$F \subseteq E$

$$\begin{tikzcd} \mathcal{F} = \{K \,/\, F \subseteq K \subseteq E\} \arrow[r, bend left, "g = \mathrm{Gal}(E/\cdot)"] & \mathcal{G} = \{H \,/\, H \leq \mathrm{Gal}(E/F)\} \arrow[l, bend left, "f = \mathrm{Fix}(\cdot)"] \end{tikzcd}$$

$\underline{fg : \mathcal{F} \to \mathcal{F}}$ $\qquad$ $\underline{gf : \mathcal{G} \longrightarrow \mathcal{G}}$

$$\{K \in \mathcal{F} \,/\, fg(K) = K\} \leftrightarrow \{H \,/\, gf(H) = H\}$$

$$F \subseteq \underbrace{fg}(F)$$

Lema: Con la notación anterior, f y g definen una biyección que invierte el orden entre $\mathcal{F}_0 = \{f(H) / H \in \mathcal{G}\}$ y $\mathcal{G}_0 = \{g(K) / K \in \mathcal{F}\}$. Además:

$\mathcal{F}_0 = \{K \in \mathcal{F} / K = fg(K)\}$ y $\mathcal{G}_0 = \{H \in \mathcal{G} / H = gf(H)\}$.

Dem:

Tenemos que $\mathcal{F}_0 \subseteq \mathcal{F}$. Así $g(\mathcal{F}_0) \subseteq g(\mathcal{F}) = \mathcal{G}_0$

Sea $K \in \mathcal{F}_0$. Por un lado $K \subseteq fg(K)$.

Como $K \in \mathcal{F}_0$, $K = f(H)$ para un $H \in \mathcal{G}$.

Entonces $g(K) = gf(H) \supseteq H$. Por lo tanto

$fg(K) \subseteq f(H) = K$ $\therefore K = fg(K)$.

Analogamente, $gf(H)=H$ para todo $H\in\mathcal{G}_0$

Acabamos de ver que para $K\in\mathcal{F}_0$ se tiene que $K=f_g(K)$. Por lo tanto

$$\mathcal{F}_0\subseteq\{K \mid f_g(K)=K\}$$ pero claramente

$$\{K\in\mathcal{F} \mid f_g(K)=K\}\subseteq\mathcal{F}_0$$

De la misma manera $\mathcal{G}_0=\{H \mid gf(H)=H\}$.

Def: Sea $F \subseteq E$ una extension de campos. Decimos que la extension es de Galois si $[E:F] < \infty$ y $F = \mathrm{Fix}(\mathrm{Gal}(E/F))$.

Notemos que por el lema anterior, si $F \subseteq E$ es una extension de grado finito y $K = \mathrm{Fix}(\mathrm{Gal}(E/F))$ entonces $K \subseteq E$ es de Galois.

Lema: Sea $F \subseteq E$ y $G = \mathrm{Gal}(E/F)$. Sea $0 \neq f \in F[x]$ y $\Omega = \{\alpha \in E \mid f(\alpha) = 0\}$. Suponga que $\Omega \neq \emptyset$. Entonces:

a) La acción de G en E permuta los elementos de Ω.

b) Si los elementos de Ω generan E sobre F, entonces G se encaja en $\mathrm{Sym}(\Omega) \cong S_n$

c) Si además, f es irreducible y E es un campo de descomposición para un polinomio sobre F, entonces G actua transitivamente sobre Ω.

Dem:

a) Sea $\alpha \in \Omega$ y $\sigma \in G$. Entonces

$f(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0$ ya que $f \in F[x]$

$\therefore \sigma(\alpha) \in \Omega$

b) Es claro que como G actua en Ω entonces hay un morfismo $G \to \mathrm{Sym}(\Omega)$. Sea K el nucleo de este morfismo. Entonces $\Omega \subseteq \mathrm{Fix}(K)$. Ademas $F \subseteq \mathrm{Fix}(K)$. Por la hipotesis, esto implica que todos los elementos de K fijan a todo E. Por lo tanto K consiste solo de la identidad y así

$$G \hookrightarrow Sym(\Omega)$$

c) Sean $\alpha, \beta \in \Omega$. Como f es irreducible existe un F-isomorfismo $\varphi : F[\alpha] \to F[\beta]$ tal que $\varphi(\alpha) = \beta$. Por otro lado, como E es el campo de descomposicion de un

Polinomio $g \in F[x]$, entonces E es un campo de descomposición de g sobre $F[\alpha]$ y sobre $F[\beta]$. Además $\hat{\varphi} g = g$. Esto implica que φ se extiende a un F-isomorfismo $\sigma : E \to E$. $\therefore \sigma \in Gal(E/F)$ y $\sigma(\alpha) = \beta$

$$
\begin{tikzcd}
E \arrow[rr, dashed, "\sigma"] & & E \\
F[\alpha] \arrow[u, dash] \arrow[rr, dashed, "\varphi"] & & F[\beta] \arrow[u, dash] \\
& F \arrow[ul, dash] \arrow[ur, dash] &
\end{tikzcd}
$$

Def: Una extension algebraica $F \subseteq E$ es normal si para cada $\alpha \in E$, el polinomio minimo $\min_F(\alpha)$ se escinde sobre E.

Equivalentemente, E es normal sobre F si cada polinomio irreducible $f \in F[x]$ que tenga una raiz en E se escinde sobre E.

Ejemplos:

Si E es una cerradura algebraica de F, ent E es normal.

La extension trivial $F \subseteq F$ es normal.

Si $[E:F]=2$, $E \supseteq F$ es normal. Sea $\alpha \in E$ y consideremos $\min_F(\alpha)$. Entonces $[E:F]=[E:F[\alpha]][F[\alpha]:F]=2$

Sup $\alpha \notin F$. Entonces $E=F[\alpha]$ y así $gr(\min_F(\alpha))=2$. Ademas $(x-\alpha) \mid \min_F(\alpha)$ en E

ie, $\min_F(\alpha) = (x-\alpha)g(x)$ con $g(x) \in E[x]$. Así $gr(g(x)) = 1$ por lo tanto $\min_F(\alpha)$ se factoriza en polinomios lineales.

Lema: Sea $F \subseteq E$ una extensión de grado finito y $\alpha \in E$. Entonces existe un campo $L \supseteq E$ y un polinomio $g \in F[x]$ tal que:

a) L es e campo de descomposición para g sobre F.

b) Todo factor irreducible de g en $F[x]$ tiene una raiz en E; y

c) $g(\alpha) = 0$.

Dem:

Consideremos una base $\alpha_1, \alpha_2, \dots, \alpha_n$ de ${}_F E$. Sea g el producto de los polinomios mínimos sobre F de α y de cada α_i ie $g(x) = \prod_{i=0}^{n} \min_F(\alpha_i)$ con $\alpha_0 = \alpha$. Por lo tanto $g(\alpha) = 0$ y cada factor irreducible tien una raiz en E.

Sea L el campo descomposicion de $g(x)$ sobre E. Tenemos que probar que L está generado por F y las raices de g. Como L es campo de descomposicion sobre E, L está generado por las raices de g y E. Pero por construccion E esta generado por algunas raices de g y F. Por lo tanto L está generado por las raices de g y F.

Teorema: Sea $F \subseteq E$ una extension con $[E:F] < \infty$. Son equivalentes:

i) E es normal sobre F.

ii) E es un campo de descomposicion sobre F para algún polinomio $g \in F[x]$.

iii) Para cada extension $L \supseteq E$, todo F-isomorfismo de E en L manda a E en E.

Dem:

$i \Rightarrow ii$ Sup. que E es normal sobre F. Usando el lema anterior obtenemos un polinomio $g \in F[x]$ y un campo $L \supseteq E$ tal que L es el campo de descomposicion de g sobre F y cada factor irreducible de g tiene una raiz en E.

Como $F \subseteq E$ es normal cada factor irreducible de g, se escinde en F. Por lo tanto g se escinde en E, es decir, todas las raíces de g están en E. Como $L \supseteq E$, entonces $L = E$.

ii $\Rightarrow$ iii) Sea $\theta : E \to L$ un F-morfismo

Sup. que E es el campo de descomposición de un polinomio $g(x) \in F[x]$. Entonces $\hat{\theta} g = g$. Así que $\theta(E)$ es campo de descomposición de g sobre F. Por la unicidad, $\theta(E) = E$.

iii $\Rightarrow$ i) Sea $\alpha \in E$ y $f = min_F(\alpha)$. Usando el lema anterior existe un campo $L \supseteq E$ y $g \in F[x]$ tal que L es el campo de descomposicion de g sobre F, cada factor irreducible de g tiene una raiz en E y $g(\alpha)=0$. Como $f | g$, f se escinde en L. Por en lema anterior, para cada raiz β de f existe $\sigma \in Gal(L/F)$ tal que $\sigma(\alpha)=\beta$

Por (iii) cada raiz de f está en E. Por lo tanto, f se escinde en E. Por lo tanto $E \supseteq F$ es normal.