Sean $F \subseteq E \subseteq K$ campos y supongamos que E es Galois sobre F. Consideremos $F \subseteq L \subseteq K$ y pongamos $M = E \cap L$. Si ningún subcampo propio de K contiene a L y a E, entonces K es Galois sobre L y la restricción de automorfismos a E define un isomorfismo de $\mathrm{Gal}(K/L)$ en $\mathrm{Gal}(E/M)$. En particular $[K:L] = [E:M]$.

$$\begin{tikzcd}
 & K \arrow[dl, dash] \arrow[dr, dash, "\mathrm{Gal}(K/L)"] & \\
E \arrow[dr, dash] & & L \arrow[dl, dash] \\
 & M \arrow[d, dash] & \\
 & F &
\end{tikzcd}$$

$$\begin{tikzcd}
K \arrow[rr, "\sigma"] \arrow[dr, dash] & & K \arrow[dl, dash] \\
 & L &
\end{tikzcd}$$

Dem:

Como $E \supseteq F$ es de Galois existe un polinomio separable $f \in F[x]$ tal que E es el campo de descomposicion de f sobre F. Así f se escinde en K. Afirmamos que K es el campo de descomposicion de f sobre L. Como f se escinde K, K contiene un campo de descomposición K_0 de f sobre L. Como $E \subseteq K$ está generado por las raíces de f y $F \subseteq L$, entonces $E \subseteq K_0$. Así $E \subseteq K_0$ y $L \subseteq K_0$. Por hipotesis $K_0 = K$.

Como f es separable sobre F, f es separable sobre L. Por lo tanto $K \supseteq L$ es de Galois.

Dado cualquier automorfismo $\sigma \in Gal(K/L)$ $\sigma(E)=E$ ya que $E \supseteq F$ es normal. Como σ fija a los elementos de L, entonces la restricción fija a los elemtos de $E \cap L$. Por lo tanto tenemos un morfismo de grupos $\rho: Gal(K/L) \to \underline{Gal(E/M)}$ dado por restriccion.

Si $N = \operatorname{Ker} \rho$, entonces $E \subseteq \operatorname{Fix}(N)$.

Ademas cada $\sigma \in Gal(K/L)$ fija a L. Ent $L \subseteq \operatorname{Fix}(N)$. Por hipotesis, $\operatorname{Fix}(N) = K$

Pero el unico elemento de $Gal(K/L)$ que fija a K es la identidad $\therefore N = \{e\}$.

Sea $M_1 = \operatorname{Fix}(\rho(Gal(K/L)))$. Entonces

$M = \operatorname{Fix}(Gal(E/M)) \subseteq M_1$. Cada automorfismo $\sigma \in Gal(K/L)$ fija a los elementos de M_1. Así $M_1 \subseteq Fix(Gal(K/L))$ i.e, $M_1 \subseteq L$. Como tambien $M_1 \subseteq E$ $M_1 \subseteq M$. Por lo tanto $M_1 = M$. Así

$$Fix(\rho(Gal(K/L))) = Fix(Gal(E/M))$$

Por el T.F.G., $\rho(Gal(K/L)) = Gal(E/M)$

$\therefore \rho$ es un isomorfismo.

y por último:

$$[E:M] = |Gal(E/M)| = |Gal(K/L)| = [K:L].$$

Cor. En la situación del teorema anterior, supongamos que $[K:F]<\infty$. Ent $[K:E]=[L:M]$.

Dem:

$$\begin{tikzcd}[column sep=small]
 & K \arrow[dl, dash] \arrow[dr, dash] & \\
E \arrow[dr, dash] & & L \arrow[dl, dash] \\
 & M \arrow[d, dash] & \\
 & F &
\end{tikzcd}$$

$$[K:M]=[K:E][E:M]$$

$$[K:E]=[K:M]/[E:M]=\frac{[K:M]}{[K:L]}$$

$$=[L:M].$$

Campos Ciclotómicos y construcciones geométricas

Def: Un elemento $\xi \in F$ es una raíz n-esima de la unidad si $\xi^n = 1$. Decimos que ξ es primitiva si $\xi^m \neq 1$ para $1 \leq m < n$.

Lema: Sea F un campo y $n \geq 1$. El conjunto de raices n-esimas de la unidad en F forman un subgrupo ciclico de F^* de orden un divisor de n. El numero de raices n-esimas de la unidad en F es exactamente n si y solo si F contiene una raíz n-esima primitiva de la unidad.

Def:

El conjunto $C \subseteq F$ de raices n-esimas de la unidad es justamente el conjunto de raices del polinomio $X^n - 1$. Por lo tanto es finito. Tenemos $C \subseteq F^*$ es un subgrupo y entonces es cíclico. Escribimos $|C| = m$ y $C = \langle \xi \rangle$. Así $m = o(\xi)$. Como $\xi^n = 1$, $m \mid n$. Si $m = n$, ξ es un raíz n-ésima primitiva. Recíprocamente, si F contiene una raíz n-ésima primitiva δ, ent $\delta \in C$ y así $\delta^m = 1$. Por lo tanto $o(\delta) = n \leq m$ y así $n = m$.

Cor. Sup. que $\xi \in F$ es una raíz n-ésima primitiva de la unidad.

a) Los elementos ξ^k para $0 \leq k < n$ son distintos y son todas las raíces n-ésimas de la unidad en F.

b) Los elementos ξ^k con $0 \leq k < n$ y $mcd(k,n)=1$ son todas las raices n-esimas primitivas de la unidad en F.

c) F contiene prescisamente $\varphi(n)$ raices n-esimas primitivas de la unidad, donde φ es la Funcion de Euler.

Lema: Un campo F tiene una extension que contiene una raiz n-esima primitiva de la unidad si y solo si $car(F)$ no divide a n. Si $E \supseteq F$ y $\xi \in E$ es una raíz n-esima primitiva de la unidad, entonces $F[\xi]$ es el campo de descomposicion de $X^n - 1$ sobre F. En particular $F[\xi]$ queda totalmente determinada (hasta F-isomorfismo) por F y n.

Dem:

Sup. $car(F) \mid n$. La $car(F) = p$ es un

numero primo y podemos escribir $n=pm$.
Entonces $X^n-1 = X^{pm}-1^p = (X^m-1)^p$ y así
este polinomio solo tiene a lo más $m<n$
raices distintas. Por lo tanto ninguna
extension puede contener una raiz n-esima
primitiva de la unidad.
Si $car(F) \nmid n$, entonces 0 es la unica raiz
de la derivada f' de $f(x)=x^n-1$ y así
$f(x)$ tiene raices distintas. Si E es el

campo de descomposición de $f(x)$ sobre F contiene n raices n-esimas de la unidad distintas, por lo tanto contiene una raiz n-esima primitiva

Si $F \subseteq E$ y $\xi \in E$ es una raiz n-esima primitiva de la unidad, entonces $F[\xi]$ contiene n raices n-esimas de la unidad y así $f(x)$ tiene sus raices en $F[\xi]$ y por lo tanto se escinde. Como ξ es una de las raices de $f(x)$. $F[\xi]$ debe de ser el campo de descomposicion de $f(x)$.

Si ξ es una raíz n-esima de la unidad en $\mathbb{C}$, entonces $|\xi|^n = |\xi^n| = |1|$ $= 1$. Así $|\xi| = 1$ y por lo tanto las raíces n-esimas de la unidad están en el circulo unitario. De hecho el Teorema de de Moivre dice que las raíces n-esimas de la unidad son de la forma

$$e^{\frac{2\pi i k}{n}} = \cos\frac{2\pi k}{n} + i \operatorname{sen}\frac{2\pi k}{n} \quad 0 \leq k < n$$

Vemos que $e^{\frac{2\pi i}{n}}$ es una raíz n-esima primitiva de la unidad.