Lema: Sea F un campo y $f(x) \in F[x]$. $f(x) \neq 0$

(i) Para $\alpha \in F$, $f(\alpha)=0$ si y solo si $(x-\alpha) \mid f(x)$ en $F[x]$.

(ii) Si $gr(f)=n$, entonces $f(x)$ tiene a lo más n raices en F.

Dem:

i] Sea $\alpha \in F$. Dividamos $f(x)$ entre $x-\alpha$, es decir, $f(x)=(x-\alpha)q(x)+r(x)$ con $r=0$ ó $gr(r)<1$. En cualquier caso $r(x)=r$ es constante. Por lo tanto

$f(\alpha)=(\alpha-\alpha)q(\alpha)+r=r$. $f(\alpha)=0 \iff r=0$

$\iff (x-\alpha) \mid f(x)$.

ii] Por induccion sobre $gr(f)=n$. Si $n=0$, entonces $f(x)$ es constante y por lo tanto no tiene raices.

Sup. que $gr(f)=n>0$. Si $f(x)$ no tiene raíces claramente se cumple el resultado. Sup. que $f(x)$ tiene una raíz $\alpha\in F$. Por (i) sucede que $f(x)=(x-\alpha)q(x)$ p.a. $q(x)\in F[x]$ con $gr(q(x))=n-1$. Si $\beta\in F$ es otra raíz de $f(x)$ con $\alpha\neq\beta$ ent $0=f(\beta)=(\beta-\alpha)q(\beta)$. Así $q(\beta)=0$. Por hip de ind. hay a lo más $n-1$ de estos β's tomando α tenemos a lo mas n raíces de $f(x)$.

Lema: Sea G un subgrupo finito del grupo multiplicativo $E^{\times}$ de un campo E. Entonces G es cíclico.

Dem:

Para probar que G es cíclico demostraremos que para primo p tal que $p \mid |G|$ G contiene a lo más un subgrupo de orden p. Sea $p \in \mathbb{Z}$ un primo tal que $p \mid |G|$. Entonces existe $\alpha \in G$ con $\alpha^p = 1$. Esto dice que α es raiz del polinomio $x^p - 1 \in E[x]$. Por el lema anterior hay a lo más $p-1$ elementos de orden $p \neq 1$ en $E^\times$. Por lo tanto no es posible que haya más de un subgrupo de orden p.

Por lo tanto G tiene que ser cíclico.

Def: Una extension de la forma $F \subseteq F[\alpha]$ se le llama extension simple; y al elemento α se le llama primitivo.

Teorema del elemento primitivo.

Teorema [Artin]: Sea $F \subseteq E$ una extension de campos de grado finito. Entonces E es simple si y solo si existen solo una cantidad finita de campos K tal que $F \subseteq K \subseteq E$.

Dem:

Sea $\mathcal{F} = \{K \mid F \subseteq K \subseteq E\}$, el conjunto de campos intermedios. Supongamos que $E = F[\alpha]$. Sea $f = \text{mín}_F(\alpha)$ y pongamos $\mathcal{P} = \{g \in E[x] \mid g \text{ es mónico y } g \mid f\}$.

Como $E[x]$ es un DFU, $f(x)$ tiene un número finito de divisores. Por lo tanto $\mathcal{P}$ es finito

Para ver que $\mathcal{F}$ es finita, daremos una función inyectiva

$$\begin{aligned} \mathcal{F} &\rightarrowtail \mathcal{P} \\ K &\mapsto g_K \end{aligned}$$

Sea $K \in \mathcal{F}$ y $g_K = \min_K(\alpha)$. Tenemos que $F \subseteq K$. Entonces $F[x] \subseteq K[x]$. Así que podemos considerar $f(x) = \min_F(\alpha) \in K[x]$. Como $f(\alpha) = 0$, entonces $g_K \mid f$ en $K[x]$. Como $F[x] \subseteq K[x] \subseteq E[x]$. Por lo tanto $g_K \in \mathcal{P}$.

Sean $a_0, a_1, \dots, a_r$ los coeficientes de g_K y consideremos $L = F[a_0, a_1, \dots, a_r]$.

$$\begin{array}{c} E = F[\alpha] \\ | \\ K \\ | \\ L \\ | \\ F \end{array}$$

Queremos probar que $K=L$

Tenemos que $g_K \in L[x]$. Como g_K es irreducible sobre K y $L \subseteq K$ entonces g_K es irreducible en $L[X]$. Por lo tanto

$$g_K = \min_L(\alpha)$$

Como tambien $g_K = \min_K(\alpha)$ y $K[\alpha] = E = L[\alpha]$, tenemos que:

$$[E:L] = gr(g_K) = [E:K]$$ pero $$[E:L] = [E:K][K:L]$$ lo que implica que $[K:L] = 1 = \dim_L K$ y $L \subseteq K$. Por lo tanto $K=L$. Por lo tanto la asignacion $K \mapsto g_K$ es inyectiva.

Recíprocamente, supongamos que $\mathcal{F}$ es finito. Haremos la prueba por inducción en $[E:F]$. Claramente si $[E:F]=1$, ie, $E=F$ entonces la extension $F\subseteq E$ es simple. Sup. que $F\subsetneq E$ y tomemos $\alpha\in E\setminus F$. Entonces $F\subsetneq F[\alpha]$,

$$\begin{array}{c} E \\ | \\ F[\alpha] \\ | \\ F \end{array}$$

y por lo tanto $[E:F[\alpha]]<[E:F]$ ya que $[E:F]=[E:F[\alpha]][F[\alpha]:F]$. Como el numero de campos intermedios entre E y F es finito entonces el numero de campos intermedios entre E y $F[\alpha]$ también es finito. Por hipotesis de inducción existe $\beta\in E$ tal que $E=F[\alpha][\beta]$
$=F[\alpha,\beta]$.

Ahora supongamos que $|F|$ es infinita y consideremos los campos $K_t = F[\alpha + t\beta]$ con t corriendo en los elementos de F. Como $F \subseteq K_t \subseteq E$ entonces deben de existir $s \neq t \in F$ tales que $K_t = K_s$.

Así $\alpha + s\beta \in K_s$ y $\alpha + t\beta \in K_s$ y entonces $(s-t)\beta \in K_s$. Como $F \subseteq K_s$, $s-t \in K_s$, lo que implica que $\beta \in K_s$ ya que $s-t \neq 0$. Así que $s\beta \in K_s$. Como $\alpha + s\beta \in K_s$, $\alpha \in K_s$. Por lo tanto $E = F[\alpha, \beta] \subseteq K_s \subseteq E$

$$E = K_s = F[\alpha + s\beta].$$

Ahora supongamos que $|F|<\infty$. Como ${}_F E$ tiene una base finita, digamos $\{e_1, \ldots, e_n\}$ y cada elemento $\alpha \in E$ se escribe $\alpha = \sum a_i e_i$ con $a_i \in F$, entonces solo hay un numero finito de posibilidades para los coeficientes a_i. Entonces solo hay un número finito de posibles combinaciones lineales. Por lo tanto $|E|$ es finita. Por un lema anterior $E^\times$ es un grupo ciclico generado, digamos, por $\alpha \in E^\times$. Por lo tanto $E = F[\alpha]$.

Cor. Sea $F \subseteq E$ una extension de campos con $E = F(\alpha)$ p.a. $\alpha \in E$. Supongamos que α es algebraico sobre F. Si $F \subseteq K \subseteq E$, entonces $K = F(\beta)$ p.a. $\beta \in K$.

Dem:

Sea $F \subseteq K \subseteq E$. Como α es algebraico, $[F[\alpha] : F] = [E : F] < \infty$ lo que implica que $[K : F] < \infty$. Como $F \subseteq E$ es simple, por el teorema anterior, solo hay un numero finito de campos intermedios entre E y F. En particular, solo hay un numero finito de campos intermedios entre F y K.

Por el teorema anterior la extension $F \subseteq K$ es simple i.e. $\exists \beta \in K$ tal que $K = F[\beta]$.