Teorema: Sea $0 \neq f \in F[x]$. Entonces existe un campo $E \supseteq F$ tal que f se escinde en $E[x]$.

Dem:

Escribamos $f(x) = g(x) \prod_{i=1}^{r} (x - \alpha_i)$ con $g(x) \in F[x]$ y $\alpha_i \in F$. (La r puede ser cero). H Hacemos inducción sobre $gr(g)$. Si el $gr(g) = 0$, entonces $f(x) = a \prod_{i=1}^{r} (x - \alpha_i)$ se escinde sobre F. Sup. que $gr(g) > 0$. Entonces g tiene un factor irreducible. Por el lema anterior hay un campo $K \supseteq F$ en el cual ese factor irreducible tiene una raíz y por lo tanto g tiene una raíz en K. Digamos que $\beta \in K$ es tal que $g(\beta)=0$. Entonces $(x-\beta) | g(x)$ en K. Por lo tanto $\exists g_0 \in K[x]$ t.q.

$$f(x) = \underline{g_0(x)}(x-\beta)\prod_{i=1}^{r}(x-\alpha_i)$$ con $\beta \in K$ y $\alpha_i \in F \subseteq K$

y $gr(g_0) < gr(g)$. Por hip. de induccion existe un campo $E \supseteq K \supseteq F$ tal que g_0 se escinde sobre E.

Por lo tanto $f(x)$ se escinde sobre E.

Def: Sea $F \subseteq E$ una extesion de campos y $f \in F[x]$. Supongamos que f se escinde sobre E. Decimos que E es el campo de descomposicion de $f(x)$ si E esta generado sobre F, por las raices de $f(x)$ en E.

Lema: Sea $f(x)\in F[x]$ y $F\subseteq L$ tal que f se escinde sobre L. Entonces L contiene un único campo de descomposición E de f sobre F. También E está contenido en cualquier otro campo intermedio $F\subseteq K\subseteq L$ en el que f se escinda.

Dem:

Escribamos $f(x)=a\prod_{i=1}^{n}(x-\alpha_i)$ donde $a\in F$ y cada $\alpha_i\in L$. Sea $E=F[\alpha_1,\dots,\alpha_n]$. Entonces $F\subseteq E\subseteq L$ y se ve que $f(x)$ se escinde sobre E.

Ahora supongamos que $F\subseteq K\subseteq L$ y que f se escinde sobre K. Como $f(x)$ se escinde en K, cada una de las α_i tiene que estar en K. Ya que si $f(x)=b\prod(x-\overline{\beta_i})$

en $K \subseteq L$. Tenemos que $r = b$. Tomando α_j

$f(\alpha_j) = 0 \Rightarrow \prod(\alpha_j - b_i)$. Por lo tanto $\alpha_j = b_i \in K$.

Esto implica que $E \subseteq K$.

Cor. Sea $0 \neq f \in F[x]$. Entonces existe un campo de descomposición de f sobre F.

Notemos que un campo de descomposicion de $f(x) \in F[x]$, siempre es una extensión finita sobre F.

Teorema: Sea $\varphi : F_1 \to F_2$ un isomorfismo de campos y sea $f_1 \in F_1[x]$ con $\hat{\varphi} f_1 = f_2$. Supongamos que E_i es un campo de descomposición de f_i sobre F_i. Entonces φ se extiende a un isomorfismo de E_1 en E_2.

Dem:

Por induccion sobre $[E_1:F_1]$. Si el grado es 1 entonces f_1 se escinde sobre F_1, lo que implica que f_2 se escinde sobre F_2. Por el teo ant. $E_2=F_2$.

Supongamos que $[E_1:F_1]>1$. Entonces f_1 no se escinde sobre F_1. Así que f tiene un factor irreducible g_1 con $gr(g_1)>1$. Sea $g_2=\hat{\varphi}g_1$. Ent g_2 es un factor irreducible de f_2 con $gr(g_2)>1$. Como f se escinde en E_1, g_1 tambien y puedo tomar una raiz α_1 de g_1. Analogamente tomamos $\alpha_2 \in E_2 \ni g_2(\alpha_2)=0$.

Ahora, sea $K_i=F_i[\alpha_i]$ con $i=1,2$.

$$\hat{\varphi}g_1=g_2 \qquad \begin{array}{ccc} K_1=F[\alpha_1] & \xrightarrow{\exists\theta} & K_2=F[\alpha_2] \\ gr(g_1)>1 \Big| & & \Big| gr(g_2)>1 \\ F_1 & \xrightarrow{\varphi} & F_2 \end{array} \qquad \theta(\alpha_1)=\alpha_2$$

Por lo tanto existe un isomorfismo $\theta: K_1 \to K_2$ que extiende a φ y $\theta(\alpha_1) = \theta(\alpha_2)$.

Afirmamos que E_1 es campo de descomposición de f_1 sobre K_1. Tenemos que $F_1 \subseteq K_1 \subseteq E_1$. Como E_1 esta generado por las raices de f_1 sobre F_1, entonces E_1 esta generado por las raices de f_1 sobre K_1.

Por hip. de ind. θ se extiende a un isomorfismo entre E_1 y E_2. $[E_1 : K_1] < [E_1 : F_1]$

Cor. Sea $f \in F[x]$ y supongamos que $E_1 \supseteq F$ y $E_2 \supseteq F$ son campos de descomposición de f sobre F. Entonces E_1 y E_2 son F-isomorfos.

Ejemplo: $X^4-1 \in \mathbb{Q}[X]$

$x^4-1=(x+1)(x-1)\ x^2+1 \in \mathbb{Q}[x]$.

x^2+1 es irreducible sobre $\mathbb{Q}$

$\mathbb{Q} \longrightarrow \mathbb{Q}[x]/\langle x^2+1\rangle$ es una extension en la cual x^2+1 tiene una raiz, i

Notemos que

$$\mathbb{Q}[x]/\langle x^2+1\rangle = \mathbb{Q}[i] \qquad X^4-1=(x+1)(x-1)(x-i)(x+i)$$

en $\mathbb{Q}[i]$.

$$\begin{array}{c} \mathbb{Q}[i] \\ \Big|\,2 \\ \mathbb{Q} \end{array}$$

$\mathbb{Q}[i]$ es el campo de descomposicion de x^4-1.

Def: Decimos que un campo E es algebraicamente cerrado si todo polinomio $0 \neq f \in E[x]$ se escinde.

Def: Dada una extensión de campos $F \subseteq E$, decimos que E es una cerradura algebraica de F si E es algebraica sobre F y todo polinomio $0 \neq f \in F[x]$ se escinde sobre E.

Lema: Sea $F \subseteq E$ una extensión algebraica. Son equivalentes:

(i) E es algebraicamente cerrado.

(ii) E es una cerradura algebraica de F.

(iii) No existe $L \supsetneq E$ con L algebraico sobre F.

(iv) No existe $L \supsetneq E$ con L algebraico sobre E.

Dem:

(i) $\Rightarrow$ (ii) Por hip. $E \supseteq F$ es algebraica, y por (i) todo polinomio

$f(x) \in F[x] \subseteq E[x]$ se escinde sobre E.

(ii) $\Rightarrow$ (iii) Sea $L \supseteq E$, con L algebraico sobre F. Sea $\alpha \in L$. Como L es alg. sobre F existe un polinomio $0 \neq f(x) \in F[x]$ tal que $f(\alpha) = 0$ ie $(x-\alpha) \mid f(x)$. Por (ii), $f(x)$ se descompone en factores de grado 1 sobre E.
Esto implica que $\alpha \in E$ $\therefore$ $E = L$

(iii) $\Rightarrow$ (iv) Si $L \supseteq E$ es alg. sobre E, como $E \supseteq F$ también el alg. ent $L \supseteq F$ es algebraica. Por (iii) $L = E$.

(iv) $\Rightarrow$ (i). Sea $0 \neq f \in E[x]$. Sabemos que existe un campo de descomposicion para f, $L \supseteq E$. Por ser campo de descomposicion la extension $E \subseteq L$ es algebraica. Por (iv), $E = L$.

$\therefore$ E es algebraicamente cerrado.

Cor. Sea $F \subseteq L$ y supongamos que L es algebraicamente cerrado. Sea $E = \{\alpha \in L \mid \alpha$ algebraico sobre $F\}$. Entonces E es la unica cerradura algebraica de F contenida en L.

Dem:

Claramente E es algebraico sobre F. Si $F \subseteq K \subseteq L$ tal que K sea algebraico sobre F

entonces $K \subseteq E$. Así que $F \subseteq E$ satisface la condición (iii) del lema anterior y entonces E es una cerradura algebraica de F.

Si $E_0 \supseteq F$ es otra cerradura alg. de F, ent $E_0 \supseteq F$ es algebraica. Por lo tanto $E_0 \subseteq E$.

Cor. Sea E un campo con la propiedad de que cada polinomio $f \in E[x]$ con $gr(f) \geq 1$ tiene al menos una raíz en E. Entonces E es algebraicamente cerrado.

Dem:

Sea $f \in E[x]$ con $gr(f) \geq 1$. Como no es constante, entonces f tiene un factor