

Tema 9.- Homomorfismos de cuerpos. Extensiones normales. Teorema fundamental de la teoría de Galois.

9.1. Caracteres de un grupo.

A la hora de resolver una ecuación $f(X) = 0$ con $f(X) \in k[X]$, tomamos un cuerpo de descomposición K de $f(X)$ sobre k , donde están todas las raíces, y consideramos el grupo $\text{Aut}(K)$. Vamos a estudiar dos relaciones:

1. A cada cuerpo $L, k \subset L \subset K$ le hacemos corresponder el subgrupo de $\text{Aut}(K)$ formado por los automorfismos de K que dejan invariante a L .
2. Dado un subconjunto C de $\text{Aut}(K)$, consideramos el conjunto de elementos de K que permanecen fijos por la acción de los automorfismos de C .

Vamos a estudiar primero la segunda relación.

DEFINICIÓN 9.1.1.— Si K es un cuerpo y $C \subset \text{Aut}(K)$ un subconjunto, representamos por $F(C)$ al conjunto de puntos fijos por C , es decir

$$F(C) = \{x \in K \mid \sigma(x) = x, \forall \sigma \in C\}$$

Otra notación muy utilizada para este conjunto es K^C .

NOTA 9.1.2.— Es evidente que $F(C)$ es un subcuerpo de K y que si $C_1 \subset C_2$ entonces $F(C_1) \supset F(C_2)$.

Queremos estudiar la relación entre $[K : F(C)]$ y $\#C$, el número de elementos de C . Probaremos que $[K : F(C)] \geq \#C$, y para ello nos hacen falta los caracteres de un grupo.

DEFINICIÓN 9.1.3.— Sea G un grupo y k un cuerpo. Se llama *carácter* de G sobre k a un homomorfismo σ de grupos $\sigma : G \rightarrow k^*$, donde $k^* = k \setminus \{0\}$ es el grupo multiplicativo del cuerpo k .

DEFINICIÓN 9.1.4.— Los caracteres $\{\sigma_1, \dots, \sigma_n\}$ de un grupo G sobre k se dicen *dependientes*, si existen $a_1, \dots, a_n \in k$ no todos nulos, tales que

$$a_1\sigma_1(g) + \dots + a_n\sigma_n(g) = 0$$

para todo $g \in G$. En otro caso se dicen *independientes*.

TEOREMA 9.1.5.— *Teorema de independencia de caracteres.* (Dedekind) Si G es un grupo, k es un cuerpo y $\{\sigma_1, \dots, \sigma_n\}$ son caracteres distintos de G sobre k , entonces estos caracteres son independientes.

COROLARIO 9.1.6.— Sea K un cuerpo y $\psi_1, \dots, \psi_n$ distintos automorfismos de K . Entonces $\psi_1, \dots, \psi_n$ son caracteres independientes del grupo K^* sobre K , es decir no hay una combinación lineal no trivial con coeficientes en K de los automorfismos dados.

PROPOSICIÓN 9.1.7.— Si K es un cuerpo y $C \subset \text{Aut}(K)$ es un subconjunto finito, entonces

$$[K : F(C)] \geq \#C$$

Demostración. Sea $C = \{\psi_1, \dots, \psi_n\}$. Supongamos que $[K : F(C)] = r < n$. Sea $w_1, \dots, w_r$ una base de K sobre $F(C)$, y consideremos el sistema lineal homogéneo

$$\begin{aligned} \psi_1(w_1)x_1 + \dots + \psi_n(w_1)x_n &= 0 \\ \psi_1(w_2)x_1 + \dots + \psi_n(w_2)x_n &= 0 \\ &\vdots \\ \psi_1(w_r)x_1 + \dots + \psi_n(w_r)x_n &= 0. \end{aligned}$$

de r ecuaciones y n incógnitas. Sabemos que tiene una solución no trivial $a_1, \dots, a_n \in K$. Sea $\alpha \in K$. Podemos encontrar $b_1, \dots, b_r \in F(C)$ tales que

$$\alpha = b_1w_1 + \dots + b_rw_r.$$

Entonces

$$\begin{aligned} a_1\psi_1(\alpha) + a_2\psi_2(\alpha) + \dots + a_n\psi_n(\alpha) &= \\ \sum_{i=1}^n a_i\psi_i(\sum_{j=1}^r b_jw_j) &= \\ \sum_{i=1}^n \sum_{j=1}^r a_i\psi_i(b_j)\psi_i(w_j) &= \\ \sum_{j=1}^r \psi_i(b_j)(\sum_{i=1}^n a_i\psi_i(w_j)) &= \\ \sum_{j=1}^r b_j(\sum_{i=1}^n a_i\psi_i(w_j)) &= 0 \end{aligned}$$

porque cada b_j está en el cuerpo fijo de las ψ_i y $\sum_{i=1}^n a_i\psi_i(w_j) = 0$ para cada j . Pero esto contradice la independencia lineal de $\psi_1, \dots, \psi_n$, de donde $n \leq r$. $\square$

DEFINICIÓN 9.1.8.— Si $K|k$ es una extensión, representamos por $\text{Gal}(K|k)$ al conjunto de automorfismos de K que dejan fijos a todos los elementos de k .

NOTA 9.1.9.— Los siguientes hechos son muy fáciles:

1. $\text{Gal}(K|k)$ es un subgrupo del grupo $\text{Aut}(K)$, que llamaremos *grupo de Galois* de la extensión.
2. $F(\text{Gal}(K|k)) \supset k$.
3. Si $K|k_1|k_2$, entonces $\text{Gal}(K|k_1) \subset \text{Gal}(K|k_2)$ es un subgrupo.
4. Si $C \subset \text{Aut}(K)$ es un subconjunto entonces $\text{Gal}(K|F(C)) \supset C$.

9.2. Extensiones normales.

Vamos a mejorar la proposición anterior, estableciendo una igualdad donde se tenía sólo una desigualdad. Además, hemos definido dos construcciones: un grupo $\text{Gal}(K|k)$ a partir de una extensión $K|k$ y una extensión $K|F(G)$ a partir de un grupo G . La nota anterior, punto 2, indica que, en general, no es una construcción la inversa de la otra, ya que 'extensión' $\rightarrow$ 'grupo' $\rightarrow$ 'extensión' no es la identidad, sin embargo el teorema siguiente demuestra que en el sentido 'grupo' $\rightarrow$ 'extensión' $\rightarrow$ 'grupo' sí se obtiene la identidad.

TEOREMA 9.2.1.— (*Artin*). Si K es un cuerpo y $G \subset \text{Aut}(K)$ es un subgrupo finito, entonces:

$$[K : F(G)] = |G|.$$

Demostración. Sea $G = \{id = \sigma_1, \sigma_2, \dots, \sigma_n\}$. Por el teorema anterior, $[K : F(G)] \geq |G| = n$. Supongamos que existen $v_1, \dots, v_{n+1}$ elementos en K linealmente independientes sobre $F(G)$. Consideremos el sistema lineal homogéneo

$$\begin{aligned} x_1\sigma_1(v_1) + \dots + x_{n+1}\sigma_1(v_{n+1}) &= 0 \\ x_1\sigma_2(v_1) + \dots + x_{n+1}\sigma_2(v_{n+1}) &= 0 \\ \vdots & \\ x_1\sigma_n(v_1) + \dots + x_{n+1}\sigma_n(v_{n+1}) &= 0 \end{aligned}$$

de n ecuaciones y $n+1$ incógnitas. Tiene soluciones no triviales $(z_1, \dots, z_{n+1}) \in K^{n+1}$. Si todos los z_i pertenecieran a $F(G)$, entonces la primera ecuación del sistema implicaría que $v_1, \dots, v_{n+1}$ son linealmente dependientes sobre $F(G)$ (recordemos que $\sigma_1 = id$).

De entre todas estas soluciones, escojamos una con un número r mínimo de elementos z_i no nulos. Reordenamos las incógnitas si fuera necesario, y podemos suponer que es

$$(\beta_1, \dots, \beta_r, 0, \dots, 0) \in K^{n+1}$$

y si dividimos por β_r podemos suponer que $\beta_r = 1$. Hemos visto que al menos uno de los elementos $\beta_1, \dots, \beta_{r-1}, 1$ no está en $F(G)$ (lo que prueba en particular que $r > 1$). Pongamos, sin pérdida de generalidad, que es β_1 . Existe un $k_0 \in \{1, \dots, n\}$ tal que $\sigma_{k_0}(\beta_1) \neq \beta_1$. El sistema de ecuaciones queda

$$\begin{aligned} \beta_1\sigma_1(v_1) + \dots + \beta_{r-1}\sigma_1(v_{r-1}) + \sigma_1(v_r) &= 0 \\ \beta_1\sigma_2(v_1) + \dots + \beta_{r-1}\sigma_2(v_{r-1}) + \sigma_2(v_r) &= 0 \\ \vdots & \\ \beta_1\sigma_n(v_1) + \dots + \beta_{r-1}\sigma_n(v_{r-1}) + \sigma_n(v_r) &= 0. \end{aligned}$$

Aplicamos el automorfismo σ_{k_0} a las ecuaciones anteriores, y nos da

$$(\sigma_{k_0}\sigma_j)(v_1)\sigma_{k_0}(\beta_1) + \dots + (\sigma_{k_0}\sigma_j)(v_{r-1})\sigma_{k_0}(\beta_{r-1}) + (\sigma_{k_0}\sigma_j)(v_r) = 0$$

para cada $j = 1, \dots, n$.

Pero los elementos

$$\sigma_{k_0}\sigma_1, \sigma_{k_0}\sigma_2, \dots, \sigma_{k_0}\sigma_n$$

son los mismos que los elementos

$$\sigma_1, \sigma_2, \dots, \sigma_n$$

en otro orden, porque G es un grupo. Si definimos el índice i por $\sigma_{k_0}\sigma_j = \sigma_i$ entonces i y j recorren el conjunto $\{1, 2, \dots, n\}$ y las ecuaciones anteriores se pueden escribir

$$\sigma_i(v_1)\sigma_{k_0}(\beta_1) + \dots + \sigma_i(v_{r-1})\sigma_{k_0}(\beta_{r-1}) + \sigma_{k_0}(v_r) = 0$$

con $i = 1, \dots, n$. Si ahora restamos estas ecuaciones de las originales obtenemos las igualdades

$$\sigma_i(v_1)(\beta_1 - \sigma_{k_0}(\beta_1)) + \dots + \sigma_i(v_{r-1})(\beta_{r-1} - \sigma_{k_0}(\beta_{r-1})) = 0.$$

Pero entonces tenemos una solución no trivial del sistema de partida, porque $\beta_1 - \sigma_{k_0}(\beta_1) \neq 0$ (por la elección de k_0), y con menor número de elementos no nulos que la de las β_i . Esto es una contradicción y tenemos que $[K : F(G)] = |G|$. $\square$

COROLARIO 9.2.2.— Sea $K|k$ una extensión finita. Entonces

$$|\text{Gal}(K|k)| \leq [K : k]$$

y la igualdad se tiene si y solamente si k es el cuerpo fijo de $\text{Gal}(K|k)$.

Demostración. Sea F_1 el cuerpo fijo de $\text{Gal}(K|k)$. Entonces

$$k \subset F_1 \subset K.$$

Por el teorema anterior, $[K : F_1] = |\text{Gal}(K|k)|$. Entonces

$$[K : k] = |\text{Gal}(K|k)|[F_1 : k],$$

que prueba el corolario. $\square$

COROLARIO 9.2.3.— Sea G un subgrupo finito de $\text{Aut}(K)$. Entonces $G = \text{Gal}(K|F(G))$, es decir, todo automorfismo de K que deje fijo a $F(G)$ está en G .

Demostración. Siempre tenemos que $G \subset \text{Gal}(K|F(G))$. Sea $G = \{\sigma_1, \dots, \sigma_n\}$. Si existe $\sigma \in \text{Gal}(K|F(G))$ que no está en G , sea F_0 el cuerpo fijo de $G \cup \{\sigma\}$. Tenemos que $F(G) \subset F_0$, porque si $z \in F(G)$ entonces $\sigma_i(z) = z$, por definición y $\sigma(z) = z$ por hipótesis. Por la proposición 9.1.7, $[K : F_0] \geq n + 1$, y por el teorema anterior $[K : F(G)] = n$, lo cual es imposible, por la fórmula de los grados. $\square$

COROLARIO 9.2.4.— Si G_1 y G_2 son subgrupos finitos de $\text{Aut}(K)$, entonces $F(G_1) = F(G_2)$ implica que $G_1 = G_2$.

Demostración. Si $F(G_1) = F(G_2)$ entonces $F(G_1)$ es fijo por G_2 . Por el corolario anterior, todo automorfismo que deje fijo $F(G_1)$ está en G_1 , luego $G_2 \subset G_1$. La otra inclusión es simétrica. $\square$

DEFINICIÓN 9.2.5.— Una extensión $K|k$ se dice *normal* o *de Galois* si es finita y

$$F(\text{Gal}(K|k)) = k.$$

EJEMPLO 9.2.6.—

1. $\mathbb{Q}[\sqrt{2}]|\mathbb{Q}$ es una extensión normal, en la que $\text{Gal}(\mathbb{Q}[\sqrt{2}]|\mathbb{Q})$ tiene dos elementos, la identidad y el $\mathbb{Q}$ -automorfismo que permuta $\sqrt{2}$ y $-\sqrt{2}$.
2. $\mathbb{Q}[\sqrt[3]{2}]|\mathbb{Q}$ no es una extensión normal, porque $\text{Gal}(\mathbb{Q}[\sqrt[3]{2}]|\mathbb{Q})$ se reduce a la identidad.

DEFINICIÓN 9.2.7.— Un polinomio irreducible $f(X) \in k[X]$ se dice *separable* si no tiene raíces múltiples en cualquier cuerpo de descomposición sobre k . Un polinomio cualquiera se dice *separable* si todos sus factores irreducibles en $k[X]$ lo son.

PROPOSICIÓN 9.2.8.— Un polinomio $f(X) \in k[X]$ tiene una raíz múltiple α si y sólo si α es raíz de su derivada $f'(X)$. en particular, $f(X)$ irreducible es separable si y sólo si tal que $\text{mcd}(f, f') = 1$.

Como consecuencia, todos los polinomios en $\mathbb{Q}[X]$ son separables. Para encontrar ejemplos no separables debemos buscar en cuerpos más 'raros'. Por ejemplo, sea $k = \mathbb{Z}/\mathbb{Z}2(Y)$, donde Y es una indeterminada, entonces $f(X) = X^2 - Y \in k[X]$ es irreducible y no es separable sobre k .

LEMA 9.2.9.— Sea $K|k$ normal y $\alpha \in K$. Entonces el polinomio mínimo de α sobre k es separable y tiene todas sus raíces en K .

Demostración. Como $K|k$ es finita, sea $f(X) \in k[X]$ el polinomio mínimo de α sobre k . Sean $\{\alpha_1, \dots, \alpha_n\}$ los distintos elementos que aparecen en $\{\sigma(\alpha), \forall \sigma \in \text{Gal}(K|k)\}$. Se tiene que $\sigma(\alpha_i) = \alpha_j$, para cada $\sigma \in \text{Gal}(K|k)$. Por tanto el polinomio $p(X) = (X - \alpha_1) \cdots (X - \alpha_n)$ está en $F(\text{Gal}(K|k))[X]$, que es $k[X]$ por la normalidad de $K|k$. Como $p(\alpha) = 0$, $f|p$, por lo que f tiene todas sus raíces distintas, y están en $\{\alpha_1, \dots, \alpha_n\} \subset K$. $\square$

TEOREMA 9.2.10.— *Caracterización de extensiones normales.* Una extensión $K|k$ es normal si y sólo si K es el cuerpo de descomposición de un polinomio separable de $f \in k[X]$. En ese caso diremos que $\text{Gal}(K|k)$ es el *grupo de Galois de f sobre k* .

Demostración. Supongamos $K|k$ normal. Por ser finita,

$$K = k(\alpha_1, \dots, \alpha_m).$$

Sean $f_i \in k[X]$ los polinomios mínimos de cada α_i , para $i = 1, \dots, m$. Por el lema anterior K es el cuerpo de descomposición de $\prod_{i=1}^m f_i \in k[X]$, que es separable.

Recíprocamente, sea K el cuerpo de descomposición de $f(X) \in k[X]$ separable. Por tanto $K|k$ es finita.

Si todas las raíces de $f(X)$ están en k , entonces $K = k$, $\text{Gal}(K|k) = \{1\}$ y $F(\text{Gal}(K|k)) = K = k$.

Supongamos que $f(X)$ tiene $n \geq 1$ raíces en $K \setminus k$ y establecemos por inducción que el resultado es cierto para todos los pares de cuerpos y polinomios separables con menos de n raíces fuera del subcuerpo. Sea $f(X) = p_1(X) \dots p_r(X)$ la descomposición en factores irreducibles en $k[X]$. Supongamos que $\text{grado}(p_1(X)) = s > 1$. Sea $\alpha_1 \in K$ una raíz de $p_1(X)$, por lo que $[k(\alpha_1) : k] = s$. Se considera $f(X) \in k(\alpha_1)[X]$ y K como cuerpo de descomposición de $f(X)$ sobre $k(\alpha_1)$. Como $p_1(X)$ es separable sus raíces $\alpha_1, \dots, \alpha_s \in K$ son todas distintas. Por el carácter indistinguible de las raíces, existen isomorfismos $\sigma_i : k(\alpha_1) \rightarrow k(\alpha_i)$, para $i = 1, \dots, s$, con $\sigma_i|_k = \text{id}$. Por el teorema de unicidad de cuerpos de descomposición, como K es un cuerpo de descomposición de f sobre $k(\alpha_i)$, para $i = 1, \dots, s$, entonces cada σ_i se extiende a un automorfismo de K , que seguimos denotando igual, que está en $\text{Gal}(K|k)$.

Para probar que $K|k$ es normal, sea $z \in F(\text{Gal}(K|k))$, y por la nota 9.1.9, $z \in F(\text{Gal}(K|k(\alpha_1)))$. Por la hipótesis de inducción $K|k(\alpha_1)$ es normal y $z \in k(\alpha_1)$. Luego

$$z = c_0 + c_1\alpha_1 + \dots + c_{s-1}\alpha_1^{s-1}$$

con $c_j \in k$, para $j = 1, \dots, s-1$. Aplicando σ_i , para $i = 1, \dots, s$ nos queda

$$z = \sigma_i(z) = c_0 + c_1\alpha_i + \dots + c_{s-1}\alpha_i^{s-1}.$$

Luego el polinomio $(c_0 - z) + c_1X + \dots + c_{s-1}X^{s-1} \in K[X]$ tiene grado $\leq s-1$ y s raíces distintas $\alpha_1, \dots, \alpha_s$. Entonces es 0 y $z = c_0 \in k$. $\square$

COROLARIO 9.2.11.— Sea $K|k$ extensión normal y $k \subset L \subset K$. Entonces $K|L$ es normal.

Demostración. Si K es el cuerpo de descomposición de un polinomio separable $f(X) \in k[X]$, entonces podemos ver $f(X) \in L[X]$ para cualquier subcuerpo L de K que contenga a k . Por tanto, la extensión $K|L$ es de Galois. $\square$

9.3. Teorema fundamental de la teoría de Galois.

DEFINICIÓN 9.3.1.— Sea $f(X) \in k[X]$ separable y K su cuerpo de descomposición sobre k . Entonces el grupo

$$G_f = \{\sigma \in \text{Aut}(K) : \sigma|_k = \text{id}\}$$

se llama grupo de la ecuación $f(X) = 0$ o del polinomio $f(X)$.

TEOREMA 9.3.2.— *Teorema Fundamental de la Teoría de Galois.* Sea $f(X) \in k[X]$ un polinomio separable, K su cuerpo de descomposición sobre k y G el grupo del polinomio

$f(X)$. Sean $\mathcal{G}$ el conjunto de subgrupos de G y $\mathcal{F}$ el conjunto de subcuerpos intermedios entre k y K . Sean las aplicaciones

$$\begin{aligned}\Phi: \mathcal{F} &\longrightarrow \mathcal{G} \\ L &\longmapsto \text{Gal}(K|L)\end{aligned}$$

y

$$\begin{aligned}\Psi: \mathcal{G} &\longrightarrow \mathcal{F} \\ H &\longmapsto F(H)\end{aligned}$$

Se verifica

1. Φ y Ψ están bien definidas, son una la inversa de la otra e invierten las inclusiones.
2. Para cada $H_1 \subset H_2 \in \mathcal{G}$ se tiene

$$\frac{|H_2|}{|H_1|} = [F(H_1) : F(H_2)].$$

3. Para cada $\sigma \in G$ y para cada $H \in \mathcal{G}$, $\Psi(\sigma H \sigma^{-1}) = \sigma(\Psi(H))$.
4. $H \triangleleft G$ si y sólo si $F(H)|k$ es normal, y en ese caso,

$$\text{Gal}(F(H)|k) \approx G/H.$$

Demostración. Dado un subgrupo H de G obtenemos un único cuerpo fijo $L = F(H)$ por el corolario 9.2.4 (a grupos distintos corresponden cuerpos distintos). Entonces la aplicación Ψ es inyectiva.

Si L es un subcuerpo de K que contiene a k , entonces la extensión $K|L$ es de Galois, por el corolario anterior, y esto significa que $F(\text{Gal}(K|L)) = L$. Así, hemos probado que todo subcuerpo L de K que contiene a k es el cuerpo fijo de un subgrupo de G . La correspondencia Ψ es entonces sobreyectiva.

Ya hemos visto que estas aplicaciones invierten las inclusiones, lo que termina de probar el primer apartado.

Si $L = F(H)$ entonces el teorema 9.2.1 nos dice que $[K : L] = |H|$. Entonces, si $H_1 \subset H_2$ son subgrupos de G se tiene que

$$[K : F(H_1)] = |H_1|, [K : F(H_2)] = |H_2|.$$

Tras dividir y aplicar la fórmula del grado obtenemos

$$\frac{|H_2|}{|H_1|} = \frac{[K : F(H_2)]}{[K : F(H_1)]} = [F(H_1) : F(H_2)].$$

En particular, $|G| = [K : k], [F(H) : k] = \frac{|G|}{|H|}$.

Para el siguiente apartado, sea $\sigma \in G$ y $L = F(H)$. Si $z \in \sigma(F(H))$ entonces $z = \sigma(\alpha)$ con $\alpha \in F(H)$ y

$$(\sigma h \sigma^{-1})(z) = \sigma h \sigma^{-1} \sigma(\alpha) = \sigma h(\alpha) = \sigma(\alpha) = z \text{ para todo } h \in H.$$

Entonces $z \in F(\sigma H \sigma^{-1})$ y $\sigma(F(H)) \subset F(\sigma H \sigma^{-1})$. Por otro lado, el grupo que deja invariante a $\sigma(F(H))$ tiene orden igual a $[K : \sigma(F(H))]$, porque

$$|\text{Gal}(K|\sigma(F(H)))| = [K : \sigma(F(H))],$$

y como $F(H)$ y $\sigma(F(H))$ son isomorfos entonces

$$[K : \sigma(F(H))] = [K : F(H)] = |H|.$$

Hemos llegado a

$$\begin{aligned} \sigma F(H) &\subset F(\sigma H \sigma^{-1}) \subset K, \\ [K : \sigma(F(H))] &= |H|, \quad [K : F(\sigma H \sigma^{-1})] = |\sigma H \sigma^{-1}| = |H| \end{aligned}$$

luego son iguales.

Sea ahora H un subgrupo normal de G . Como para todo $\sigma \in G$ se tiene que $\sigma H \sigma^{-1} = H$, por el apartado anterior vemos que $\sigma(F(H)) = F(H)$ para todo $\sigma \in G$. Es decir, la acción de G sobre K estabiliza $F(H)$. Podemos considerar el siguiente homomorfismo de grupos

$$\begin{aligned} \varphi : G &\rightarrow \text{Aut}(F(H)|k) \\ \sigma &\mapsto \sigma|_{F(H)} \end{aligned}$$

Tenemos que

$$\begin{aligned} \ker(\varphi) &= \{\sigma \in G \mid \varphi(\sigma) = id_{F(H)}\} = \\ &= \{\text{automorfismos de } K \text{ que dejan fijo a } F(H)\} = H. \end{aligned}$$

Sea $G' = \text{im } \varphi$. Entonces $G/H \simeq G'$, que es subgrupo de $\text{Gal}(F(H)|k)$. Por tanto, $|G/H| \leq |\text{Gal}(F(H)|k)|$. Además, $|G/H| = |G|/|H| = [F(H) : k]$. Por otro lado, siempre tenemos que $|\text{Gal}(F(H)|k)| \leq [F(H) : k]$, por lo que

$$[F(H) : k] = |\text{Gal}(F(H)|k)|.$$

Por el corolario 9.2.4 se tiene que $F(\text{Gal}(F(H)|k)) = k$ y entonces $F(H)|k$ es una extensión normal. Además, en este caso $G/H \simeq G' = \text{Gal}(F(H)|k)$.

Recíprocamente, supongamos que $F(H)$ es normal sobre k , con H subgrupo de G . Escribamos $F(H) = k[\alpha_1, \dots, \alpha_m]$. Si $\sigma \in G$ entonces $\sigma(\alpha_i)$ es una raíz del polinomio mínimo de α_i sobre k . Entonces $\sigma(\alpha_i) \in F(H)$. De aquí, $\sigma(F(H)) = F(H)$, y por el apartado anterior $\sigma H \sigma^{-1} = H$. $\square$