Cor. Sea $F \subseteq E$ una extension de grado finito. Entonces existe un campo $L \supseteq E$ tal que $[L:F] < \infty$ y $F \subseteq L$ es normal.

Def: Decimos que un polinomio $f(x) \in F[x]$ de grado n tiene raices distintas, si f tiene n raices diferentes en cada campo en el que se escinde.

Lema: Sea $0 \neq f \in F[x]$. Son equivalentes:

i) f tiene raices distintas.

ii) Si $F \subseteq K$ y $\alpha \in K$, entonces $(x-\alpha)^2$ no divide a $f(x)$ en K.

iii) Existe $K \supseteq F$ tal que f tiene $gr(f)$ raices (diferentes) en K.

Dem:

i) $\Rightarrow$ ii) Sea $K \supseteq F$ y $\alpha \in K$. Si $(x-\alpha)^2 \mid f(x)$, ent $f(x) = (x-\alpha)^2 g(x)$ con

$g(x) \in K[x]$. Remplazando K por un campo más grande, podemos suponer que $g(x)$ se escinde en K. Entonces $f(x)$ también se escinde en K, ya que $f(x) = (x-\alpha)^2 g(x)$. Por hipotesis, todas las raices de $f(x)$ en K son distintas entonces las raices de $g(x)$ tambien son distintas. Una raiz de f es α y como las demás son distintas, deben de ser raices de $g(x)$ así que no puede haber un termino $(x-\alpha)^2$ ☹

ii ⇒ iii | Sea K un campo de descomposición de $f(x)$ sobre F. Entonces $f(x)$ se escinde sobre K, es decir, $f(x) = a(x-\alpha_1)\cdots(x-\alpha_n)$ con $n = gr(f)$. Si $\alpha_1 = \alpha_2$, entonces $(x-\alpha_1)^2 \mid f(x)$, lo que no puede ser.

iii ⇒ i | Sea $K \supseteq F$ el campo en el cual f tiene $gr(f) = n$ raíces diferentes. Si $L \supseteq K$, entonces f sigue teniendo n raíces diferentes. Tenemos que ver que

$f(x)$ tiene el mismo numero de raices en cualesquiera dos extensiones L_1 y L_2 en las que se escinda. Cada raiz de f en L_i está en un campo de descomposicion E_i de $f(x)$ tal que $F \subseteq E_i \subseteq L_i$. Como E_i es campo de descomposicion de $f(x)$, entonces E_1 y E_2 son F-isomorfos. Entonces f debe tener mismo numero de raices en L_1 que L_2.

Def: Un polinomio $0 \neq f \in F[x]$ es separable sobre F si cada factor irreducible de f en $F[x]$ tiene raíces distintas.

Notemos que si un polinomio f se escinde en un campo E, entonces f es separable sobre E.

Lema: Sea $F \subseteq E$ y $f \in F[x]$ separable sobre F. Entonces f es separable sobre E.

Dem:

Sea $h \in E[x]$ un factor irreducible de $f(x)$. Por la unicidad de la factorización en irreducibles de $f(x)$ en $E[x]$, debe de existir un factor irreducible $g(x) \in F[x]$

tal que $h \mid g$. Por hipotesis todas las raices de g son distintas. Por lo tanto las raices de h tambien son distintas.

$\therefore f$ es separable sobre E.

Ejemplo: Sea K un campo de característica $p \neq 0$ y sea $F = K(y)$ el campo de fracciones de $K[y]$. Tenemos que y es un elemento primo del DFU $K[y]$. Usando el criterio de Eisenstein, tenemos que $x^p - y \in F[x]$ es irreducible. Afirmamos que $x^p - y$ no es separable. Sea α una raiz de $x^p - y$ en alguna extension $E \supseteq F$. Así $\alpha^p - y = 0$ ie, $y = \alpha^p$. Por lo tanto

$$x^p - y = x^p - \alpha^p = (x - \alpha)^p \in E[x]$$

Teorema: Sea F un campo y supongamos que $F[x]$ contiene un polinomio inseparable. Entonces F tiene que ser infinito y de característica prima.

Def: Sea $F \subseteq E$ una extension de campos. Un elemento $\alpha \in E$ algebraico sobre F es separable sobre F si $\min_F(\alpha)$ es separable sobre F. Se dice que la extension $E \supseteq F$ es separable si cada $\alpha \in E$ es separable.

Cor. Sup. que $F \subseteq K \subseteq E$ y que E es una extension separable de F. Entonces $E \supseteq K$ y $K \supseteq F$ son separables.

Dem:

Como $K \subseteq E$, la extension $F \subseteq K$ es separable.

Sea $\alpha \in E$ y consideremos $g = \min_K(\alpha)$ y $f = \min_F(\alpha)$. Como $f(\alpha) = 0$ y $F[x] \subseteq K[x]$ $g \mid f$. Como todas las raices de f son distintas, las raices de g tambien.

$K \subseteq E$ es separable.

Lema. Sea $G \leq \mathrm{Aut}(E)$ y $F = \mathrm{Fix}(G)$. Sea $\alpha \in E$ y supongamos que $\Lambda = \{\sigma(\alpha) / \sigma \in G\}$ es finito. Entonces α es algebraico sobre F. Mas aún, si $f = \min_F(\alpha)$ entonces,

$G = \mathrm{Gal}(E/F)$

$\alpha \in \Lambda$ y $f(\alpha) = 0$.

a) f tiene raices distintas

b) f se escinde sobre E.

c) Λ es el conjunto de todas las raices de f en E; y

d) $\mathrm{gr}(f) = |\Lambda|$.

Dem:

Consideremos el polinomio $p(x) \in E[x]$ dado por:

$$p(x) = \prod_{\beta \in \Lambda} (x - \beta)$$

Notemos que G solo permuta los elementos de Λ

Por lo tanto $\hat{\sigma}$ solo permuta los polinomios $(x-\beta)$, $\beta \in \Delta$. Así $\hat{\sigma}(p(x)) = p(x) \in F[x]$.

Como $\alpha \in \Delta$, entonces $p(\alpha)=0$, es decir, α es algebraico sobre F. Además, como $p(\alpha)=0$, $f \mid p$. Como todos los elementos de Δ son distintos, entonces todas las raices de f tienen que ser distintas.

Por otro lado, todo los elementos de Λ son raices de f, así que $gr(p) = |\Lambda| \leq gr(f)$

Esto implica que $f(x) = p(x)$ y $gr(f) = |\Lambda|$