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

Teorema. Sea $F \subseteq E$ una extension de grado finito. Son equivalentes:

i) E es una extensión de Galois de F.

ii) E es separable y normal.

iii) E es el campo de descomposicion sobre F para un polinomio separable en $F[x]$.

Dem:

$i \Rightarrow ii$ | Sea $\alpha \in E$ y $f = min_F(\alpha)$. Tenemos que demostrar que f tiene raices distintas y que se escinde en E. Escribimos $G = Gal(E/F)$ y $\Lambda = \{\sigma(\alpha) \mid \sigma \in G\}$.

Tenemos que todos los elementos de Λ son raices de f Esto implica que $|\Lambda| \leq gr(f) < \infty$ Por hipotesis $Fix(G) = F$ Aplicando el

el lema anterior, f tiene todas sus raices distintas y además se escinde en E.
Por lo tanto E es normal y separable sobre F.

ii ⇒ iii Como E es normal un teorema anterior, E es el campo de descomposición de un polinomio $g \in F[x]$. Sea f un factor irreducible de g. Entonces f debe tener alguna raiz $\alpha \in E$. Como E es separable entonces por hipotesis f debe de tener todas sus raices distintas. Por lo tanto g es separable.

iii ⇒ i] Supongamos que E es el campo de descomposicion sobre F de $g \in F[x]$ que es separable. Sea $G = Gal(E/F)$ y $K = Fix(G)$. Tenemos que ver que $K = F$. Haremos la prueba por inducción sobre $[E:F]$. Si $[E:F] = 1$, ent $E = F$ y $G = \{e\}$. Por lo tanto $Fix(G) = F$. Supongamos que $[E:F] > 1$. Como E está generado por las raices de g y F, debe de haber una raiz $\alpha \in E \setminus F$. Entonces $[E:F] = [E:F[\alpha]][F[\alpha]:F]$, asi que $[E:F[\alpha]] < [E:F]$. Tenemos que E sigue siendo el campo de descomposicion de $g \in F[x]$. Ademas, g es separable sobre $F[\alpha]$.

Por hipotesis de induccion la extension $F[\alpha] \subseteq E$ es de Galois, es decir,

$$F[\alpha] = Fix\left(Gal\left(E/F[\alpha]\right)\right) \supseteq Fix(G) = K$$

ya que $Gal\left(E/F[\alpha]\right) \subseteq G$.

Sea $f=\min_F(\alpha)$. Como $g(\alpha)=0$, $f|g$ entonces f se escinde en E.
Sea Ω el conjunto de raíces de f en E. Como g es separable, todas las raíces de f son distintas. Así que $|\Omega|=gr(f)$. Por un lema anterior sabemos que G actua transitivamente en Ω, es decir, Ω es una sola orbita.

Sea $h=\min_K(\alpha)$. Como $K=Fix(G)$, $G\subseteq Gal(E/K)$. Ent G permuta las raices de h en E. Como α es una de esas raices, entonces cada $\sigma(\alpha)$ también para $\sigma\in G$. Por lo tanto

todo elemento de Ω es raiz de h. Así

$$[K[\alpha]:K] = gr(h) \geq |\Omega| = gr(f) = [F[\alpha]:F].$$

Como $F \subseteq K \subseteq F[\alpha]$, $K[\alpha] = F[\alpha]$. Por lo tanto

$$[F[\alpha]:K][K:F] = [F[\alpha]:F] \leq [K[\alpha]:K] = [F[\alpha]:K]$$

Esto implica que $[K:F] = 1$ y

por lo tanto $K = F$.

Cor. Sean $F \subseteq K \subseteq E$ campos y supongamos que E es Galois sobre F.
Entonces E es Galois sobre K.

Dem:

Como $E \supseteq F$ es de Galois, E es el campo de descomposición de un polinomio separable g sobre F. Entonces g sigue siendo separable sobre K. y además E es el campo de descomposicion de g sobre K. Por lo tanto $K \subseteq E$ es de Galois.

Notemos que si $F \subseteq K \subseteq E$ con $F \subseteq E$ de Galois, la extension $F \subseteq K$ no tiene que ser Galois

Tomemos $x^3 - 2 \in \mathbb{Q}[x]$, con raices $\sqrt[3]{2}, \alpha_1$ y α_2

El campo de descomposicion del polinomio es $\mathbb{Q}[\sqrt[3]{2}, \alpha_1]$. Por el teorema anterior $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt[3]{2}, \alpha_1]$ es de Galois. Pero $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt[3]{2}]$ no es de Galois.

$$\mathcal{F} = \{K \mid F \subseteq K \subseteq E\} \underset{f = \mathrm{Fix}(\cdot)}{\overset{g = \mathrm{Gal}(E/\cdot)}{\rightleftarrows}} \{H \leq \mathrm{Gal}(E/F)\} = G$$

$$\mathcal{F}_0 = \{K \mid K = fg(K)\} \longleftrightarrow \{H \mid H = gf(H)\} = G_0$$

Si $E \supseteq F$ es de Galois y $K \in \mathcal{F}$ entonces $E \supseteq K$ es de Galois, es decir, $fg(K) = K$

Por lo tanto $\mathcal{F} = \mathcal{F}_0$.

Lema: Sea $F \subseteq E$ de grado finito. Entonces $|Gal(E/F)| < \infty$.

Dem:

Denotemos $G = Gal(E/F)$ y tomemos elementos $\alpha_i \in E$ tales que $E = F[\alpha_1, \dots, \alpha_n]$

Ser $f(x) = \prod \min_F(\alpha_i)$ y sea Ω el conjunto de raices de f en E. Entonces Ω es finito y además Ω genera a E sobre F. Por un lema anterior G se puede ver como un subgrupo $G \hookrightarrow Sym(\Omega)$. Como Ω es finito, entonces G es finito.