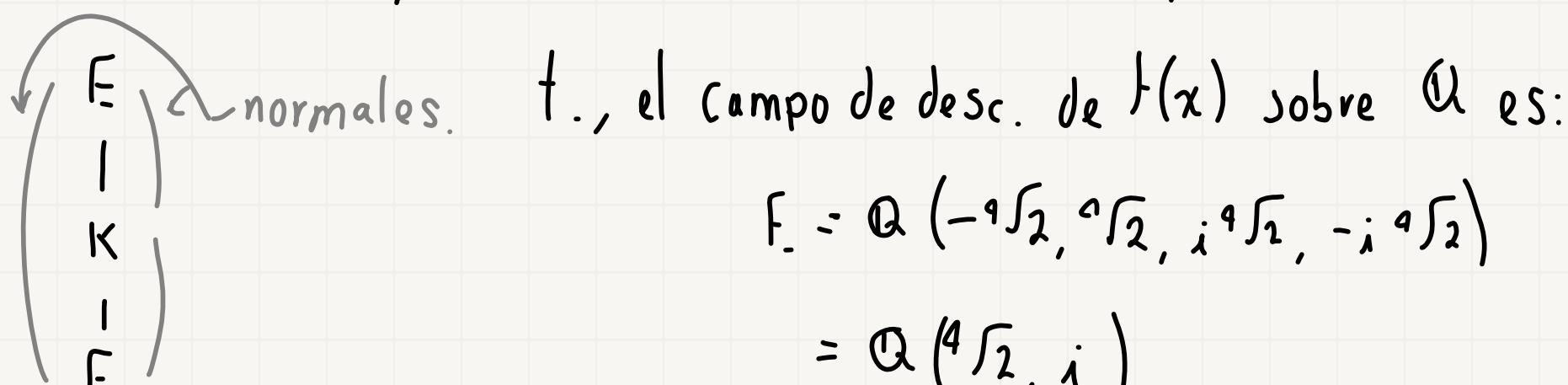
Como  $\bar{F} \subseteq \bar{K}$ , se tiene que  $f_i(x) \in K[x] \& S_i \subseteq \bar{K}, \forall i$   
F.I. Por lo tanto:

$$KE = KF(S) = K(S)$$

i.e.  $KE/K$  es normal, pues  $KE$  es el campo de des. de la familia  $\{f_i(x)\}_{i \in I}$  en  $K[x]$ . □

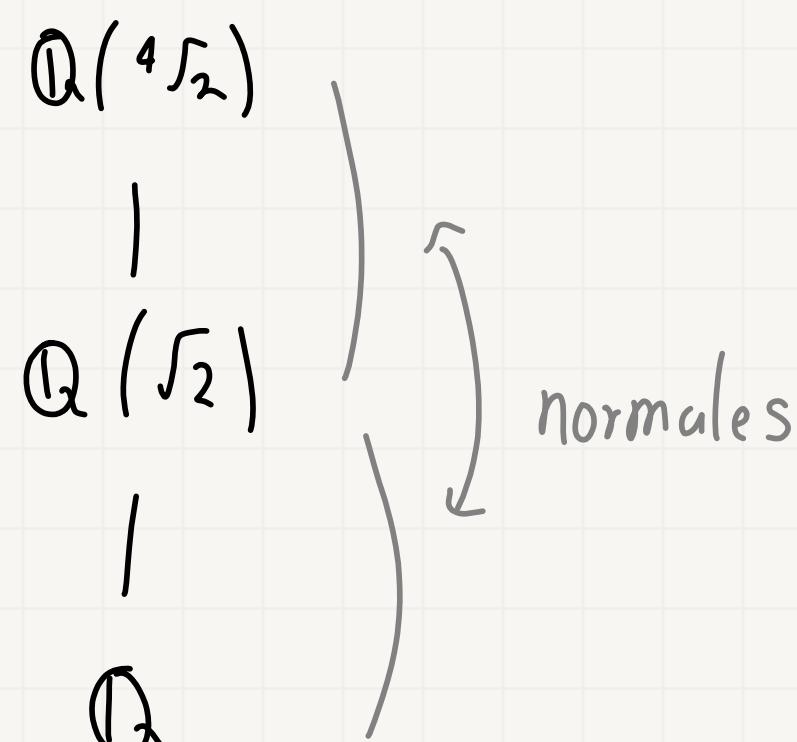
**Obs)** La clase de extensiones normales. Afirmamos que no es una clase distinguida. En efecto,

en efecto, sea  $f(x) = x^4 - 2 \in \mathbb{Q}[x]$  cuyas raíces son  $\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}$  y  $-i\sqrt[4]{2}$ . En-



Consideremos la torre de campos.  $K = \mathbb{Q}(\sqrt[4]{2})$  y  $F = \mathbb{Q}$ .  $E/F$  es normal y por la p-rop. ant.  $E/K$  lo es, pero  $K/F$  no es normal yu qm?  $\sqrt[4]{2}i$  es raíz de  $x^4 - 2 \in \mathbb{Q}(x)$ , y  $\sqrt[4]{2} \in \mathbb{Q}(\sqrt[4]{2})$ , pero  $i\sqrt[4]{2} \notin \mathbb{Q}(\sqrt[4]{2})$ .

Por otro lado, considere la torre de campos, por lo ant.  $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$  no es normal.



**Proposición.**

Sean  $E/F$  y  $K/F$  extensiones normales con  $E$  y  $K$  subcampos de un campo común, ent.  
 $EK/F$  es normal.

**Dem.**

Expresamos  $E = F(S)$  &  $K = F(T)$  como campos de desc. de familias de pol.  $\{f_i(x)\}_{i \in J}$  y  $\{g_j(x)\}_{j \in J}$  sobre  $F$ .

Definimos  $U := S \cup T$ . Ent.

$$F(U) = F(S \cup T) = F(S)(T) = EF(T) = EK$$

i.e.  $EK$  es el campo de desc. sobre  $F$  de la fam. de pol.  $\{f_i(x), g_j(x)\}_{(i,j) \in I \times J}$  en  $F$ .

Luego  $EK/F$  es normal. □

**Proposición.**

Sea  $E/F$  una ext. algebraica y  $\bar{F}$  una cerradura alg. de  $F$  m  $E \subseteq \bar{F}$ . Ent,

i)  $\bar{F}/F$  es normal.

ii) Sea  $\{K_i\}_{i \in I}$  una familia de subcampos de  $\bar{F}$  que contienen a  $E$  y que  $K_i/F$  es normal,  $\forall i \in I$ . Ent.

$$K := \bigcap_{i \in I} K_i$$

es un subcampo de  $\bar{F}$  que contiene a  $E$  y tal que  $K/F$  es normal.

**Dem.**

De (i): Es inmediato.

De (ii): Basta probar que  $K/F$  es normal. Sea  $\alpha \in K$  &  $\beta \in \bar{F}$   $F$ -conjugados. Ent.  $\alpha \in K_i$ ,  $\forall i \in I$ , como  $K_i/F$  es normal y  $\alpha$  y  $\beta$  son  $F$ -conjugados  $\Rightarrow \beta \in K_i, \forall i \in I \Rightarrow \beta \in K$ . Luego  $E/K$  es normal. □

**Obs)** La intersección de extensiones normales sobre un mismo campo base  $F$ , es normal.

**Def.** Sea  $E/F$  una extensión algebraica y  $\bar{F}$  una cerradura algebraica de  $F$  m  $E \subseteq \bar{F}$ . Un-

a Cerradura normal de la extensión  $E/F$  es la intersección de la familia  $\{K \mid K \text{ es subcampo de } \bar{F} \text{ y } E \subseteq K \text{ y } K/F \text{ es normal}\}$ .

Así, la cerradura normal de una extensión algebraica  $E/F$  es el mínimo subcampo  $N$  de  $\bar{F}$  que contiene a  $E$ , tal que  $N/F$  es normal.

**Obs)** Cualesquier dos cerraduras normales de una ext. alg. algebraica  $E/F$  son  $F$ -isomórfas.

### Teorema.

Sea  $E/F$  una extensión algebraica y  $\bar{F}$  una cerradura alg. de  $F$  en  $E \subseteq \bar{F}$ . Sea  $N$  un subcampo de  $\bar{F}$  que contiene a  $E$ . Ent.  $N$  es la cerradura normal de  $E/F \Leftrightarrow N$  es el campo de jsc. de la familia de polinomios  $\{f_\alpha(x)\}_{\alpha \in E \setminus F}$  donde  $f_\alpha(x) = \text{irr}(\alpha, F, x) \quad \forall \alpha \in E \setminus F$ .

### Dem.

Sea  $N$  la cerradura normal de la extensión  $E/F$ , y sea  $N_0 = F(S)$ , donde

$$S := \bigcup_{\alpha \in E \setminus F} S_\alpha$$

dónde  $S_\alpha = \{\beta \in \bar{F} \mid f_\alpha(\beta) = 0\}, \forall \alpha \in E \setminus F$ . Para probar el resultado, basta ver que

$$N = N_0$$

Se tiene que  $F \subseteq N_0$  y  $N_0/F$  es normal, luego  $N \subseteq N_0$  por def. de cerradura normal.

Sea  $\beta \in S \Rightarrow \exists \alpha \in E \setminus F$  en  $f_\alpha(\beta) = 0 \Rightarrow \alpha \& \beta$  son  $F$ -conjugados donde  $\alpha \in E \subseteq N$

como  $N/F$  es normal, ent.  $\beta \in N$ . Así,  $S \subseteq N$  y por ende

$$N_0 \subseteq N$$

$$\therefore N = N_0$$

□

### Teorema.

Sea  $E/F$  una extensión algebraica,  $\bar{F}$  una cerradura alg. de  $F$  en  $E \subseteq \bar{F}$  y  $U \subseteq$

$E \cap E = F(u)$ . Si  $N$  es la cerradura normal de  $E/F$ , ent.  $N$  es el campo de descomposición de la familia de polinomios  $\{f_\alpha(x)\}_{\alpha \in U}$  donde  $f_\alpha(x) = \text{irr}(\alpha, F, x)$   $\forall \alpha \in U$ .

Dem.

Sea  $N_1$  el campo de descomposición de la familia de polinomios  $\{f_\alpha(x)\}_{\alpha \in U}$ . Sobre  $F$ . Tenemos que  $N_1/F$  es extensión normal. Notemos que  $F = F(u) \subseteq F(S) = N_1$ , donde  $S$  es el conjunto de raíces en  $\bar{F}$  de la fam. de pol.  $\{f_\alpha(x)\}_{\alpha \in U}$ . Luego ent. necesariamente  $N \leq N_1$  por minimalidad. Pero de ac. con la demostración del t. ant. se tiene que  $N_1 \leq N$ .  $\therefore N = N_1$ . □

Corolario.

Si  $E/F$  es una extensión finita &  $N$  es la cerradura normal de  $E/F$ , ent.  $N/F$  es una extensión finita.

Dem.

Sea  $U \subseteq E$  finito y  $E = F(U)$ . De acuerdo con la dem. del t. ant., tenemos que  $S$  debe ser finito y  $N = F(S)$ . Luego la extensión  $N/F$  es alg. y f.g.  $\Rightarrow N/F$  es finita. □

Ejemplo.

1) Sea  $n \in \mathbb{N}$ . Encontremos la cerradura normal de  $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ . Denotemos por  $\zeta_n = e^{\frac{2\pi i}{n}}$   $\in \mathbb{C}$ . Sabemos que  $\zeta_n$  es una raíz  $n$ -ésima primitiva de la unidad, i.e.  $\zeta_n$  es generador del grupo cíclico  $\langle \zeta_n \rangle$  constituido por las todas las raíces  $n$ -ésimas de la unidad. Si  $f(x) = \text{irr}(\zeta_n, \mathbb{Q}, x) \in \mathbb{Q}[x]$ , se tiene que  $f(x) | (x^n - 1)$ . Luego, todas las raíces de  $f(x)$  son raíces  $n$ -ésimas de la unidad. Luego, estas raíces son potencias de  $\zeta_n$ , por tanto la cerradura normal de  $\mathbb{Q}(\zeta_n)/\mathbb{Q}$  es  $(\mathbb{Q}(\zeta_n))$ . En part.  $\mathbb{Q}(\zeta_n)/\mathbb{Q}$

es normal.

### Teorema.

Sea  $F \subseteq E \subseteq L$  una torre de campos y  $\varphi: E \rightarrow L$  un  $F$ -homomorfismo. Si  $L/F$  es normal ent.  $\varphi$  se puede extender a un  $F$ -automorfismo de  $L$ .

Dem.

Sea  $\bar{F}$  una cerradura algebraica de  $F \cap L \subseteq \bar{F}$ , y  $\varphi: E \rightarrow L$  un  $F$ -homomorfismo. Como  $L/F$  es algebraica,  $\varphi$  la podemos extender a un  $F$ -homomorfismo  $\bar{\varphi}: L \rightarrow \bar{F}$ . Pero como  $L/F$  es normal, ent.  $\bar{\varphi}$  es un  $F$ -automorfismo de  $L$ .  $\square$

Obs) Sea  $E/F$  una extensión finita y  $\bar{F}$  una cerradura algebraica de  $F \cap E \subseteq \bar{F}$ . Entonces, la cantidad de  $F$ -homomorfismos de  $E$  en  $\bar{F}$  es finita. En efecto, sea  $\alpha_1, \dots, \alpha_n \in E \setminus F$

$$E = F(\alpha_1, \dots, \alpha_n)$$

Sea  $\varphi: E \rightarrow \bar{F}$  un homomorfismo cualquiera, ent.  $\varphi$  está completamente determinado por su acción sobre  $\alpha_1, \dots, \alpha_n$ . Pues si  $\beta \in E$ , ent.  $\exists h(x_1, \dots, x_n) \in F[x_1, \dots, x_n]$  m

$$\begin{aligned} \beta &= h(\alpha_1, \dots, \alpha_n) \\ \Rightarrow \varphi(\beta) &= \varphi(h(\alpha_1, \dots, \alpha_n)) \\ &= h(\varphi(\alpha_1), \dots, \varphi(\alpha_n)) \\ &= h(\varphi(\alpha_1), \dots, \varphi(\alpha_n)) \end{aligned}$$

Pero, notemos que para cada  $i \in [1, n]$ , si  $f_i(x) = \text{irr}(\alpha_i, F, x)$ , ent.  $\varphi(\alpha_i)$  y  $\alpha_i$  son  $F$ -conjugados. Por lo tanto, sólo hay una cantidad finita de  $F$ -homomorfismos de  $E$  en  $\bar{F}$ .

## Teorema.

Sean  $F \subseteq K \subseteq E \subseteq L$  una torre de campos con  $L/F$  extensión normal y finita. Supóngase que la cantidad de  $K$ -homomorfismos de  $E$  en  $L$  es  $n$ . Si  $\varphi$  es un  $F$ -homomorfismo de  $K$  en  $L$ , ent.  $\varphi$  tiene exactamente  $n$  extensiones a homomorfismos de  $E$  en  $L$ .

## Dem.

Sean  $\psi_1, \dots, \psi_n$  los  $K$ -homomorfismos de  $E$  en  $L$ . Extendemos cada  $\psi_j$  a  $K$ -automorfismos  $\bar{\psi}_j : L \rightarrow L$ . También extendemos  $\varphi$  a un  $F$ -automorfismo  $\bar{\varphi}$  de  $L$  en  $L$ .

Definimos para cada  $j \in [1, n]$ :

$$\varphi_j := \bar{\varphi} \circ \bar{\psi}_j|_E : E \rightarrow L$$

Afirmamos que  $\varphi_j$  son todos los  $F$ -homomorfismos distintos de  $E$  en  $L$  que son extensiones de  $\varphi$ .

En efecto, es claro que todos los  $\varphi_j$  son homomorfismos. Más aún, son  $F$ -homomorfismos de  $E$  en  $L$ . Por otro lado, si  $\alpha \in K$ , ent.

$$\begin{aligned}\varphi_j(\alpha) &= \bar{\varphi} \circ \bar{\psi}_j|_E(\alpha) \\ &= \bar{\varphi}(\alpha) \\ &= \varphi(\alpha)\end{aligned}$$

i.e las  $\varphi_j$  son extensiones de  $\varphi$ . Probemos que  $\forall j, k \in [1, n]$  con  $j \neq k$  se tiene que

$$\varphi_j \neq \varphi_k$$

$$\begin{aligned}\text{Como } \psi_j \neq \psi_k, \exists \beta \in E \text{ tal que } \psi_j(\beta) \neq \psi_k(\beta) \Rightarrow \bar{\psi}_j(\beta) \neq \bar{\psi}_k(\beta) \\ \Rightarrow \bar{\varphi}(\bar{\psi}_j(\beta)) \neq \bar{\varphi}(\bar{\psi}_k(\beta))\end{aligned}$$

(Por ser  $\bar{\varphi}$  inyectiva).

$$\therefore \varphi_j(B) \neq \varphi_k(B)$$

Finalmente, sea  $\sigma: E \rightarrow L$  un  $F$ -homomorfismo extensión de  $\psi$ . Extendemos  $\sigma$  a un  $F$ -automorfismo de  $L$ , y la denotamos por  $\bar{\sigma}$ . Tenemos que  $\bar{\varphi}^{-1} \circ \bar{\sigma}$  es un automorfismo de  $L$  que deja fijo a los elementos de  $K$ , ya que si  $r \in K$  ent.

$$\begin{aligned} (\bar{\varphi}^{-1} \circ \bar{\sigma})(r) &= \bar{\varphi}^{-1}(\bar{\sigma}(r)) \\ &= \bar{\varphi}^{-1}(\varphi(r)) \\ &= \bar{\varphi}^{-1}(\bar{\varphi}(r)) \\ &= r \end{aligned}$$

$$\therefore \bar{\varphi}^{-1} \circ \bar{\sigma}|: E \rightarrow L$$

es un  $K$ -homomorfismo de  $E$  en  $L \Rightarrow \exists j \in [1, n] \cap \bar{\varphi}^{-1} \circ \bar{\sigma}|_E = \psi_j = \bar{\psi}_j|_E \Rightarrow \forall B \in E$

$$(\bar{\varphi}^{-1} \circ \bar{\sigma})(B) = \bar{\psi}_j(B)$$

i.e.

$$\bar{\sigma}(B) = \bar{\varphi} \circ \bar{\psi}_j(B)$$

$$\Rightarrow \sigma(B) = \bar{\varphi} \circ \bar{\psi}_j|_E(B) = \varphi_j(B), \forall B \in E$$

$\therefore \sigma = \varphi_j$  para algún  $j \in [1, n]$ .

## Proposición.

Sea  $F$  un campo &  $f(x) \in F[x] \setminus F$ .

i) Si  $\text{car}(F) = 0$ , ent.  $f'(x) \neq 0$ .

ii) Si  $\text{car}(F) = p > 0$ , ent.  $f'(x) = 0 \Leftrightarrow \exists g(x) \in F[x]$  tal que  $f(x) = g(x^p)$ .

Dem.

Expresamos a  $f(x)$  como:

$$f(x) = a_0 + a_1 x + \dots + a_n x^n, \quad n \geq 1 \text{ y } a_n \neq 0.$$

De (i): Se tiene que  $f'(x) = n a_n x^{n-1} + \dots$  donde  $n a_n \neq 0$  ya que  $\text{car}(F) = 0$ . Por tanto  $f'(x) \neq 0$ .

De (ii):

$\Leftarrow$ ) Supongamos que  $\exists g(x) \in F[x]$  tal que  $f(x) = g(x^p)$ . Expresamos  $g(x) = b_0 + b_1 x + \dots + b_m x^m$ , donde  $b_m \neq 0$ . Ent.

$$\begin{aligned} f(x) &= g(x^p) = b_0 + b_1 x^p + \dots + b_m x^{pm} \\ \Rightarrow f'(x) &= pb_1 x^{p-1} + \dots + pm b_m x^{pm-1} \\ &= 0 x^{p-1} + \dots + 0 x^{pm-1} \\ &= 0 \end{aligned}$$

$\Rightarrow$ ) Supongamos que  $f'(x) = 0$ , donde  $f'(x) = \sum_{i=1}^n i a_i x^{i-1}$ , ent.  $i a_i = 0, \forall i \in [1, n]$ . Si  $a_i \neq 0$  ent.  $i \cdot 1 = i = 0 \Rightarrow \text{car}(F) = p | i, \forall i \in [1, n], a_i \neq 0$ . Luego  $\exists m_i \in \mathbb{N}$  m  $i = pm_i$ .  $\forall i \in [1, n], a_i \neq 0$ .

Por ende:

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

dónde  $g(x) = a_0 + a_{pm_1} x^{m_1} + \dots + a_{pm_n} x^{m_n}$ , donde  $a_{pm_i} \neq 0 \quad \forall i \in [1, n] \text{ m } a_i \neq 0, g(x) \neq 0$

□

## Corolario.

Sea  $F$  campo y  $f(x) \in F[x]$  irreducible.

- i) Si  $\text{car}(F) = 0$ , ent. todas sus raíces son simples.
- ii) Si  $\text{car}(F) = p > 0$ , ent.  $f(x)$  tiene una raíz múltiple  $\Leftrightarrow \exists g(x) \in F[x]$  m  $f(x) = g(x^p)$ .

Dem.

Es inmediata.

□

## Teorema.

Sea  $F$  un campo con  $\text{car}(F) = p > 0$ . Sea  $f(x) \in F[x]$  irreducible, y  $e$  el entero no neg. tal que  $f(x) \in F[x^{p^e}]$  pero  $f(x) \notin F[x^{p^{e+1}}]$ . Sea  $\Psi(x) \in F[x]$  m  $f(x) = \Psi(x^{p^e})$ . Ent.

- i)  $\Psi(x)$  es un polinomio irreducible de  $F[x]$ .
- ii) Todas las raíces de  $\Psi(x)$  son simples.
- iii) Todas las raíces de  $f(x)$  tienen la misma multiplicidad, a saber  $p^e$ .
- iv) Si  $m = \text{grad}(\Psi(x)) \Rightarrow \text{grad}(f(x)) = p^e m$ .

Dem.

De (i): Si  $\Psi(x)$  fuera descomponible, ent.  $\exists g(x), h(x) \in F[x]$  m  $\text{grad}(g(x)), \text{grad}(h(x))$

$\geq 1$  y:

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

donde  $g_1(x) = g(x^{p^e})$  y  $h_1(x) = h(x^{p^e})$  con  $\text{grad}(g_1(x)), \text{grad}(h_1(x)) \geq 1 \Rightarrow f(x)$  es reducible x.c. Luego  $\Psi(x)$  es irreducible.

De (ii): Supongamos que  $\Psi(x)$  admite una raíz múltiple  $\Rightarrow \exists g(x) \in F[x]$  s.t.  $\Psi(x) = g(x^p)$ .  
 $\Rightarrow f(x) = \Psi(x^{p^e}) = g(x^{p^{e+1}}) \in F[x^{p^{e+1}}]_{\neq c}$ .

Entonces  $\Psi(x)$  tiene todas sus raíces simples.

De (iii): Sea  $m = \text{grad}(\Psi(x))$ . Sean  $B_1, \dots, B_m \in \bar{F}$  todas las raíces de  $\Psi(x)$  en alguna Cerradura alg. de  $F$ .

$$\begin{aligned}\Rightarrow \Psi(x) &= a(x - B_1) \cdots (x - B_m) \text{ con } a \in F. \\ \Rightarrow f(x) &= \Psi(x^{p^e}) \\ &= a(x^{p^e} - B_1) \cdots (x^{p^e} - B_m)\end{aligned}$$

Para cada  $i \in [1, m]$ , sea  $\alpha_i \in \bar{F}$  raíz del polinomio  $x^{p^e} - B_i$ , i.e.  $B_i = \alpha_i^{p^e}$ . Notemos que si  $i \neq j$ , ent.  $\alpha_i \neq \alpha_j$ .

$$\begin{aligned}\Rightarrow f(x) &= a(x^{p^e} - B_1) \cdots (x^{p^e} - B_m) \\ &= a(x^{p^e} - \alpha_1^{p^e}) \cdots (x^{p^e} - \alpha_m^{p^e}) \\ &= a(x - \alpha_1)^{p^e} \cdots (x - \alpha_m)^{p^e}\end{aligned}$$

$\Rightarrow f(x)$  tiene por raíces a  $\alpha_1, \dots, \alpha_m$  y todas tienen multiplicidad  $p^e$ .

De (iv): Es inmediato. □

### Corolario.

Sea  $F$  campo y  $f(x) \in F[x]$  irreducible. Ent. todas las raíces de  $f(x)$  tienen la misma multiplicidad. Si  $\text{car}(F) = 0$ , la mult. es 1. Y si  $\text{car}(F) = p > 0$  ent. todas las raíces de  $f(x)$  tienen multiplicidad  $p^e$  para algún  $e > 0$ .

### Dem.

Es inmediata. □

De acuerdo con las notaciones del teorema cont. y su demostración, tenemos que el grado de

$\psi$  es llamado el grado de separabilidad de  $f$ , y el entero no neg.  $e$  es llamado el grado de inseparabilidad de  $f$ .

Así pues, el grado de separabilidad de  $f$  es el número de raíces distintas de  $f$ . Si  $\alpha \in \bar{F}$  con  $f(x) = \text{irr}(\alpha, F, x)$ , ent. el grado de separabilidad de  $\alpha$  es el grado de separabilidad de  $f$ , y el exponente  $e$  de inseparabilidad de  $f$  será el exponente de inseparabilidad de  $\alpha$ . Por supuesto,  $\text{car}(F) = p > 0$ .

Si  $\text{car}(F) = 0$  y  $f(x) \in F[x]$  es pol. irreducible, ent. el grado de separabilidad de  $f$  es el número de raíces dist. de  $f$ , que coincide con su grado. Si  $\alpha \in \bar{F}$  y  $f(x) = \text{irr}(\alpha, F, x)$ , se tiene que el grado de separabilidad de  $\alpha$  es el grado de separabilidad de  $f$ .

En cualquier caso,  $\text{car}(F) = p > 0$  el grado de separabilidad de  $\alpha$  se denota por:

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

Si  $\text{car}(F) = 0$ , ent.

$$[F(\alpha) : F]_s = [F(\alpha) : F] = \text{grad}(\text{irr}(\alpha, F, x))$$

Si  $\text{car}(F) = p > 0$ , ent.

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

### Proposición.

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

### Dem.

Sea  $f(x) = \text{irr}(\alpha, F, x)$ . Sean  $\alpha_1, \dots, \alpha_m \in \bar{F}$  las raíces distintas de  $f(x)$ . Tenemos que  $m = [F(\alpha) : F]_s$ .

Sea  $\varphi : F(\alpha) \rightarrow \bar{F}$  un  $F$ -homomorfismo. Sabemos que  $\psi$  está completamente determinado

da por su acción sobre  $\alpha$ , teniendo que  $\varphi(\alpha)$  es raíz de  $f(x)$ , i.e.  $\varphi(\alpha) = \alpha$ : 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.

□

**Def.** 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 alg. d<sub>2</sub>  $F$  que contiene a  $E$ . Tal cardinal es denotado por  $[E : F]_s$ .

**Teorema.**

Sea  $E/F$  una extensión finita y  $K$  un campo intermedio de  $E/F$ . Ent.

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

**Dem.**

Ya se tiene.

□

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

**Obs**) Sea  $F$  campo y  $\bar{F}$  cerradura alg. de  $F$ .

i) Si  $\alpha \in \bar{F}$ , ent.  $\alpha$  es separable sobre  $F \Leftrightarrow f(x) = \text{irr}(\alpha, F, x)$  es tal que todos sus raíces son simples. Cuando esto ocurre, decimos que  $f(x)$  es separable sobre  $F$ .

ii) Es decir, un polinomio irreducible  $f(x) \in F[x]$  es separable.

iii) Si  $g(x) \in F[x]$ , decimos que  $g(x)$  es separable sobre  $F$  si sus factores irreducibles son separables sobre  $F$ .

## Proposición.

Sea  $E/F$  una extensión finita con  $\text{car}(F) = p > 0$ . Ent. existe un elemento  $t \geq 0$  tal que

$$[E:F] = p^t [E:F]_s, t \in \mathbb{Z}.$$

En part. si  $p \nmid [E:F]$ , ent.  $[E:F] = [E:F]_s$ .

## Dem.

Sean  $\alpha_1, \dots, \alpha_n \in E$  m  $E = F(\alpha_1, \dots, \alpha_n)$ . Consideramos la torre de campos  $F \subseteq F(\alpha_1) \subseteq \dots \subseteq F(\alpha_1, \dots, \alpha_{n-1}) \subseteq F(\alpha_1, \dots, \alpha_n)$ . Sea  $e_i$  el exponente de inseparabilidad de  $\alpha_i$  sobre  $F(\alpha_1, \dots, \alpha_{i-1})$ , para  $i = 2, \dots, n$  &  $e_1$  es el grado de inseparabilidad de  $\alpha_1$  sobre  $F$ .

Luego:

$$\begin{aligned}[E:F]_s &= [F(\alpha_1, \dots, \alpha_n) : F(\alpha_1, \dots, \alpha_{n-1})]_s \cdots [F(\alpha_1) : F]_s \\ &= \frac{1}{p^{e_n}} [F(\alpha_1, \dots, \alpha_n) : F(\alpha_1, \dots, \alpha_{n-1})] \cdots \frac{1}{p^{e_1}} [F(\alpha_1) : F] \\ \Rightarrow [E:F] &= p^{e_1 + e_2 + \dots + e_n} [E:F]_s, t = e_1 + e_2 + \dots + e_n \geq 0, t \in \mathbb{Z}. \end{aligned}$$

□

Obs) Si  $E/F$  es una ext. finita y  $\text{car}(F) = 0$ , ent.  $[E:F]$ .

## Proposición.

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

- i)  $\alpha^{p^e}$  es separable sobre  $F$ .
- ii) Las sig. cond. son equivalentes:
  - a)  $\alpha$  es separable sobre  $F$ .
  - b)  $[F(\alpha) : F]_s = [F(\alpha) : F]$ .
  - c)  $e = 0$ .
  - d)  $F(\alpha) = F(\alpha^p)$ .

**Dem.**

De (i): Sea  $f(x) = \text{irr}(\alpha, F, x)$  &  $\Psi(x) \in F[x]$  m  $\Psi(x^{p^e}) = f(x)$ , pero  $f(x) \notin F[x^{p^{e+1}}]$ . Sabemos que  $\Psi(x)$  es irr. sobre  $F$  y todas sus raíces son simples, donde:

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

i.e.  $\alpha^{p^e}$  es raíz de  $\Psi(x)$ , por lo cual  $\Psi(x) = \text{irr}(\alpha^{p^e}, F, x)$ . Por tanto  $\alpha^{p^e}$  es separable sobre  $F$ .

De (ii): Es claro que  $a) \Leftrightarrow b) \Leftrightarrow c)$ . Probaremos que  $a) \Leftrightarrow d)$ . Antes, notemos que

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

$a) \Rightarrow d)$ : Sea  $f(x) = \text{irr}(\alpha, F, x)$ . Tenemos que  $g(x) := x^p - \alpha^p \in F(\alpha^p)[x]$  y  $g(\alpha) = 0 \Rightarrow \text{irr}(\alpha, F(\alpha^p), x) | g(x)$  &  $\text{irr}(\alpha, F(\alpha^p), x) | f(x)$  en  $F(\alpha^p)[x]$ .

Entonces, como todas las raíces de  $f(x)$  son simples, ent. todas las raíces de

$$h(x) = \text{irr}(\alpha, F(\alpha^p), x)$$

también son simples; además  $h(x) | x^p - \alpha^p = (x - \alpha)^p \Rightarrow h(x) = x - \alpha \Rightarrow \alpha \in F(\alpha^p)$ .  $\therefore F(\alpha) = F(\alpha^p)$ .

$d) \Rightarrow a)$ : Recíprocamente, supongamos que  $F(\alpha^p) = F(\alpha)$  pero  $\alpha$  no es separable sobre  $F$ . Siendo  $f(x) = \text{irr}(\alpha, F, x)$ , tenemos que  $f(x) \in F[x^p]$ , i.e. existe  $g(x) \in F[x]$  m  $f(x) = g(x^p)$  donde  $\text{gr}(f(x)) = p \text{gr}(g(x)) > \text{gr}(g(x))$ . Notemos que  $g(x)$  tiene por raíz a  $\alpha^p$ , pues  $g(\alpha^p) = f(\alpha) = 0 \Rightarrow \text{irr}(\alpha^p, F, x) | g(x) \Rightarrow [F(\alpha^p) : F] = \text{gr}(\text{irr}(\alpha^p, F, x)) \leq \text{gr}(g(x)) < \text{gr}(f(x)) = [F(\alpha) : F]$ , luego  $F(\alpha^p) \not\subseteq F(\alpha)$ . Por tanto,  $\alpha$  es separable sobre  $F$ .

□

**Proposición.**

Sea  $E/F$  una ext. finita. Ent.  $E/F$  es separable  $\Leftrightarrow [E : F]_S = [E : F]$ .

Dem.

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

$$F \subseteq F(\alpha_1) \subseteq \dots \subseteq F(\alpha_1, \dots, \alpha_{n-1}) \subseteq F(\alpha_1, \dots, \alpha_n) = E$$

Para cada  $i \in [2, n]$ , tenemos que  $\alpha_i$  es separable y por ende, lo es sobre  $F(\alpha_1, \dots, \alpha_{i-1})$ .

Luego,

$$\begin{aligned} [E:F]_S &= [F(\alpha_1, \dots, \alpha_n):F(\alpha_1, \dots, \alpha_{n-1})]_S \cdot \dots \cdot [F(\alpha_1, \alpha_2):F(\alpha_1)]_S \cdot [F(\alpha_1):F]_S \\ &= [F(\alpha_1, \dots, \alpha_n):F(\alpha_1, \dots, \alpha_n)] \cdot \dots \cdot [F(\alpha_1, \alpha_2):F(\alpha_1)] \cdot [F(\alpha_1):F] \\ &= [E:F] \end{aligned}$$

$\Leftarrow$  Sea  $\alpha \in E$  arbitrario. Tenemos lo sig.

$$\begin{aligned} [E:F(\alpha)]_S \cdot [F(\alpha):F]_S &= [F:F]_S \\ &= [E:F] \\ &= [E:F(\alpha)] \cdot [F(\alpha):F] \dots (1) \end{aligned}$$

dónde  $[E:F(\alpha)]_S \leq [E:F(\alpha)]$  &  $[F(\alpha):F]_S \leq [F(\alpha):F]$ . Por tanto, de (1) se

Sigue que:

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

i.e.  $\alpha$  es separable sobre  $F$ . Como el  $\alpha$  fue arb. ent. se sigue que  $E/F$  es una ext. separable.

□

Obs) Sea  $F \subseteq K \subseteq E$  una torre de campos y  $\alpha \in E$  separable sobre  $F$ . Ent.  $\alpha$  es separable sobre  $K$ . Más general, sea  $E/F$  y  $K/F$  extensiones de campos y  $\alpha \in E$  separable sobre  $F$ . Si  $\alpha$  es elemento de un campo  $L$  extensión de  $K$ , ent.  $\alpha$  es separable sobre  $K$ .

## Proposición.

Sea  $E/F$  una extensión de campos y  $S \subseteq E$  m  $E = F(S)$ . Sea  $K = \{ \alpha \in E \mid \alpha \text{ es separable sobre } F \}$ . Ent.

i)  $K$  es subcampo intermedio de la ext.  $E/F$ .

ii)  $E/F$  es separable  $\Leftrightarrow \alpha$  es separable sobre  $F, \forall \alpha \in S$ .

Dem.

De (i): Si  $\alpha \in F \Rightarrow \alpha$  es alg. sobre  $F$  &  $f(x) = x - \alpha = \text{irr}(\alpha, F, x) \Rightarrow \alpha$  es sep. sobre  $F$ .  $\Rightarrow F \subseteq K \subseteq E$ .

Sean ahora  $\alpha, \beta \in K$ . Consideremos el campo intermedio  $F(\alpha, \beta)$  de la ext.  $E/F$ . Luego, consideremos la torre de campos  $F \subseteq F(\alpha) \subseteq F(\alpha, \beta) \subseteq E$ .

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

i.e  $F(\alpha, \beta)/F$  es separable, luego  $\alpha - \beta, \alpha\beta, \alpha^{-1} \in F(\alpha, \beta)$  son sep. sobre  $F$ .  $\therefore$

$K$  es campo.

De (ii):

$$\begin{array}{c}
 E \\
 \sqsubset F_i \sqcap F_s \\
 \left. \begin{array}{c} F_i \\ F_s \end{array} \right\} \text{P.i.} \\
 \left. \begin{array}{c} F_i \sqcap F_s \\ F_i \sqsubset F_s \end{array} \right\} \text{P.i.} \\
 \left. \begin{array}{c} F_i \sqcap F_s \\ F_i \sqsubset F_s \end{array} \right\} \text{P.i.} / \text{S.e.} \\
 F_i \sqcap F_s = F
 \end{array}$$







## Notas.

- 1) Sean  $K$  campo. Decimos que  $F$  es una extensión del campo  $K$ , si  $K \subseteq F$  y  $F$  es campo.  
 $F/K$  se llama una extensión de campos.
- 2) Deben ser no triviales, luego  $[0]$  y  $(0)$  no serían elementos de  $F$ . De esta forma  $1 \in (S)$ .
- 3)  $K(S) = B$ . Probar que  $B$  es subcampo de  $F$ . Si  $\alpha, \beta \in B \Rightarrow \alpha - \beta, \alpha\beta, \alpha^{-1} \in B$ . Para el último caso:
- $$\alpha = \frac{f(u_1, \dots, u_n)}{g(u_1, \dots, u_n)}, \quad \beta = \frac{h(v_1, \dots, v_m)}{t(v_1, \dots, v_m)}, \quad f(x_1, \dots, x_n), g(x_1, \dots, x_n) \in K[x_1, \dots, x_n] \text{ y}$$
- $$h(y_1, \dots, y_m) \in K(y_1, \dots, y_m) \text{ y lo mismo con } t.$$

4) Si fuera trivial,  $\deg|_F(1) = 0 \Rightarrow 1 \in \langle f(x) \rangle \Rightarrow \langle f(x) \rangle = F[x]_{\neq 0}$ , pues  $\deg(f(x)) \geq 1$ .

5) Si  $r = g(\alpha)$  y  $r_i = g_i(\alpha)$ , ent.

$$\begin{aligned}\overline{\varphi_i}(r * r_i) &= \overline{\varphi_i}(g(\alpha) * g_i(\alpha)) \\ &= \overline{\varphi_i}((g * g_i)(\alpha)) \\ &= (g * g_i)^{\varphi_i}(\beta_i) \\ &= (g^{\varphi_i} * g_i^{\varphi_i})(\beta_i) \\ &= g^{\varphi_i}(\beta_i) * g_i^{\varphi_i}(\beta_i) \\ &= \overline{\varphi_i}(r) * \overline{\varphi_i}(r_i)\end{aligned}$$