4.1 Teorema. Sea $f(x) \in F[x]$ con $gr(f(x)) = n \geq 1$, existe $\sigma : F \to K$ extensión de F tal que K tiene todas las raices de $\sigma^*(f(x))$. Además $[K : \sigma(F)] \leq n!$

Demostración. Haremos inducción sobre el grado de $f(x)$. Si $gr(f(x)) = 1$, entonces F tiene a su única raíz y trivialmente $[F : F] = 1 = 1!$. Ahora supongamos que vale para n y que $gr(f(x)) = n + 1$. Por el Teorema 3.1, existe $\sigma_1 : F \to K_1$ monomorfismo tal que $[K_1 : \overline{F}] \leq (n + 1)$ y además K_1 tiene una raíz de $\sigma_1^*(f(x))$, sea $b \in K_1$ tal raíz. Ahora por el Corolario 2.1, tenemos que $\sigma_1^*(f(x)) = (x - b)t(x)$ con $t(x) \in K_1[x]$, como $n \geq gr(t(x)) > 0$, entonces existe $\sigma_2 : K_1 \to K$ monomorfismo, donde $\sigma_2^*(t(x))$ tiene todas sus raices y además $[K : \sigma_2(K_1)] \leq n!$. Como $\sigma = \sigma_2 \circ \sigma_1 : F \to K$ es monomorfismo, veamos que $(\sigma_2 \circ \sigma_2)^*(f(x))$ tiene todas sus raices en K y luego que $[K : \sigma_2 \circ \sigma_1(F)] \leq (n + 1)!$. Pero $(\sigma_2 \circ \sigma_1)^*(f(x)) = \sigma_2^* \circ \sigma_2^*(f(x)) = \sigma_1^*((x - b)t(x)) = (x - \sigma_2(b))\sigma_2(t(x))$, es claro que $\sigma_2(b) \in K$ y junto con las raices de $\sigma_2^*(t(x))$ serían todas las raices de $(\sigma_2 \circ \sigma_2)^*(f(x))$ y estas se encuentran en K. Ahora como $[K : \sigma_2(\sigma_1(F))] = [K : \sigma_2(K_1)][\sigma_2(K_1) : \sigma_2(\sigma_1(F))] \leq n![\sigma_2(K_1) : \sigma_2(\sigma_1(F))]$, el resultado se sigue si $[\sigma_2(K_1) : \sigma_2(\sigma_1(F))] = [K_1 : \sigma_1(F)]$, pero si en el Lema 3.1, tomamos los campos $\sigma_1(F)$ y $\sigma_2(\sigma_1(F))$, el isomorfismo $\sigma_2 : K_1 \to \sigma_2(K_1)$ los morfismo inclusión $in_1 : \sigma_1(F) \to K_1$ y $in_2 : \sigma_2(\sigma_1(F)) \to \sigma_2(K_1)$, observamos que $\sigma_2(in_1(\sigma_1(a))) = in_2(\sigma_2(\sigma_1(a)))$, obtenemos que $[\sigma_2(K_1) : \sigma_2(\sigma_1(F))] = [K_1 : \sigma_1(F)]$ ya que $[K_1 : \sigma_1(F)] \leq n + 1$. □

Podemos definir el siguiente concepto, dado un polinomio $f(x) \in F[x]$, definiremos el campo de descomposición de $f(x)$. Sabemos existe K campo y $\sigma : F \to K$ monomorfismo tal que $\sigma^*(f(x))$ tiene todas sus raices en K. Si tomamos el mínimo subcampo K_0 de K con $\sigma(F) \subseteq K_0$, que tenga todas las raices de $\sigma^*(f(x))$, este subcampo deberá ser su campo de descomposición, veamos que tal campo es único salvo isomorfismo.

4.2 Teorema. Si $f(x) \in F[x]$ con $gr(f(x)) \leq 1$ y K_1 y K_2 campos con $\sigma_1 : F \to K_1$, $\sigma_2 : F \to K_2$ monomorfismos tales que K_1 tiene todas las raices de $\sigma_1^*(f(x))$ y ningún otro subcampo propio T_0 de K_1 tal que $\sigma_1(F) \leq T_0$ cumple esto, y análogamente K_2 tiene todas las raices de $\sigma_2^*(f(x))$ y ningún otro subcampo propio M_0 de K_2 tal que $\sigma_2(F) \leq M_0$ cumple esto, entonces existe $\overline{\gamma} : K_1 \to K_2$ isomorfismo tal que $\overline{\gamma}(\sigma_1(z)) = \sigma_2(z)$ para todo $z \in F$.

Demostración. Notar que $K_1 = \sigma_1(F)(a_1, \cdots, a_n)$ donde $a_1, \cdots, a_n \in K_1$ son todas las raices de $\sigma_1^*(f(x))$ y además $[K_1 : \sigma_1(F)] \leq n + 1$. Haremos inducción sobre el grado de $f(x)$. Si $gr(f(x)) = 1$, entonces $[K_1 : \sigma_1(F)] \leq 1! = 1$, por tanto $K_1 = \sigma_1^*(F)$, análogamente $K_2 = \sigma_2^*(F)$, podemos tomar $\overline{\sigma} = \sigma_2 \circ \sigma_1^{-1} : \sigma_1(F) \to \sigma_2(F)$, y cumple lo pedido.

Ahora supongamos que se cumple para n y sea $gr(f(x)) = n + 1$. Sea $p(x)$ un factor irreducible de $F(x)$ y $a \in K_1$ y $b \in K_2$ las respectivas raices de $\sigma_1^*(p(x))$ y $\sigma_2^*(p(x))$, sabemos, por el Teorema 3.2, que existe $\overline{\sigma} : \sigma_1(F)(a) \to \sigma_2(F)(b)$ isomorfismo tal que $\overline{\sigma}(\sigma_1(z)) = \sigma_2(z)$ para todo $z \in F$ y $\overline{\sigma}(a) = b$. Sea $\sigma_1^*(f(x)) = (x - a)q(x)$, donde

$q(x) \in \sigma_1(F)(a)[x]$, esto es posible ya que $\sigma_1^*(f(x)) \in \sigma_1(F)[x] \subseteq \sigma_1(F)(a)[x]$ y $x - a \in \sigma_1(F)(a)[x]$. Veamos la siguiente situación $in : \sigma_1(F)(a) \to K_1$, $in \circ \overline{\sigma} : \sigma_1(F)(a) \to K_2$ son monomorfismos $gr(q(x)) = n$, queremos demostrar que K_1 tiene todas las raices de $in^*(q(x))$, y K_2 tiene todas las raices de $(in \circ \overline{\sigma})^*(q(x))$. Por un lado como $in^*(q(x)) = q(x)$ y $q(x)|\sigma_1^*(f(x))$, se cumple lo primero. Pero, $(\overline{\sigma} \circ \sigma_1)^*(f(x)) = \sigma_2^*(f(x))$, por otro lado $(\overline{\sigma} \circ \sigma_1)^*(f(x)) = \overline{\sigma}^*((x-a)q(x)) = (x-b)\overline{\sigma}^*(q(x))$, así que todas las raices de $(in \circ \overline{\sigma})^*(q(x))$ son todas las raices de $\sigma_2^*(f(x))$ salvo b, y estas estan en K_2.

Finalmente si existiera un subcampo propio T_0 de K_1 con $\sigma_1(F)(a) \leq T_0$, que tuviera todas las raices de $in^*(q(x)) = q(x)$, entonces K_0 sería un campo propio de K_1, con todas las raices de $\sigma_1^*(f(x))$, analogamente tenemos que si M_0 fuera un subcampo propio de K_2 con $\overline{\sigma}(\sigma_1(F)(a)) \leq M_0$ y que tuviera todas las raices de $(in \circ \overline{\sigma})^*(q(x))$, como $b \in M_0$, entonces M_0 tendría todas las raices de $\sigma_2^*(f(x))$, lo cual no puede ser. Por hipótesis inductiva, existe $\overline{\gamma} : K_1 \to K_2$ isomorfismo tal que $\overline{\gamma}(in(w)) = in \circ \overline{\sigma}(w)$ para todo $w \in \sigma_1(F)(a)$. En particular tenemos que para todo $z \in F$ se tiene que $\sigma_1(z) \in \sigma_1(F)(a)$, así que se cumple que $\overline{\gamma}(in(\sigma_1(z)) = in(\overline{\sigma}(\sigma_1(z))) = \sigma_2(z)$. □

Podemos decir que el campo de descomposición de un polinomio $f(x) \in F[x]$, es la mínima extensión generalizada de F que contiene todas las raices de $f(x)$ y que además este campo siempre existe y es único salvo isomorfismo. Es más

4.1 Corolario. Si $f(x) \in F[x]$ y $\sigma : F \to K$ monomorfismo, donde K es un campo de descomposición de $f(x)$, entonces $\sigma^*(f(x)) = A\prod_{i=1}^{n}(x - a_i)$, donde $A, a_i \cdots, a_n \in K$.

5. Raices múltiples

5.1 Definición. Sean K una extensión de F, $f(x) \in F[x]$ y $a \in K$. Diremos que a es una raíz de multiplicidad $m \in \mathbb{N}$ si y sólo si $(x-a)^m$ divide a $f(x)$ pero $(x-a)^{m+1}$ no divide a $f(x)$ en $K[x]$. Diremos que una raíz de un polinomio, es una raíz múltiple si su multiplicidad es mayor que 1.

Denotaremos por $Car(F)$ a la caracteristica de F. Ya que $Car(F) = 0$ si y sólo si $\{n \in \mathbb{N} : n \cdot 1 = 0\} = \emptyset$. Es fácil demostrar que si $F \leq K$ $car(F) = 0$ si y sólo si $Car(K) = 0$. Si $f(x) = \sum_{i=0}^{n} a_i x^i$, denoteremos $f'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$.

5.1 Teorema. Sea F con $Car(F) = 0$, y $f(x) \in F[x]$.Entonces: $f(x)$ tiene una raíz múltiple si y sólo si $f(x)$ y $f'(x)$ no son coprimos, es decir tienen un factor comun de grado mayor que 0 en $F[x]$.

Demostración. Supongamos que $f(x)$ tiene una raíz múltiple α en alguna extensión K de F. Entonces $f(x) = (x-\alpha)^m q(x)$ con $m > 1$ y para algún $q(x)$ en $K[x]$, entonces $f'(x) = (x-\alpha)^m q'(x) + m(x\alpha)^{m-1}q(x)$, es decir $x - \alpha$ es un divisor comun de $f(x)$ y $f'(x)$ en $K[x]$. Ahora bién, si $f(x)$ y $f'(x)$ fueran coprimos en $F[x]$, entonces $1 =$

$r(x)f(x)+s(x)f'(x)$ para algunos polinomios en $r(x), s(x) \in F[x]$, pero $F[x] \subseteq K[x]$, asi que $x-\alpha$ divide a $r(x)f(x)$ y a $s(x)f'(x)$ en $K[x]$, es decir $x-\alpha$ divide a 1 en $K[x]$, lo cual no es posible.

Ahora supongamos que $f(x)$ no tiene raices múltiples, es decir todas sus raices son distintas. Podemos pensar a $f(x) \in K[x]$ donde K es el campo de descomposición de $f(x)$, asi que tendremos que $f(x) = \prod_{i=1}^{n}(x-\alpha_i)$ con $\alpha_i \neq \alpha_j$ si $i \neq j$. Calculamos $f'(x)$ en $K[x]$, y tenemos que $f'(x) = \sum_{i=1}^{n}\left(\prod_{i\neq j}(x-\alpha_j)\right)$. Si $t(x)$ es un factor común no trivial de $f(x)$ y $f'(x)$, entonces $t(\alpha_{i_0}) = 0$ para alguna $\alpha_{i_0} \in K$, es decir $f'(\alpha_{i_0}) = 0$, pero $f'(\alpha_{i_0}) = \prod_{j\neq i_0}(\alpha_{i_0}-\alpha_j) \neq 0$ ya que para toda $j \neq i_0$, se tiene que $(\alpha_j - \alpha_{i_0}) \neq 0$. Así que $f(x)$ y $f'(x)$ son coprimos. □

5.1 Corolario. Si $Car(F) = 0$ y $f(x)$ es irreducible en $F[x]$, entonces no tiene raices múltiples.

5.2 Teorema Sea K un campo de caracteristica 0, si $a, b \in K$ algebraicos sobre un subcampo F de K, entonces existe $c \in F(a,b)$ tal que $F(c) = F(a,b)$.

Demostración. Sean $f(x), g(x) \in F[x]$ polinomios irreducibles en $F[x]$ tales que $f(a) = 0$ y $g(b) = 0$. Sea K_1 una extensión de F que contenga todas las raices de $f(x)$ y también de $g(x)$, sean $A = \{a_1, a_2, \cdots, a_n\}$ y $B = \{b_1, b_2, \cdots, b_m\}$ los conjuntos de todas las raices distintas de los respectivos polinomios $f(x)$ y $g(x)$. Desmostraremos que existe $\gamma \in F$ tal que para todo $i > 1$ y $j > 1$, se tiene que $a_i + \gamma b_j \neq a + \gamma b$. Pero $a_i + \gamma b_j = a + \gamma b$ si y sólo si $\gamma = \frac{a_i - a}{b - b_j}$ y $\gamma \neq 0$, como $CarF = 0$, entonces F es infinito, bastará tomar $\gamma \in F \setminus \{\frac{a_i - a}{b - b_j} : i > 1, j > 1\} \cup \{0\}$, para que cumpla lo pedido. Ahora vamos a demostrar que si $c = a + \gamma b$, entonces $F(c) = F(a,b)$. Como $c \in F(a,b)$, entonces $F(c) \leq F(a,b)$. Ahora mostraremos que $a, b \in F(c)$, tomamos $h(x) = f(c - \gamma x) \in F(c)$, tenemos que $h(b) = f((a + \gamma b) - \gamma b) = f(a) = 0$. Sea K_2 extensión de K_1 (y por tanto de F y $F(c)$) que tenga todas las raices de $h(x)$ en $K_2[x]$; $x - b$ divide a $g(x)$ y a $h(x)$. Para $j > 1$, como $h(b_j) = f(a + \gamma b - \gamma b_j)$, $h(b_j) = 0$ si y sólo si $a + \gamma b - \gamma b_j = a_i$, es decir, si y sólo si $a + \gamma b = a_i + \gamma b_j$. Ahora si $a_i = a$, entonces $\gamma = 0$, lo cual no puede ser, así que $h(b_j) \neq 0$ para $j > 1$. Si $r(x) = mcd(g(x), h(x))$ en $K_2[x]$, $r(x)$ tiene como única raíz a b, si $gr(r(x)) \geq 2$, entonces $(x-b)^2 | r(x)$, y así $(x-b)^2 | g(x)$, pero no puede ser porque $g(x)$ es irreducible; así que $r(x) = x - b$. Como $h(x), g(x) \in F(c)[x]$, si $s(x)$ su maximo comun divisor de ellos en $F(c)[x]$, este no puede ser trivial ya que entonces $r(x)$ sería trivial, y además debe dividir a $x - b$ en $K_2[x]$, luego entonces $x - b = s(x)$. Es decir $x - b \in F(c)[x]$, es decir $b \in F(c)$, como $\gamma b \in F(c)$, tenemos finalmente que $a \in F(c)$ y por tanto $F(a,b) = F(c)$. □

5.2 Corolario. Sea $Car(F) = 0$ y $F \leq K$ una extensión finita de F, entonces existe $c \in K$, tal que $K = F(c)$

Demostración. Se puede demostrar por indución que $F(a_1, \cdots, a_n) = F(c)$ para algún $c \in F(a_1, \cdots, a_n)$. Ahora si $[K : F] < \infty$, sea $\{a_1, \cdots, a_n\}$ una base de ${}_FK$, entonces $K = F(a_1, \cdots, a_n)$ y por tanto $K = F(c)$ para algún $c \in K$. □

6. Teoría de Galois

Todos los campos en esta sección tienen caracterisitca 0.

Sea K un campo denotamos por $\mathcal{A}(K) = \{T : T \text{ es un automorfismo de } K\}$. Sean $\mathcal{F}(K) = \{F : F \text{ es subcampo de } K\}$ y $\mathcal{O}(K) = \{H : H \text{ subgrupo de } \mathcal{A}(K)\}$; podemos definir dos estructuras duales:Dado $H \in \mathcal{O}(K)$ y $F \in \mathcal{F}(K)$, denotamos por $K_H = \{\alpha \in K : T(\alpha) = \alpha \text{ para todo } T \in H\}$ y $G(K, F) = \{T \in \mathcal{A}(K) : T(\alpha) = \alpha \text{ para todo } \alpha \in F\}$. Veamos las siguientes propiedades

6.1 Lema. Sea $H \in \mathcal{O}(K)$ y $F \in \mathcal{F}(K)$, entonces $K_H \in \mathcal{F}(K)$ y $G(K, F) \in \mathcal{O}(K)$

Demostración. Sean $\alpha, \beta \in K_H$ y $T \in H$, entonces $T(\alpha \pm \beta) = T(\alpha) \pm T(\beta) = \alpha \pm \beta$ y $T(\alpha\beta) = T(\alpha)T(\beta) = \alpha\beta$, y si $\alpha \neq 0$, entonces $T(\alpha^{-1}) = (T(\alpha))^{-1} = \alpha^{-1}$, así que $K_H \in \mathcal{F}(K)$. Ahora, sea $T_1, T_2 \in G(K, F)$ y $\alpha \in F$, entonces $T_1 \circ T_2(\alpha) = T_1(T_2(\alpha)) = T_1(\alpha) = \alpha$, así que $T_1 \circ T_2 \in G(K, F)$. Por otro lado calculemos $(T_1)^{-1}(\alpha) = (T_1)^{-1}(T_1(\alpha)) = \alpha$, por tanto $G(K, F) \in \mathcal{O}(K)$. □

Veamos ahora la importante propiedad de los automorfismos.

6.2 Lema. Sean $T_1, \cdots, T_n \in \mathcal{A}(K)$ diferentes, entonces no existen $a_1, \cdots, a_n \in K$ no todos cero tal que $\sum_{i=1}^{n} a_i T_i(x) = 0$ para todo $x \in K$

Demostración. Supongamos que existen $a_1, \cdots, a_n \in K$ no todos cero tal que $\sum_{i=1}^{n} a_i T_i(x) = 0$ para todo $x \in K$. Sean
$L = \{l : \text{ existen } a_{i_1}, \cdots, a_{i_l} \in K \setminus \{0\} \text{ con } \{1_1, \cdots, i_l\} \subset \{1, \cdots, n\} \text{ y}$
$\sum_{j=1}^{l} a_{i_j} T_{i_j}(x) = 0 \text{ para todo } x \in K\}$.

Por el supuesto tal conjunto es no vacío, sea $m = min\ L$. Entonces existen $i_1, \cdots, i_m \in \{1, \cdots, n\}$ y $a_{i_1}, \cdots, a_{i_m} \in K \setminus \{0\}$, tal que $\sum_{j=1}^{m} a_{i_j} T_{i_j}(x) = 0$ para todo $x \in K$. Ahora como $T_{i_1} \neq T_{i_m}$, existe $c \in K$ tal que $T_{i_1}(c) - T_{i_m}(c) \neq 0$. Obtenemos las siguientes relaciones:

$$\sum_{j=1}^{m} a_{i_j} T_{i_j}(cx) = 0 \text{ para todo } x \in K$$

$$T_{i_1}(c)(\sum_{j=1}^{m} a_{i_j} T_{i_j}(x)) = 0 \text{ para todo } x \in K.$$