Restando a la primera la segunda obtenemos

$$\sum_{j=2}^{m} a_{i_j}(T_{i_j}(c) - T_{i_1}(c))T_{i_j}(x) = 0 \text{ para todo } x \in K.$$

Como $a_{i_m}(T_{i_m}(c) - T_{i_1}(c)) \neq 0$, entonces tenemos un número en L más pequeño que m, lo cual no es posible. $\square$

Auxiliados con este resultado obtenemos:

6.1 Teorema. Sean $F \leq K$, si $[K : F] < \infty$, entonces $|G(K, F)| \leq [K : F]$.

Demostración. Sean $a_1, \cdots, a_n \in K$ una base de ${}_F K$, y supongamos que existen $T_1, \cdots, T_{n+1} \in G(K, F)$ diferentes. formamos el siguiente sistema lineal homogeneo de $n \times (n + 1)$, el cual es indeterminado:

$$\begin{array}{llllll}
T_1(a_1)x_1 & + & T_2(a_1)x_2 & + \cdots + & T_{n+1}(a_1)x_{n+1} & = 0 \\
T_1(a_2)x_1 & + & T_2(a_2)x_2 & + \cdots + & T_{n+1}(a_2)x_{n+1} & = 0 \\
. & & & & & \\
. & & & & & \\
. & & & & & \\
T_1(a_n)x_1 & + & T_2(a_n)x_2 & + \cdots + & T_{n+1}(a_n)x_{n+1} & = 0
\end{array}$$

Así que existe una solución no trivial es decir existen $x_1, \cdots, x_{n+1}$ no todos cero tal que

$$\sum_{i=1}^{n+1} T_i(a_j)x_i = 0 \text{ para todo } J \in \{1, \cdots, n\}$$

Ahora sea $\alpha \in K$, entonces $\alpha = \sum_{j=1}^{n} b_j a_j$ con $b_j \in F$. Entonces

$\sum_{i=1}^{n+1} x_i T_i(\alpha) = \sum_{i=1}^{n+1} x_i(\sum_{j=1}^{n} T_i(b_j a_j)) = \sum_{i=1}^{n+1} \sum_{j=1}^{n} x_i b_j T_i(a_j) = \sum_{j=1}^{n} b_j(\sum_{i=1}^{n+1} x_i T_i(a_j)) = 0$.

Pero esto contradice el Lema 6.2 $\square$

Vamos a concentrarnos es ciertos tipos de extensión.

6.1 Definición. Sea $F \leq K$, diremos que K es una extensión normal sobre F, si
(1) $[K : F] < \infty$
(2) $K_{G(K,F)} = F$

Veamos la siguiente proposición técnica:

6.1 Proposición. Sea $a \in K$ y $H = \{T_1, \cdots, T_n\}$ subgrupo de $G(K, F)$, si $\alpha_1 = \sum_{i=1}^{n} T_i(a)$, $\alpha_2 = \sum_{i<j} T_i(a)T_j(a)$, ..., $\alpha_n = \prod_{i=1}^{n} T_i(a)$, entonces
(a) $\alpha_i \in K_H$ para toda i,
(b) $p(x) = \prod_{i=1}^{n}(x - T_i(a)) \in K_H[x]$, con únicas raices el conjunto A.

Demostración. (a) Si $A = \{T_1(a), \cdots, T_n(a)\}$ cada α_j es la suma de los productos de j elementos de A sin repetición en sus indices. Notemos que $\{T_i \circ T_j : j \in \{1, \cdots, n\} = H$ para todo i, entonces $T_i(\alpha_1) = \alpha_1$. En general, asociamos a cada l-ada $(j_1, \cdots, j_l)$, de elementos en $\{1, \cdots, n\}$ sin repetición la l-ada $\theta_i((j_1, \cdots, j_l)) = (r_1, \cdots, r_l)$ donde $T_{r_s} = T_i \circ T_{j_s}$, como son automorfismo no hay repetición, por otro lado esta relación es función y ademas es inyectiva ya que si $\theta_i((j_1, \cdots, j_l)) = \theta_i((m_1, \cdots, m_l))$, con $(j_1, \cdots, j_l) \neq (m_1, \cdots, m_l)$, entonces existe $j_{n_0} \neq m_{n_0}$, pero $T_{r_{n_0}} = T_i \circ T_{j_{n_0}} = T_i \circ T_{m_{n_0}}$, luego $T_{j_{n_0}} = T_{m_{n_0}}$, lo cual no es posible, así que θ_i es biyectiva. Así que $T_i(T_{j_1}(a) \dots T_{j_l}(a)) = T_i \circ T_{j_i}(a) \dots T_i \circ T_{j_l}(a)$ y correspondera a uno y sólo un sumando de α_l y de esta manera serán todos los sumandos de α_l, por tanto $T_i(\alpha_l) = \alpha_l$. Por tanto $\alpha_j \in K_H$.

(b) Para este caso, bastará usar las formúlas de Vieta y convencerse que

$$p(x) = \prod_{i=1}^{n}(x - T_i(a)) = x^n - \alpha_1 x + \cdot + (-1)^n \alpha_n$$

□

Ahora veremos un teorema fundamental:

6.2 Teorema. Si K es una extensión normal sobre F y H subgrupo de $G(K, F)$, entonces:

(1) $[K : K_H] = |H|$

(2) $H = G(K, K_H)$

(3) En particular, cuando $H = G(K, F)$, tenemos que $[K : F] = |G(K, F)|$

Demostración. Sea $H \leq G(K, F)$, pero $|G(K, K_H)| \leq [K : K_H]$ (ver Teorema 6.1), como para $T \in H$ y $z \in K_H$, s ecumple que $T(z) = z$, entonces $H \leq G(K, K_H)$, entonces $|H| \leq |G(K, K_H)| \leq [K : K_H]$. Demostaremos que $[K : K_H] = |H|$ lo cual demostrará (2) y (3) es sólo un caso particular de (2).

Como $[K : F] < \infty$, y como $F \leq K_H \leq K$, tenemos que $[K : K_H] < \infty$. Por el Corolario 5.2, existe $a \in K$ tal que $K = K_H(a)$, sea $H = \{T_1, \cdots, T_n\}$, el polinomio (ver Proposición 6.1)

$$p(x) = \prod_{i=1}^{n}(x - T_i(a)) \in K_H[x]$$

Pero $[K : K_H] = [K_H(a) : K_H] = gr(m(x))$, donde $m(x)$ es el polinomio de grado mínimo en en $K_H[x]$ tal que $m(a) = 0$, así que $gr(m(x)) \leq gr(p(x)) = |H|$. □

Veamos finalmente una caracterización de la s extensiones normales.

6.3 Teorema. es una extensión normal sobre F si y sólo si K es el campo de descomposición de de un polinomio en $F[x]$.

Demostración. Asumamos que K es normal sobre F, $K = F(a)$ para algún $a \in K$. Denotamos $G(K,F) = \{T_1, \cdots, T_n\}$, nuevamente

$$p(x) = \prod_{i=1}^{n}(x - T_i(a)) \in K_{G(K,F)}[x] = F[x].$$

Así que K tiene todas las raices de $p(x)$, las cuales son $\{T_1(a), \cdots, T_n(a)\}$ pero además a es raíz de $p(x)$, si $F \leq M \leq K = F(a)$ y en M están todas las raices de $p(x)$, entonces $a \in M$, entonces $M = F(a)$. Por tanto K es el campo de descomposición de $p(x) \in F[x]$.

Ahora supongamos que K es el campo de descomposición de algún polinomio $f(x) \in F[x]$. Haremos inducción sobre $[K : F]$. Si $[K : F] = 1$, es claro que K es normal sobre F. Ahora ~~entonces (K,T)~~ veamos el caso en que $f(x)$ tiene una factorización en factores lineales o tiene un factor irreducible de grado mayor que 1. En el primer caso entonces nuevamente $K = F$, veamos el segundo caso y sea $q(x) \in F[x]$ factor irreducible. sabemos que todas sus raices se encuentran en K y además son diferentes. Sean $\{b_1, \cdots, b_r\}$ todas raices diferentes de $q(x)$. Tomamos $[K : F(b_1)] = r = gr(q(x)) > 1$, además K es nuevamente campo de descomposición de $f(x) \in F(b_1)[x]$, cualquier campo $F(b_1) \leq M \leq K$ que contenga todas las raices de $f(x)$ debe ser K, ya que K es campo de descomposición de $f(x) \in F[x]$. Además

$$[K : F(b_1)] = \frac{[K : F]}{[F(b_1) : F]} = \frac{n}{r} < n.$$

Por hipótesis inductiva tenemos que K es normal sobre $F(b_1)$. Sea $z \in K_{G(K,F)}$, queremos demostrar que $z \in F$. Pero si $\tau \in G(K, F(b_1)) \subseteq G(K,F)$, entonces $\tau(z) = z$, entonces $z \in F(b_1)$. Así que (ver Teorema 1.1)

$$z = \sum_{i=0}^{r-1} c_i b_1^i \text{ con } c_i \in F.(*)$$

Como $f(x) \in F(b_1)[x]$ y K campo de descomposición de $f(x)$, sea $\gamma : F(b_1) \to F(b_i)$ isomorfismo tal que $\gamma(b_1) = b_i$, entonces para todo $j \in \{1, \cdots, r\}$, existe T_j, un automorfismo de K tal que $T_j(in(z)) = in \circ \gamma(z)$ para todo $z \in F(b_1)$, en particular $T_j(b_1) = \gamma(b_1) = b_i$ (ver Teorema 3.2 y Teorema 4.2). Ahora bien aplicando T_i a $(*)$, obtenemos:

$$z = \sum_{i=0}^{r-1} c_i b_j^i$$

Entonces el polinomio $l(x) = c_{r-1}x^{r-1} + \cdots + c_1 x + (c_0 - z)$, tiene como raices a $b_1, \cdots, b_r$, lo cual solo es posible si $l(x) = 0$, entonces $c_0 - z = 0$, entonces $z = c_0 \in F$. $\square$