Álgebra III

Rodrigo Raya Castellano
Universidad de Granada

Índice

1. Polinomios simétricos

Sea A un anillo y $A[X_1, \cdots, X_n]$ el anillo de polinomios en las indeterminadas $X_1, \cdots, X_n$ con coeficientes en A.

Definamos para cada $\sigma \in S_n$ un homomorfismo de anillos

$$f_\sigma : A[X_1, \cdots, X_n] \to A[X_1, \cdots, X_n]$$

tal que $f_\sigma(X_i) = X_{\sigma(i)}$ para todo $1 \leq i \leq n$. Intuitivamente esta transformación renombra o permuta las variables del polinomio.

Proposición 1.1.
Para cada σ, f_σ es un isomorfismo de anillos con inverso $f_{\sigma^{-1}}$.

Definición 1.1 (Polinomios simétricos)**.**
Un polinomio $p \in A[X_1, \cdots, X_n]$ es simétrico si es invariante por f_σ para cada $\sigma \in S_n$, esto es, $\forall \sigma \in S_n . f_\sigma(p) = p$.

El conjunto de los polinomios simétricos de $A[X_1, \cdots, X_n]$ se denota por $Sim(A[X_1, \cdots, X_n])$.

Se suele usar la notación $\sum X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}$ para denotar la suma de todos los monomios distintos que se pueden generar mediante permutaciones de las variables sobre el monomio $X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}$.

Ejemplo 1.1:

$$\sum X_1^3 = X_1^3 + X_2^3 + X_3^3$$

$$\sum X_1^2 X_2 = X_1^2 X_2 + X_1^2 X_3 + X_2^2 X_1 + X_2^2 X_3 + X_3^2 X_2 + X_3^2 X_1$$

Proposición 1.2.
$Sim(A[X_1, \cdots, X_n])$ es un subanillo de $A[X_1, \cdots, X_n]$ y contiene a A.

Demostración. Todo polinomio constante es simétrico. Claramente, el subconjunto de los polinomios constantes es un subanillo de $A[X_1, \cdots, X_n]$ y por abuso del lenguaje diremos que $A[X_1, \cdots, X_n]$ contiene a A, en realidad, contiene a los polinomios constantes, que son isomorfos a A.

Veamos que $Sim(A[X_1, \cdots, X_n])$ es un subanillo. Por lo anterior, $1, -1 \in Sim(A[X_1, \cdots, X_n])$ y podemos comprobar que la suma y el producto son cerrados en $Sim(A[X_1, \cdots, X_n])$. En efecto, si $p, q \in Sim(A[X_1, \cdots, X_n])$ entonces $f_\sigma(p+q) = f_\sigma(p) + f_\sigma(q) = p+q \wedge f_\sigma(pq) = f_\sigma(p) f_\sigma(q) = pq$. Estas condiciones son suficientes para afirmar que $Sim(A[X_1, \cdots, X_n])$ es un subanillo de $A[X_1, \cdots, X_n]$. □

Definición 1.2.
Un polinomio es homogéneo si todos sus monomios tienen el mismo grado.

Ejemplo 1.2: El polinomio $x^5 + 2x^3y^2 + 9xy^4$ es un polinomio homogéneo de grado cinco en dos variables.

Podemos reducir el estudio de los polinomios simétricos al estudio de los polinomios simétricos homogéneos.

Proposición 1.3.
1. Todo polinomio de $A[X_1, \cdots, X_n]$ se puede expresar de forma única como una suma de polinomios homogéneos, es decir, $\forall p \in A[X_1, \cdots, X_n]$ p se expresa de forma única como $p = p_0 + \cdots + p_r$ suma de polinomios homogéneos de grado i. A los polinomios p_i se les llama componentes homogéneas de p.

2. Un polinomio $p \in A[X_1, \cdots, X_n]$ es simétrico $\iff$ cada una de sus componentes homogéneas lo es.

Definición 1.3 (Polinomios simétricos elementales)**.**
Los polinomios simétricos elementales en las variables $X_1, \cdots, X_n$ son los siguientes:

$$e_1 = \sum_{i=1}^{n} X_i$$

$$e_2 = \sum_{i_1<i_2} X_{i_1} X_{i_2}$$

$$\cdots$$

$$e_n = \sum_{i_1<\cdots<i_n} X_{i_1} \cdots X_{i_n}$$

Esto es se trata de polinomios homogéneos y simétricos que presentan para cada sumando las posibles combinaciones en orden lexicográfico.

Se suelen denotar $(X_1), \cdots, (X_1 \cdots X_r)$ o $\sum X_1, \cdots, \sum X_1 X_2 \cdots X_n$.

Proposición 1.4.
Sea $p \in A[X_1, \cdots, X_n, T] = A[T][X_1, \cdots, X_n]$ *dado por*

$$p = (T - X_1) \cdots (T - X_n)$$

Este polinomio como elemento de $A[X_1, \cdots, X_n][T]$ *se escribe como*

$$p = T^n + (-1)e_1 T^{n-1} + (-1)^2 e_2 T^{n-2} + \cdots + (-1)^n e_n$$

Obsérvese que la anterior relación cuando se considera el homomorfismo de evaluación nos da una relación entre las raíces y los coeficientes del polinomio presentado en su forma estándar.

Teorema 1.5 (Teorema fundamental de los polinomios simétricos)**.**
$Sim(A[X_1, \cdots, X_n]) \cong A[e_1, \cdots, e_n]$

Demostración. Dado un polinomio $F \in A[X_1, \cdots, X_n]$ lo escribo de forma única en función de sus componentes homogéneas $F = F_0 + \cdots + F_m$ y por los resultados anteriores, estudiar que F sea simétrico equivale a estudiar que las componentes homogéneas de F sean simétricas.

Vamos a describir un método para dado un polinomio homogéneo y simétrico obtenerlo como polinomio en los polinomios simétricos elementales e_i de forma única.

Para empezar definimos la relación $a \prod_i X_i^{k_i} > b \prod_i X_i^{h_i}$ si el primer índice t para el que las potencias de las variables difieren, se tiene que $k_t > h_t$. Esta relación no ordena todavía los monomios de mi polinomio homogéneo. Falta ver que si dos monomios se escriben igual salvo el coeficiente líder entonces son iguales. Para conseguirlo hacemos una primera transformación, agrupando los términos de la forma $a \prod_i X_i^{k_i}$ en un solo monomio.

Está claro que la relación sobre el conjunto de monomios resultante, es un relación de orden estricto total (antireflexiva, antisimétrica, transitiva y total). Entonces en cada paso puedo elegir un mayor monomio. Sea este $a \prod_i X_i^{k_i}$ En este monomio se va a verificar que $\forall i. k_i \geq k_{i+1}$, esto es, los exponentes están ordenados en orden decreciente. Se razona por contradicción. Si existiera $i < j$ tal que $k_i \leq k_j$ entonces podríamos construir el monomio $a X_1^{k_1} \cdots X_i^{k_j} \cdots X_j^{k_i} \cdots X_n^{k_n} \geq a \prod_i X_i^{k_i}$. En contradicción con que $c \prod_i X_i^{k_i}$ era el mayor monomio. (¿por qué esta relación no sirve en el ambiente general de los polinomios simétricos?)

Construimos el polinomio $g = e_1^{k_1-k_2} e_2^{k_2-k_3} \cdots e_{n-1}^{k_{n-1}-k_n} e_n^{k_n}$ y observamos que el término líder de cada e_i es $x_1 \cdots x_i$. Teniendo en cuenta que el término líder respecto a $>$ de un producto es el producto de los términos líderes de los factores, tenemos que el término líder de g es

$$x_1^{k_1-k_2}(x_1x_2)^{k_2-k_3} \cdots (x_1 \cdots x_n)^{k_n} = x_1^{k_1-k_2+k_2-k_3+\cdots+k_n} x_2^{k_2-k_3+\cdots+k_n} \cdots x_{n-1}^{k_{n-1}-k_n+k_n} x_n^{k_n} = x_1^{k_1} \cdots x_n^{k_n}$$

Como consecuencia f y cg tienen el mismo término líder y el polinomio $f_1 = f - cg$ es un polinomio simétrico (pues f y cg son simétricos) y homogéneo con un término líder estrictamente menor según el orden definido en $>$. Este proceso debe terminar cuando se llega a un f_m tal que $f_m = 0$ que no tiene términos líder. Si $f_m = f - cg - c_1g_1 - \cdots - c_{m-1}g_{m-1}$, se sigue que $f = cg + c_1g_1 + \cdots + c_{m-1}g_{m-1}$. Cada g_i es un polinomio en los e_i. Esto completa la existencia.

Veamos que la descomposición es única. Consideramos una aplicación $\phi : A[u_1, \cdots, u_n] \to A[x_1, \cdots, x_n]$ dado por $u_i \mapsto e_i$ donde visualizamos e_i como un polinomio en los x_i. Claramente, esto define un único homomorfismo entre ambos anillos y la imagen de dicho homomorfismo podría ser denotada (notación, ya que no se puede usar símbolos para variables que hayan sido utilizados para definir polinomios) por $A[e_1, \cdots, e_n]$ los polinomios dados en función de e_i. Por ser la imagen por un homomorfismo podemos definir un subanillo $A[e_1, \cdots, e_n]$ y podemos restringir a un homomorfismo $\phi : A[u_1, \cdots, u_n] \to A[e_1, \cdots, e_n]$. Este homomorfismo es sobreyectivo por definición y la unicidad se demuestra provando que $Ker(f) = \{0\}$.

En efecto, dado un polinomio $h \in A[u_1, \cdots, u_n] - \{0\}$ aplicamos ϕ a cada uno de sus términos $c\prod u_i^{b_i}$ transformándolo en $c\prod e_i^{b_i}$ y por un argumento similar al anterior, vemos que el término líder de este polinomio es $cx_1^{b_1+\cdots+b_n} x_2^{b_2+\cdots+b_n} + x_n^{b_n}$. Claramente, la imagen de h, $\phi(h)$ será suma de los términos de esta forma. El punto esencial aquí es que la aplicación $(b_1, \cdots, b_n) \mapsto (b_1 + \cdots + b_n, b_2 + \cdots + b_n, b_n), \cdots, b_n)$ es biyectiva y por tanto los términos líderes no pueden cancelarse de modo que $\phi(h)$ no puede ser 0.

□

EJERCICIO 1.1:

- Demostrar que dados $f, g \in F[x_1, \cdots, x_n] \neq 0$ tenemos que $TL(fg) = TL(f)TL(g)$ donde TL denota el término líder de un polinomio. (quizás esto no es necesario por ser ?)
- Demostrar que la aplicación $(b_1, \cdots, b_n) \mapsto (b_1 + \cdots + b_n, b_2 + \cdots + b_n, b_n), \cdots, b_n)$ biyectiva. Considera el término de $h(u_1, \cdots, h_n)$ para el cual $ce_1^{b_1} \cdots e_n^{b_n}$ es maximal. Prueba que este término es de hecho el término líder de $h(e_1, \cdots, e_n)$. Ver que esto implica que si $h \neq 0$ entonces $\phi(h) \neq 0$.

1.1. Resultante y discriminante

Utilizando polinomios simétricos vamos a estudiar las raíces comunes de dos polinomios con coeficientes en un dominio de integridad.

Sea A un dominio de integridad y K su cuerpo de fracciones. Sean $p, q \in K[X]$ de grado n y m respectivamente de la forma

$$p = \sum_{i=0}^{n} a_i X^i$$

y

$$q = \sum_{i=0}^{m} b_i X^i$$

Proposición 1.6.
Son equivalentes:

1. $mcd(p,q) \neq 1$*, esto es,* p, q *tienen alguna raíz común en* K*.*
2. Existen $p_1, q_1 \in A[X] - \{0\}$ *con* $gr(p_1) \leq n-1$*,* $gr(q_1) \leq m-1$ *y* $pq_1 = qp_1$*.*
3. $R(p,q) = 0$

Demostración. 1. $\implies$ 2.) Considere el máximo común divisor de p, q, esto es, $mcd(p,q)$. Sabemos que $mcd(p,q)mcm(p,q) = pq$. Como $mcd(p,q) \neq 1$ tenemos que $mcm(p,q) \neq pq$. Por definición de mínimo común múltiplo deben existir p_1, q_1 tales que $m = p_1 q = q_1 p$. Además, claramente, $gr(m) < gr(p), gr(q)$ y como en un dominio de integridad $gr(pq) = gr(p) + gr(q)$ tenemos que como $pq_1 = m$ necesariamente $gr(q_1) < gr(q)$ y análogamente $gr(p_1) < gr(p)$.

2. $\implies$ 1.) Recíprocamente, supongamos una tal factorización $pq_1 = qp_1$. Como $K[X]$ con K un cuerpo es un dominio euclídeo, se tiene que es un dominio de factorización única. Consideremos la factorización en irreducibles de la ecuación $pq_1 = qp_1$. Como $gr(p_1) < gr(p)$ habrá algún factor de p que sea factor de p_1 y por tanto será factor de q. En consecuencia, p, q no tienen un máximo común divisor constante.

Podemos hallar estos polinomios resolviendo la ecuación $pq_1 - qp_1 = 0$. □

La expresión de la resultante en términos de determinantes es:

Teorema 1.7.
En la situación anterior, se verifica:

1. La resultante $R(p,q)$ *es un polinomio homogéneo de grado* m *en los* a_i *y de grado* n *en los* b_j*.*
2. Existen polinomios P, Q *con coeficientes polinomios en los* a_i, b_j *y grados menores que* $n-1, m-1$ *respectivamente, verificando que* $R(p,q) = pQ + qP$*.*
3. Sean α_i *raíces de* p *y* β_j *raíces de* q *en* $K[X]$*. Entonces, la resultante es salvo constante el producto de las diferencias de las raíces:*

$$R(p,q) = a_n^m \prod_{i=0}^{n} q(\alpha_i) = (-1)^{nm} b_m^n \prod_{j=1}^{m} p(\beta_j) = a_n^m b_m^n \prod_{i,j=1}^{n,m} (\alpha_i - \beta_j)$$

Demostración. 1. La resultante de los polinomios Tp, q tiene las m primeras filas multiplicadas por T. Por las reglas de cálculo con determinantes, tenemos que, $R(Tp,q) = T^m R(p,q)$. Por tanto, $R(p,q)$ es un polinomio homogéneo de grado m en los a_i.

2.

3. Sea T un indeterminada. Definimos $R(T) = R(p, q-T)$ y denotamos $\gamma_i = q(\alpha_i)$. Claramente, $p, q-T$ tienen α_i como raíz común. Por tanto, $R(\gamma_i) = 0$. Obsérvese quién es $q - T$. $q - T$ como polinomio en T es un polinomio lineal. $q - T$ como polinomio en X es el polinomio q donde a su término constante se le ha restado T.

Ahora, como el sumando de mayor grado en T se obtiene al multiplicar los elementos de la diagonal de $R(p, q-T)$, $R(T)$ es un polinomio de grado n cuyo coeficente líder es $(-1)^n a_n^m$ y entonces $R(T)$ se escribe como $R(T) = (-1)^n a_n^m \prod_{i=1}^m (T - \gamma_i) = a_n^m \prod_{i=1}^m (T - \gamma_i)$. (revisar)

Además, $\gamma_i = q(\alpha_i) = b_m \prod_{i=j}^m (\alpha_i - \beta_j)$ y evaluando en $T = 0$ la expresión anterior, queda, $R(p,q) = a_n^m b_m^n \prod_{i=1}^n \prod_{j=1}^m (\alpha_i - \beta_j)$.

□

Proposición 1.8 (Cálculo efectivo del determinante)**.**
1. $R(p,q) = (-1)^{nm} R(q,p)$.
2. Sean $p, q \in A[X]$ *y sea* $r \in A[X]$ *el resto de la división euclídea de* q *entre* p*. Entonces,* $R(p,q) = a_n^{m-gr(r)} R(p,r)$.
3. Si $a \in A$ *entonces* $R(p,a) = a^n$.

Demostración. 1. Uno es evidente ya que al permutar dos filas el determinante cambia de signo. Como se permutan las filas mn veces, el resultado es alterado por $(-1)^{nm}$. □

2. Extensiones de cuerpos

2.1. Preliminares

Empezamos con algunos recordatorios del álgebra de anillos.

Teorema 2.1.
Dado un cuerpo F y $f \in F[X]$ no constante entonces son equivalentes:

- *El polinomio f es irreducible en F.*
- *El ideal $< f >$ es maximal.*
- *El anillo cociente $F[x]/ < f >$ es un cuerpo.*

Ejemplo 2.1: $\frac{\mathbb{R}}{<x^2+1>} \cong \mathbb{C}$

Definición 2.1 (Extensión de cuerpos)**.**
Sean K y F son dos cuerpos con K un subcuerpo de F. Entonces se dice que F es un cuerpo extensión de K y lo denotaremos por $K \subseteq F$.

Observando que, todo subcuerpo es un ideal, tenemos definido $\frac{F}{K}$ y lo llamaremos una extensión de cuerpos de K.

Proposición 2.2 (Estructura de las extensiones como espacio vectorial)**.**
Si $\frac{F}{K}$ es una extensión de cuerpos, entonces F tiene estructura de espacio vectorial sobre K.

Demostración. Consideramos como conjunto de escalares K y como conjunto de vectores F. Dado que K es un subcuerpo de F, tenemos que todas las propiedades de espacio vectorial se verifican por las propiedades de cuerpo de F. □

Definición 2.2 (Grado de una extensión)**.**
Sea $\frac{F}{K}$ una extensión de cuerpos. El grado de la extensión, $[F : K]$, es la dimensión de F como espacio vectorial sobre K. Si $[F : K]$ es finito entonces se dice que la extensión es finita. En otro caso se dice que es infinita.

Definición 2.3 (Torre de cuerpos)**.**
Una torre de cuerpos es una cadena de subcuerpos de un cuerpo F $F_0 \subseteq \cdots \subseteq F_m = F$. Al menor subcuerpo F_0 se le llama cuerpo base.

Lema 2.3 (Base de una torre de cuerpos)**.**
Sea $K \subseteq F \subseteq E$ una torre de cuerpos.

Sea $\{u_i\}$ una base de E sobre F y $\{v_j\}$ una base de F sobre K. Entonces $\{u_i v_j\}$ es una base de E sobre K.

Demostración. 1. $\{u_i v_j\}$ es sistema de generadores. En efecto, podemos escribir para cada $e \in E$:

$$e = \sum u_i f_i = \sum u_i (\sum v_j k_{ij}) = \sum (u_i v_i) k_{ij}$$

2. $\{u_i v_j\}$ son linealmente independientes. Aplicando la independencia lineal de cada de las bases:

$$\sum u_i v_j k_{ij} = \sum u_i (\sum v_j k_{ij}) = 0$$

y se tiene que $k_{ij} = 0$. □

Proposición 2.4 (Teorema de la torre de cuerpos)**.**
Sea $K \subseteq F \subseteq E$ una torre de cuerpos.

$\frac{E}{K}$ es finita $\iff$ $\frac{F}{K}, \frac{E}{F}$ son finitas.

En cuyo caso, $[E : K] = [E : F][F : K]$.

Demostración. Teniendo una base de cada uno de ellos, calculamos la base de la torre de inclusiones, que nos la dimensión. □

Corolario 2.5.
1. Sea $F_0 \subseteq \cdots \subseteq F_m$ una torre de cuerpos entonces:

$\frac{F_m}{F_0}$ es finita $\iff$ $\frac{F_{i+1}}{F_i}$ son finitas.

En cuyo caso, $[F_m, F_0] = \prod_{i=m}^{1} [F_i : F_{i-1}]$

2. Sea $\frac{F}{K}$ una extensión de grado primo entonces no existe ningún cuerpo intermedio propio.

2.2. Algunas extensiones naturales

Nuestro ahora es describir algunos subanillos y subcuerpos de interés para una extensión $K \subseteq F$.

Definición 2.4 (Subanillo y subcuerpo generados por un conjunto)**.**
Sea $\frac{F}{K}$ una extensión de cuerpos e $Y \subseteq F$. Definimos los siguientes conjuntos:

1. $K[Y] = \{\sum k_{i_1 \cdots i_r} \prod_{j=1}^{r} y_{i_j} : k_{i_1 \cdots i_r} \in K, y_{i_j} \in Y\}$ es el conjunto de las expresiones polinómicas en los elementos de Y con coeficientes en K.
2. $K(Y) = Q(K[Y])$, esto es, $K(Y)$ es el cuerpo de fracciones de $K[Y]$. Esto se puede ver como el conjunto de expresiones racionales en los elementos de Y con coeficientes en K.

Definición 2.5 (Caso finito)**.**
Si $Y = \{u_1, \cdots, u_r\}$ entonces $K[Y] = K[u_1, \cdots, u_r]$ y $K(Y) = K(u_1, \cdots, u_r)$. Esto es, $K[Y]$ es el conjunto de las expresiones polinómicas en las indeterminadas u_i con coeficientes en K y $K(Y)$ es el conjunto de las expresiones racionales en las indeterminadas u_i con coeficientes en K.

Definición 2.6 (Extensión de generación finita)**.**
Cuando $F = K(\alpha_1, \cdots, \alpha_n)$ con $\alpha_i \in F$, se dice que F es de generación finita.

Si $n = 1$ la extensión se dice simple y al generador se le llama elemento primitivo para la extensión.

Proposición 2.6 (Generación de subcuerpos por adjunción)**.**
Sea $\frac{F}{K}$ una extensión de cuerpos e $Y \subseteq F$.

1. El subanillo generado por K, Y es $K[Y]$
2. El subcuerpo generado por K, Y es $K(Y)$.
3. Si $Z \subseteq Y$ entonces:

- $K[Y \cup Z] = K[Y][Z] = K[Z][Y]$
- $K(Y \cup Z) = K(Y)(Z) = K(Z)(Y)$

4. Para cada $\alpha \in K(Y)$ existe $Z \subseteq Y$ finito tal que $\alpha \in K(Z)$.

Demostración. 1. Llamemos polinomios en Y al miembro derecho y denotémoslo por P.

Claramente, P es un subanillo de F ya que si tomo $x = \sum k \prod_{j=1}^{r} y_{i_j}, y = \sum k' \prod_{j=1}^{r} y'_{i_j}$ entonces $x - y = \sum k \prod_{j=1}^{r} y_{i_j} - \sum k' \prod_{j=1}^{r} y'_{i_j} = \sum k \prod_{j=1}^{r} y_{i_j} + \sum(-k') \prod_{j=1}^{r} y'_{i_j} \in P$ ya que K es un cuerpo. También el producto es cerrado en F, si tomo $x = \sum k \prod_{j=1}^{r} y_{i_j}, y = \sum k' \prod_{j=1}^{r} y'_{i_j}$ entonces $xy = \sum \sum kk' \prod y_{ij} y'_{ij}$ donde hemos utilizado la propiedad distributiva general. Finalmente, basta tomar un producto vacío y el 1 de K para poder asegurar que $1 \in P$.

Veamos ahora que debe coincidir con el mínimo generado por K e Y.

$\subseteq$) Como $K, Y \subseteq K[Y]$ claramente, $K[Y] \subseteq P$.

$\supseteq$) Como un subanillo es cerrado para productos y sumas de sus elementos se deduce que $K[Y] \supseteq P$.

2. Esto se sigue de que el cuerpo de fracciones es el menor cuerpo que contiene a un anillo.

3. Hay que tener cuidado ya que Y puede ser infinito.

$\supseteq$) Como $K[Y \cup Z]$ es el menor subanillo que contiene a K, Y, Z. Como contiene a K, Y contiene al menor subanillo que engendran $K[Y]$ y como contiene a Z, contiene al menor subanillo que engendran $K[Y], Z$ esto es $K[Y][Z]$.

$\subseteq$) Como $K[Y][Z]$ es el menor subanillo que contiene a $K[Y], Z$ y $K[Y]$ es el menor subanillo que contiene a K, Y, entonces claramente $K[Y][Z]$ es el menor subanillo que contiene a K, Y, Z y por tanto $K[Y][Z] = K[Y \cup Z]$.

Análogamente se procede para cuerpos.

4. Si $\alpha \in K(Y)$ es una función racional en los valores de Y. El polinomio del denominador estará en número de variables r y el del denominador en r' tomando el máximo, es claro que $\alpha \in K(\{y_1, \cdots, y_{max(r,r')}\})$ □

Definición 2.7 (Extensión producto)**.**
Sean E, F subcuerpos de un cuerpo L tal que contienen un subcuerpo común K. El compuesto de E y F es el menor subcuerpo de L que contiene a E y a F. Lo denotaremos por EF.

Claramente $EF = E(F) = F(E)$.

2.3. Extensiones algebraicas

Definición 2.8 (Elementos algebraicos y trascendentes)**.**
Dada $\frac{F}{K}$ una extensión de cuerpos, un elemento $\alpha \in F$ se llama algebraico sobre K si existe un polinomio no nulo $f(x) \in K[X]$ tal que $f(\alpha) = 0$. En caso contrario diremos que es trascendente.

Si todo elemento de F es algebraico en K entonces la extensión $\frac{F}{K}$ se dice algebraica.

Recuérdese la propiedad universal de los anillos de polinomios, existe un único h_α tal que hace comutar el diagrama inferior y este h_α es de la forma $h_\alpha(f) = f(\alpha)$, esto es, el homomorfismo de evaluación en α.

$$\begin{array}{ccc} K & \xrightarrow{i} & F \ni \alpha \\ \downarrow{\scriptstyle i} & \nearrow_{h_\alpha} & \\ K[X] & & \end{array}$$

Claramente, un elemento $\alpha \in K$ es algebraico $\iff Ker(h_\alpha) \neq \{0\}$.

Obsérvese que $Ker(h_\alpha)$ no es más que el conjunto de las expresiones polinómicas en la variable α y coeficientes en K que son cero.

Proposición 2.7 (Introducción del polinomio mínimo)**.**
Dada una extensión de cuerpos $\frac{F}{K}$ y $\alpha \in F$ un elemento algebraico sobre K, existe un único polinomio irreducible y mónico f tal que $Ker(h_\alpha) = \langle f \rangle$. Esta última condición se expresa diciendo que α es raíz del polinomio y cualquier otro polinomio del que α sea raíz, es un múltiplo de este.

Demostración. Como $K[X]$ es un dominio euclídeo con función euclídea el grado, en particular es un dominio de ideales principales y ya que $Ker(h_\alpha)$ es un ideal estará generado por un polinomio f. Para ver que es irreducible, vemos que:

- no es nulo ya que α es algebraico y por tanto $Ker(\alpha) \neq \{0\}$.
- no es unidad ya que las unidades de $K[X]$ son los polinomios constantes, no nulos y α no puede ser raíz de estos.
- Si $f = g_1 g_2$ entonces $(g_1 g_2)(\alpha) = g_1(\alpha) g_2(\alpha) = 0$ de donde algún $g_i(\alpha) = 0$ pues K es en particular un dominio de integridad supongamos que es $g_1(\alpha) = 0$. Por tanto, $g_1 \in < f >$, esto es, existe un polinomio h tal que $g_1 = hf$ y en consecuencia, $f = g_1 g_2 = hf g_2 = h g_2 f$ y en consecuencia, como estamos en un dominio de integridad $hg_2 = 1$ luego $g_2 \in U(K[X])$ y por tanto g_1 está asociado a f.

Claramente, como K es un cuerpo puedo conseguir que sea mónico multiplicando por la constante inverso del término líder, que es un polinomio asociado al original.

Finalmente, si g es un polinomio de grado mínimo tal que $g(\alpha) = 0$ entonces, $g \in \langle f \rangle$ y como antes g es asociado a f.

□

Definición 2.9 (Polinomio mínimo)**.**
Al polinomio anterior, se le llama polinomio mínimo de α sobre K y se denota por $Irr(\alpha, K)$.

En general puede no ser sencillo demostrar la igualdad dada por la proposición anterior. En la práctica, se usan criterios equivalentes para reconocer al polinomio mínimo.

Proposición 2.8 (Criterios de polinomio mínimo)**.**
Dada una extensión de cuerpos $\frac{F}{K}$ y $\alpha \in F$ un elemento algebraico sobre K. Sea $p \in K[X]$ el polinomio mínimo de α sobre K. Si $f \in K[X]$ es un polinomio mónico entonces $f = p$ sí y sólo sí se dan algunas de las siguientes condiciones:

1. f es un polinomio de grado mínimo satisfaciendo $f(\alpha) = 0$.
2. f es irreducible sobre K y $f(\alpha) = 0$.

Demostración. Véase Cox, página 74. □

Proposición 2.9 (Propiedades del polinomio mínimo)**.**
Dada una extensión de cuerpos $\frac{F}{K}$ y $\alpha \in F$ un elemento algebraico sobre K:

1. Se verifica que $K(\alpha) \cong \frac{K[X]}{<Irr(\alpha,K)>}$. En particular, $K[\alpha] = K(\alpha)$.

2. $n = [K(\alpha) : K] = gr(Irr(\alpha, K))$ y $\{1, \alpha, \cdots, \alpha^{n-1}\}$ es una base de $K(\alpha)$ como K-espacio vectorial.

Demostración. 1. Por el primer teorema de isomorfía sabemos que $\frac{K[X]}{<Irr(\alpha,K)>} \cong h_\alpha(K[X]) = K[\alpha]$. Por el teorema 2.1 tenemos que el miembro derecho es un cuerpo y la imagen por un isomorfismo seguirá siéndolo.

Como $K[\alpha]$ es el menor subanillo que contiene a α, K y además resulta que es un cuerpo, también será el menor cuerpo que contiene a K y α, esto es $K(\alpha)$.

2. A priori, el primer teorema de isomorfía da un isomorfismo $f_\alpha([g]) = h_\alpha(g)$ por tanto, todo elemento de $K(\alpha)$ se puede poner como $g(\alpha) = \sum_{i=0}^{m} b_i\alpha^i$.

Vamos a ver que en realidad podemos tener un sistema de generadores más pequeño. Para ello, basta elegir un representante adecuado. Dado g elijo g_1 en su clase tal que $g \equiv g_1\ mod(Irr(\alpha, K))$ donde hemos utilizado el algoritmo de la división y entonces $gr(g_1) = r < n$ entonces claramente $g(\alpha) = g_1(\alpha) = \sum_{i=1}^{r} k_i\alpha^i$ y por tanto $\{1, \alpha, \cdots, \alpha^{n-1}\}$ es un sistema de generadores.

Veamos que son independientes. Si $\sum_{i=0}^{n-1} k_i\alpha^i = 0$ entonces α es raíz del polinomio $\sum_{i=0}^{n-1} k_iX^i$. Pero este polinomio tiene grado menor que $Irr(\alpha, K)$ y está en $< Irr(\alpha, K) >$ luego necesariamente, debe ser nulo y por tanto $k_i = 0$. □

Obsérvese que si $\alpha \in F$ es trascendente sobre K entonces $K[X] \cong K[\alpha] \neq K(\alpha)$.

EJEMPLO 2.2:
- Consideremos la extensión $\mathbb{Q}(\sqrt{2})$ sobre $\mathbb{Q}$. Observemos que el polinomio $Irr(\sqrt{2}, \mathbb{Q}) = x^2 - 2$. Por tanto, $\mathbb{Q}(\sqrt{2}) \cong \frac{\mathbb{Q}}{<x^2-2>} \cong \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$
- El polinomio $p = x^4 - 10x^2 + 1 = (x - \sqrt{2} - \sqrt{3})(x - \sqrt{2} + \sqrt{3})(x + \sqrt{2} - \sqrt{3})(x + \sqrt{2} + \sqrt{3})$ y por tanto $\sqrt{2} + \sqrt{3}$ es algebraico en $\mathbb{Q}$. Además p es irreducible (para verlo utilícese la reducción a $\mathbb{Z}_3$)y mónico. En particular, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\}$. (ver Cox, pag. 78)

2.4. Relación entre extensiones finitas y algebraicas

Tenemos por tanto una gama de extensiones finitas determinadas por los $[K(\alpha) : K]$ con α algebraico, la pregunta es si estas extensiones son algebraicas. Vamos a ver que todas las finitas lo son.

Proposición 2.10.
Sea $\frac{F}{K}$ una extensión.

1. Si es finita, entonces es algebraica. Además, si $\alpha \in F$ entonces $gr(Irr(\alpha, K))|[F : K]$.
2. Es finita de grado $n \iff$ Es de generación finita con n generadores algebraicos.
3. Si es generado por generadores algebraicos (no necesariamente de forma finita) entonces es algebraica.

Demostración. 1. Sea $\alpha \in F$, supongamos que la extensión $\frac{F}{K}$ es finita. Entonces los elementos $\{1, \alpha, \cdots, \alpha^n\}$ son dependientes. Luego existe un polinomio no nulo $f = \sum_{i=0}^{n} k_iX^i$ del que α es raíz y por tanto α es algebraico.

Para la segunda parte, basta considerar la torre de cuerpos $K \subseteq K(\alpha) \subseteq F$ y observar que por el teorema de la torre de cuerpos las extensiones son finitas y se tiene que $[F : K] = [F : K(\alpha)][K(\alpha) : K] = [F : K(\alpha)]gr(Irr(\alpha, K))$ y por tanto, $gr(Irr(\alpha, K))|[F : K]$

2. $\Rightarrow$) Consideramos una base de F como K-espacio vectorial. Sea esta $\{\alpha_1, \cdots, \alpha_n\}$. Entonces $F = \{\sum a_i\alpha_i : a_i \in K\} \subseteq K(\alpha_1, \cdots, \alpha_n) \subseteq F$ y esto prueba que $F = K(\alpha_1, \cdots, \alpha_n)$. Por la proposición anterior tenemos que la extensión es algebraica y por tanto todos los α_i son algebraicos.

$\Leftarrow$) Sea $F = K(\alpha_1, \cdots, \alpha_n)$ y sean $K_i = K(\alpha_1, \cdots, \alpha_i)$. Tenemos que

$$K_i = F(\alpha_1, \cdots, \alpha_i) = F(\alpha_1, \cdots, \alpha_{i-1})(\alpha_i) = K_{i-1}(\alpha_i)$$

Observe ahora que como α_i es algebraico en K también es algebraico sobre $K_{i-1} \supseteq K$ luego

$$[K_i : K_{i+1}] = [K_{i-1}(\alpha_i) : K_{i-1}]$$

pero la última extensión es finita por el teorema de estructura como cociente para valores algebraicos. Como

$$[F : K] = \prod [K_i : K_{i-1}]$$

y cada factor es finito. Hemos acabado.

3. Si F es generado por generadores algebraicos sobre K α_i entonces tomemos un $\alpha \in F$ y veamos que necesariamente es algebraico. Lo que estamos diciendo es que todo elemento de F pertenece a $K(\{\alpha_i\})$ pero hemos visto que debe existir un subconjunto finito de α_i tal que $\alpha \in K(\alpha_{i_1}, \cdots, \alpha_{i_r})$. Esta extensión por el apartado anterior necesariamente es finita y por tanto es algebraica y por tanto α es algebraico sobre K. □

La pregunta es, ¿toda extensión algebraica es finita? La respuesta es que no. Véase, [1]

Proposición 2.11.
Sea $K \subseteq F \subseteq E$ una torre de cuerpos.

1. $\frac{E}{K}$ es una extensión algebraica $\iff$ $\frac{E}{F}, \frac{F}{K}$ es una extensión algebraica.
2. $\frac{E}{K}$ es una extensión finita $\iff$ $\frac{E}{F}, \frac{F}{K}$ es una extensión finita.

Sea $K \subseteq L \subseteq E$ y $K \subseteq F \subseteq E$ dos torres de cuerpos.

3. Si $\frac{L}{K}$ es una extensión algebraica entonces $\frac{LF}{K}$ es una extensión algebraica.
4. Si $\frac{L}{K}$ es una extensión finita entonces $\frac{LF}{K}$ es una extensión finita.

Sea $K \subseteq L \subseteq E$ y $K \subseteq F \subseteq E$ dos torres de cuerpos.

3. Si $\frac{L}{K}, \frac{F}{K}$ son extensiones algebraicas entonces $\frac{LF}{K}$ es una extensión algebraica.
4. Si $\frac{L}{K}, \frac{F}{K}$ son extensiones finitas entonces $\frac{LF}{K}$ es una extensión finita.

3. Cuerpos de descomposición

3.1. Herramientas previas

Proposición 3.1 (Teorema de Kronecker)**.**
Sea K un cuerpo y $f \in K[X]$ no constante entonces existe una extensión $\frac{F}{K}$ y un $\alpha \in F$ tal que $f(\alpha) = 0$.

Demostración. Podemos limitarnos al caso en que f sea irreducible. Ya que si g es un factor irreducible de f, toda raíz suya, es raíz de f. Demostrar que los irreducibles tienen raíces equivale a demostrar que los no constantes (no nulos, no unidades) tienen raíces.

Sea pues, f irreducible. Entonces, $F = \frac{K[X]}{\langle f \rangle}$ es un cuerpo. Consideramos la proyección canónica $\phi : K \to F$ tal que $a \mapsto a + \langle f \rangle$ que es un homomorfismo. Entonces identificamos K con $Img(\phi)$ y tenemos que F es un cuerpo extensión de K.

Haciendo $\alpha = x + \langle f \rangle$ si $f = \sum a_i X^i$ entonces

$$f(\alpha) = \sum (a_i + \langle f \rangle)(x + \langle f \rangle)^i = (\sum a_i x^i) + \langle f \rangle = f + \langle f \rangle = 0 + \langle f \rangle$$

Esto es $f(\alpha) = 0$. □

Definición 3.1 (Extensión de un homomorfismo)**.**
Sean $\frac{F_1}{K_1}, \frac{F_2}{K_2}$ extensiones de cuerpos y $\tau : F_1 \to F_2, \sigma : K_1 \to K_2$ homomorfismos. τ es una extensión de σ si $\tau|_{K_1} = \sigma$ y τ es un homomorfismo sobre K si $\sigma = 1_K$.

Proposición 3.2 (Propiedades de las extensiones de homomorfismos)**.**
Sea $\sigma : K_1 \to K_2$ un isomorfismo de cuerpos:

1. *Existe un único isomorfismo $\overline{\sigma}$ extensión de σ entre los anillos de polinomios tal que $X \mapsto X$.*

   Además, $\overline{\sigma}$ preserva grados e irreducibles.

   $$\begin{array}{ccc} K_1[X] & \overset{\overline{\sigma}}{\dashrightarrow} & K_2[X] \\ \vert & & \vert \\ K_1 & \xrightarrow{\sigma} & K_2 \end{array}$$

2. *Si $\tau : F_1 \to F_2$ es una extensión de σ entonces si $u \in F_1$ es raíz de $f \in K_1[X]$ entonces $\tau(u) \in F_2$*

   es raíz de $\overline{\sigma}(f) \in K_2[X]$.

   $$\begin{array}{ccccc} u \in F_1 & & \xrightarrow{\tau} & & F_2 \ni \tau(u) \\ \vert & & & & \vert \\ f \in K_1[X] & & \xrightarrow{\overline{\sigma}} & & K_2[X] \ni \overline{\sigma}(f) \\ \vert & & & & \vert \\ K_1 & & \xrightarrow{\sigma} & & K_2 \end{array}$$

3. *Sea f_1 un polinomio irreducible de K_1 con raíz $u_1 \in F_1$. Supongamos $u_2 \in F_2$ raíz de $f_2 = \overline{\sigma}(f_1)$. Entonces existe un único isomorfismo $\tau : K_1(u_1) \to K_2(u_2)$ sobre σ tal que $\tau(u_1) = u_2$.*

   Además el número de extensiones $\tau : K(u_1) \to F_2$ sobre σ es el número de raíces distintas de f_2

$$\begin{array}{ccc} u_1 \in F_1 & \text{———} & F_2 \ni u_2 \\ \Big| & & \Big| \\ K_1(u_1) & \overset{\tau}{\dashrightarrow} & K_2(u_2) \\ \Big| & & \Big| \\ f_1 \in K_1[X] & \xrightarrow{\overline{\sigma}} & K_2[X] \ni f_2 \end{array}$$

en F_2.

Demostración. Veamos cada una de las cuestiones.

1. Se trata de una aplicación de la propiedad universal del anillo de polinomios donde el homomorfismo que factoriza es la composición del homomorfismo σ con la inclusión de K_2 en $K_2[X]$ de modo que fijamos $X \in K_2[X]$ y por la propiedad existe un único homomorfismo tal que $X \to X$. Este homomorfismo es una extensión de σ ya que $\overline{\sigma} \circ p_1 = p_2 \circ \sigma$ donde p_i son las inmersiones en los anillos de polinomios. Se comprueba fácilmente que es un isomorfismo.

$$\begin{array}{ccc} K_1 & \xrightarrow{p_1} & K_1[X] \\ & \searrow^{p_2 \circ \sigma} & \downarrow \overline{\sigma} \\ & & K_2[X] \end{array}$$

   Es fácil observar que $\overline{\sigma}$ preserva grados ya que todo homomorfismo que nace en un cuerpo es inyectivo por tanto $\overline{\sigma}(\sum a_i X^i) = \sum \sigma(a_i) X^i$ y en particular la imagen del de mayor grado no es cero pues $Ker(\sigma) = \{0\}$.

   También preserva irreducibles. Sea $f \in K_1[X]$ irreducible y supongamos que $\overline{\sigma}(f)$ no lo es. Entonces sea $\overline{\sigma}(f) = \prod f_i$ una descomposición en factores irreducibles. Aplicando $\overline{\sigma}^{-1}$ entonces $f = \prod \overline{\sigma}^{-1}(f_i)$ y como los isomorfismos preservan el cero y las unidades se concluye que f no es irreducible. Por tanto, $\overline{\sigma}(f)$ debe ser irreducible.

2. Si $f = \sum a_i X^i$ entonces:

$$\overline{\sigma}(f)(\tau(u)) = \sum \sigma(a_i)(\tau(u))^i = \sum \tau(a_i)(\tau(u))^i = \tau(\sum a_i u^i) = \tau(0) = 0$$

3. Se hace el siguiente cálculo:

$$K(u_1) \cong \frac{K_1[X]}{\langle f_1 \rangle} \cong \frac{K_2[X]}{\langle f_2 \rangle} \cong K(u_2)$$

   Los isomorfismos de los extremos son únicos ya que provienen de una aplicación del primer teorema de isomorfía. Para ver que el isomorfismo de la mitad es único de nuevo hay que aplicar la propiedad universal del anillo cociente al siguiente diagrama:

$$\begin{array}{ccccc} K_1[X] & \xrightarrow{\overline{\sigma}} & K_2[X] & \xrightarrow{p} & \frac{K_2[X]}{\langle f_2 \rangle} \\ \downarrow{\scriptstyle p'} & & & \nearrow & \\ \frac{K_1[X]}{\langle f_1 \rangle} & & & & \end{array}$$

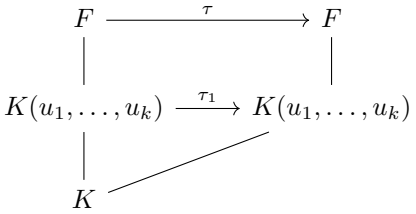
   Además por el estructura del isomorfismo está claro que es un isomorfismo sobre σ, esto es, preserva el valor de σ sobre los elementos de K_1.

   Por lo anterior, hay uno por cada raíz de f_2 pero no puede haber más porque la imagen de u_1 determina completamente el morfismo y porque la imagen de una raíz debe ser una raíz.

□

Corolario 3.3.

Todo endomorfismo sobre extensiones algebraicas F/K es un automorfismo .



Demostración. Sea $u_1 \in F$, $f = Irr(u, K)$ y u_i las raíces de f en F. Observemos que $K(u_1, \ldots, u_k)/K$ es finita ya que el cuerpo extensión es de generación finita mediante generadores algebraicos.

Por el apartado anterior, con $\sigma = 1|_K$ entonces tenemos que $\overline{\sigma}$ fija K y X luego fija todos los polinomios, es decir, es también la identidad. En consecuencia, $\tau(u_i) = u_j$. Pero además, como todo homomorfismo que nace en un cuerpo es inyectivo tenemos que τ induce una permutación de las raíces de modo que en la imagen están todas. Por tanto, τ induce un monomorfismo τ_1 en $K(u_1, \ldots, u_k)$.

Por otra parte, τ_1 es sobreyectiva ya que tenemos un monomorfismo de espacios vectoriales de dimensión finita. Por tanto, τ_1 es un automorfismo. De nuevo, τ es monomorfismo por nacer en un cuerpo y será sobreyectiva pues existe $v \in K(u_1, \ldots, u_k)$ tal que $u = \tau_1(v) = \tau_(v)$. □

3.2. Definición del cuerpo de descomposición

Definición 3.2 (Cuerpo de descomposición de un polinomio)**.**
Sea $f \in K[X]$ un polinomio no constante.

Una extensión $\frac{E}{K}$ es un cuerpo de descomposición de f sobre K si:

1. f factoriza en $F[X]$ como producto de polinomios lineales, $f = c\prod(X - \alpha_i)$ con $c \in K$ y $\alpha_i \in E$.
2. f no descompone en ningún subcuerpo intermedio, E es el menor cuerpo donde esto ocurre.

Proposición 3.4 (Existencia del cuerpo de descomposición)**.**
Sea $f \in K[X]$ un polinomio no constante de grado n y raíces α_i.

1. $E = K(\alpha_1, \ldots, \alpha_n)$ es un cuerpo de descomposición de f.
2. $[E : K] \leq n!$ donde n es el grado de f.

Demostración. Hagamos inducción sobre n. Si $n = 1$, $f = a_0x + a_1$ con $a_0 \neq 0$ y $a_0, a_1 \in K$. Haciendo $E = K = K(\alpha_1)$ entonces tomando $\alpha_1 = -a_1/a_0 \in K$ tenemos que $f = a_0(x - \alpha_1)$ y además $[F : K] = 1$.

Suponga el teorema cierto para $n-1$, por el teorema de Kronecker existe una raíz α_1 de f en un cuerpo extensión F y entonces $x - \alpha_1$ es un factor de f en $F[X]$ de modo que $f = (x - \alpha_1)g$ con $g \in F[X]$ de grado $n - 1$. Aplicando la hipótesis de inducción a g obtenemos una extensión de F_1, L, tal que $g = a_0\prod(x - \alpha_i)$ y por tanto, también f descompone en L además sabemos que $[L : F] \leq (n - 1)!$.

Esta descomposición $f = c\prod(x - \alpha_i)$ en L me dice que en $K(\alpha_1, \cdots, \alpha_n)$, f también descompone y claramente es la mínima extensión que lo verifica. Por tanto, $E = K(\alpha_1, \ldots, \alpha_n)$ es un cuerpo de descomposición para f y además como $[F(\alpha_1) : K] = gr(Irr(\alpha_1, F)) = n$ se tiene que

$$[L : K] = [L : F][F(\alpha_1) : K] \leq n!$$

□

Teorema 3.5 (Unicidad del cuerpo de descomposición)**.**
Sea $\sigma : K_1 \to K_2$ un isomorfismo de cuerpos. Sea F_1 el cuerpo de descomposición de $f \in K_1[X]$ y F_2 el cuerpo de descomposición de $\overline{\sigma}(f) \in K_2[X]$. Entonces $F_1 \cong F_2$ mediante un isomorfismo que extiende a σ.

$$\begin{array}{ccc} F_1 & \xrightarrow{?} & F_2 \\ | & & | \\ K_1 & \xrightarrow{\sigma} & K_2 \end{array}$$

Como consecuencia el cuerpo de descomposición de $f \in K[X]$ es único salvo isomorfismo sobre K.

Demostración. Por inducción sobre $n = gr(f)$. Obsérvese que siempre $gr(f) = gr(\overline{\sigma}(f))$ ya que probamos que el isomorfismo $\overline{\sigma}$ preserva grado.

Si $n = 1$ entonces $gr(f) = gr(\overline{\sigma}(f)) = 1$ y tenemos que $F_i = K_i$ de modo que nos sirve el propio σ como isomorfismo sobre σ.

Si $n > 1$ y supongamos el teorema cierto para polinomios de grado menor. Tomo $u_1 \in F_1$ raíz de f. Como $Irr(u_1, K)|f$ tenemos que $\sigma(Irr(u_1, K))|\sigma(f)$. Como $\overline{\sigma}$ preserva irreducibles, es claro que $\overline{\sigma}(Irr(u_1, K)|\overline{\sigma}(f)$ y podemos considerar una raíz suya u_2 que existe por ser F_2 el cuerpo de descomposición de $\overline{\sigma}(f)$. Por la proposición 3.2 con las herramientas auxiliares sabemos que existe un único isomorfismo $\sigma_1 : K(u_1) \to K(u_2)$ extensión de σ tal que $\sigma_1(u_1) = u_2$.

Ahora, aplicamos la hipótesis de inducción a los polinomios $f_i = (X - u_i)g_i$. F_i es un cuerpo de descomposición de g_i sobre $K_i(u_i)$ ya que como $X - u_i \in K_i(u_i)[X]$, el algoritmo de la división sobre cuerpos nos dice que $g_i \in K_i(u_i)[X]$ y claramente F_i contiene todas sus raíces. Por tanto, existe un isomorfismo extensión $\tau : F_1 \to F_2$ de σ_1 y como σ_1 también extiende a σ se deduce que τ extiende a σ.

Finalmente, si consideramos el isomorfismo identidad en K entonces obtenemos que hay un isomorfismo entre los posibles distintos cuerpos de descomposición de K. □

Corolario 3.6 (Finitud de la extensión del cuerpo de descomposición)**.**
El cuerpo de descomposición E de un polinomio no constante $f \in K[X]$ determina una extensión finita.

Demostración. En el teorema de existencia hemos probado que $[E : K] \leq n!$ y en el teorema de unicidad hemos demostrado que todos los cuerpos de descomposición son isomorfos. Pero el grado de una extensión se mantiene por isomorfismo. □

Corolario 3.7 (Elementos conjugados en cuerpos de descomposición)**.**
Sea $p \in K[X]$ irreducible con cuerpo de descomposición F. Sean $\alpha, \beta \in F$ raíces de p. Entonces existe un isomorfismo $\sigma : F \to F$ sobre K tal que $\alpha \mapsto \beta$.

Demostración. El proceso es el mismo que en la demostración anterior donde se toma $\sigma = Id$, de modo que las raíces u_i son raíces del mismo polinomio y claramente podemos elegir cualquier de ellas para el isomorfismo σ_1. □

3.3. Cuerpo de descomposición de una familia de polinomios

Definición 3.3.
Sea $\mathcal{F} \subseteq K[X]$ una familia de polinomios no constantes. Una extensión $\frac{E}{K}$ es un cuerpo de descomposición de $\mathcal{F}$ sobre K si para cualquier polinomio $f \in \{$ descompone en factores lineales y E es el menor cuerpo donde esto ocurre.

Proposición 3.8 (Existencia y unicidad del cuerpo descomposición de una familia)**.**
Sea K un cuerpo y $\mathcal{F}$ una familia de polinomios de $K[X]$.

1. *$E = K(\{u \in F : \exists f \in \mathcal{F}.f(u) = 0\})$ es un cuerpo de descomposición de $\mathcal{F}$.*
2. *El cuerpo de descomposición de una familia de polinomios sobre K es único salvo isomorfismo sobre K.*

4. Clausura algebraica

Definición 4.1 (Cuerpo algebraicamente cerrado)**.**
Un cuerpo es algebraicamente cerrado si verifica alguna de las siguientes propiedades.

Proposición 4.1 (Caracterización de los algebraicamente cerrados)**.**
Sea K un cuerpo. Son equivalentes:

1. *Todo polinomio $f \in K[X]$ no constante tiene al menos una raíz en K.*
2. *Todo polinomio $f \in K[X]$ no constante descompone en K.*
3. *Los polinomios irreducibles en $K[X]$ son los polinomios de grado 1.*
4. *K no tiene extensiones algebraicas propias.*

Demostración. 1. Se obtiene por inducción en el grado del polinomio y utilizando el algoritmo de la división de polinomios sobre un cuerpo.

2. Si $f \in K[X]$ fuera irreducible, no puede ser constante (pues entonces sería unidad) y por hipótesis descompone en factores lineales $f = \prod c(X - u_i)$ con $u_i \in k \wedge c \in K$. Pero los polinomios lineales son irreducibles en $K[X]$ y hemos obtenido una factorización de f en términos de irreducibles a menos que el número de factores sea 1 en cuyo caso $gr(f) = 1$.

3. Sea $\frac{E}{K}$ una extensión algebraica y $u \in E$. Como $Irr(u, K)$ es un polinomio irreducible, por hipótesis, debe ser $gr(f) = 1$, pero entonces $E = K$.

4. Sea $f \in K[X]$ un polinomio no constante, por el teorema de Kronecker existe una extensión donde f tiene una raíz α y entonces $\frac{K(\alpha)}{K}$ es una extensión algebraica y por hipótesis $K(\alpha) = K$ y claramente se tendrá que $\alpha \in K$.

□

Proposición 4.2 (Propiedades de los cuerpos algebraicamente cerrados)**.**
Se verifican las siguientes propiedades:

1. *Todo cuerpo algebraicamente cerrado es infinito.*
2. *Sea $\frac{E}{K}$ una extensión de cuerpos con E un cuerpo algebraicamente cerrado. Los elementos algebraicos de K forman un cuerpo algebraicamente cerrado.*

   Demostración. Veamos cada una de las propiedades:

   Si K es un cuerpo finito formo el polinomio $f(x) = \prod_{k \in K}(x - k) + 1$ que no tiene raíces en K y se deduce que el cuerpo no puede ser algebraicamente cerrado.

   b) Hemos en los ejercicios que el conjunto F de elementos de E que son algebraicos sobre K forma un cuerpo. para ver que es algebraicamente cerrado, tomo un polinomio $f \in F[X]$ no constante. Este polinomio sobre $E[X]$ debe tener una raíz ya que E es algebraicamente cerrado y la raíz $u \in E$ debe ser algebraica sobre F, completar con [3]

□

Definición 4.2 (Clausura algebraica)**.**
Una extensión de cuerpos $\frac{E}{K}$ es una clausura algebraica de K si:

1. $\frac{E}{K}$ es algebraica.

2. E es algebraicamente cerrado.

Dicho, de otro modo, la extensión es algebraica y no existe una extensión algebraica mayor.

Proposición 4.3 (Caracterización de la clausura algebraica)**.**
Dada una extensión $\frac{E}{K}$, son equivalentes:

1. *E/K clausura algebraica.*
2. *E/K algebraica y todo polinomio $f \in K[X]$ no constante descompone en factores lineales en $E[X]$.*
3. *E es cuerpo de descomposición de todos los polinomios no constantes de K.*
4. *E/K algebraica y todo polinomio no constante tiene una raíz en E.*

Demostración. Veamos que $1 \implies 2 \implies 3 \implies 1$ y dejaremos la equivalencia con 4 para más adelante:

1. Por defición $\frac{E}{K}$ es algebraica y todo polinomio no constante descompone en factores lineales por la caracterización de los cuerpos algebraicamente cerrados.
2. Sea $\mathcal{F}$ la familia de polinomios no constantes y sea S el conjunto de las raíces de los polinomios de $\mathcal{F}$. Como todo polinomio descompone en E claramente $E \supseteq S, K$ luego $E \supseteq K(S)$. Para ver la igualdad, obsérvese que como la extensión es algebraica todo elemento de E está en $K(S)$.
3. Claramente E es una extensión algebraica de K ya que $E = K(S)$ con S el conjunto de las raíces de los polinomios no constantes y las raíces son raíces de polinomios sobre K y los elementos de K son raíces de los polinomios sobre K, $X - k$.

   Vamos a ver que E no admite extensiones algebraicas propias. En efecto, supongamos un polinomio $g \in E[X]$ con cierta raíz $u \notin E$. Claramente, la extensión $\frac{E(u)}{E}$ es algebraica y como $\frac{E}{K}$ es algebraica tendremos que $\frac{E(u)}{K}$ es algebraica. Entonces el polinomio mínimo de u sobre K debe descomponer en E por ser E el cuerpo de descomposición de todos los polinomios no constantes sobre K, esto es, $f = Irr(u, K) = \prod(x - u_i)$. Como $f(u) = 0$ existirá un i tal que $u_i = u \in E$. Contradicción.

□

Proposición 4.4 (Invarianza de la clausura mediante extensiones algebraicas)**.**
Sea $\frac{F}{K}$ una extensión algebraica entonces $\overline{F} = \overline{K}$.

Demostración. Ser algebraicamente cerrado no depende del cuerpo base de la extensión. Por tanto, basta ver que una extensión es algebraica si y solo si lo es la otro. Pero sabemos que $\frac{E}{K}$ es algebraica $\iff$ $\frac{E}{F}, \frac{F}{K}$ son algebraicas y por hipótesis sabemos que $\frac{F}{K}$ es algebraica. □

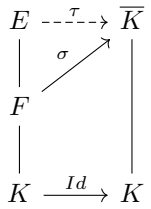
Teorema 4.5 (Teorema de Steinitz)**.**
Para todo cuerpo K existe una clausura algebraica $\overline{K}$.

Dos clausuras algebraicas de un mismo cuerpo son isomorfas sobre K.

Demostración. Sabemos que existe un cuerpo de descomposición para la familia de polinomios de grado mayor que 0 sobre K. Pero además por la caracterización de la clausura algebraica este cuerpo será la clausura algebraica de K.

Claramente, cualquiera dos algebraicas son cuerpos de descomposición de la familia de polinomios de grado mayor que 0 sobre K pero se ha visto que estos cuerpos de descomposición son isomorfos. □

Teorema 4.6 (Extensión de un homomorfismo a la clausura bajo extensiones algebraicas)**.**
Sea $K \subseteq F \subseteq E$ una torre de extensiones algebraicas. Sea $\overline{K}$ la clausura algebraica de K. Entonces todo homomorfismo $\sigma : F \to \overline{K}$ sobre K tiene una extensión $\tau : E \to \overline{K}$ (también sobre K).



Demostración. Aplicamos el lema de Zorn al conjunto

$$S = \{(E_i, \sigma_i) : F \subseteq E_i \subseteq E, \sigma_i : E_i \to \overline{K} \text{ sobre K }, \sigma_i|_F = \sigma\}$$

Este no es vacío ya que $(E, \sigma) \in S$ y está ordenado mediante el orden

$$(E_i, \sigma_i) \leq (E_j, \sigma_j) \iff E_i \subseteq E_j \wedge \sigma_j|_{E_i} = \sigma_i$$

Cualquier cadena totalmente ordenada está acotada superiormente. En efecto, si $E' = \cup E_i$ y definimos para $z \in E'$ $\sigma'(z) = \sigma_i(z)$ donde $z \in E_i$ tenemos una buena definición pues los homomorfismos se extienden unos a otros y por un razonamiento similar σ' es un homomorfismo [2] y claramente, (E', σ') es una cota superior. Por el lema de Zorn existe un elemento maximal del conjunto. Sea este (E_1, σ_1).

Veamos que $E_1 = E$ y que $\tau = \sigma_1$. En otro caso tomamos $u \in E \setminus E_1$ y entonces $gr(Irr(u, K)) \geq 2$ y busco una raíz distinta v de $Irr(u, K)$ en $\overline{K}$. Para llegar a una contradicción veo que construyo un homomorfismo de $E_1(u)$ en $\overline{K}$ que lleve una raíz en otra y veo que contiene a este propiamente. Los detalles están en el primer hecho destacado en [2]. No está claro que podamos usar los teoremas anteriores porque trabajan con extensiones de isomorfismos no de homomorfismos. □

Para entender la siguiente prueba hace falta la noción de cardinalidad de conjuntos. De forma intuitiva, la biyección de conjuntos define una relación de equivalencia en el conjunto de todos los conjuntos. Se llama número cardinal a una de estas clases de equivalencia.

En el conjunto de las clases de equivalencia se definen las siguientes operaciones:

1. $C_1 + C_2 = [A_1] + [A_2] = [A_1 \dot{\bigcup} A_2]$
2. $C_1 \times C_2 = [A_1] \times [A_2] = [A_1 \times A_2]$

Una referencia adecuada es el apéndice de [6].

Proposición 4.7 (Cardinalidad de la clausura algebraica)**.**
Sea K un cuerpo y $\overline{K}$ su clausura algebraica.

1. *Si K es finito, entonces la clausura es $\overline{K}$ es infinito numerable.*
2. *Si K es infinito entonces la clausura algebraica tiene el mismo cardinal que K.*

Demostración. Llamemos M_n al conjunto de todos los polinomios mónicos de grado n sobre K. Claramente, M_n y K^n son biyectivos. Además $K[X] = \dot{\bigcup} M_n$. En particular $|K[X]| = \sum_{n \in \mathbb{N}} |M_n|$.

La extensión $\frac{\overline{K}}{K}$ es algebraica y en general tenemos una cota dada por $|K[X]||\mathbb{N}|$ ya que si S denota a las raíces de los polinomios no constantes con coeficientes en K entonces $\overline{K} \subseteq S$

1. Si K es un cuerpo finito observamos que $\overline{K}$ no puede ser finita. Esto es así porque si $\overline{K}$ fuera finita con p elementos, entonces sus elementos serían raíces de $X^p - X$ y por tanto $X^p - X$ no puede tener raíces en $\overline{K}$ y esto contradice que $\overline{K}$ es algebraicamente cerrado. Por tanto, el cardinal de $\overline{K}$ no puede ser finito.

   Observemos que si K es finito entonces $|K[X]| = |K| \sum_{n\in\mathbb{N}} |M_n|$ donde M_n es el conjunto de los polinomios mónicos de grado n. Pero $|M_n| = |K|^n$ y tenemos claramente que $|K[X]|$ es numerable. Por la cota anterior sabemos que $|\overline{K}| = |K[X]||\mathbb{N}|$ y por tanto, $\overline{K}$ es numerable.

2. Si K es infinito, $|K|^n = |K|$ y entonces $|K[X]| = |K|$. De nuevo por nuestra cota tendremos que $|\overline{K}| = |K|$.

□

5. Extensiones normales

5.1. Extensiones conjugadas

Definición 5.1 (Elementos conjugados sobre un cuerpo)**.**
Sea K un cuerpo.

$u, v \in \overline{K}$ son conjugados sobre K si se verifica alguna de las siguientes condiciones equivalentes.

Proposición 5.1 (Caracterización de elementos conjugados)**.**
Sean $u, v \in \overline{K}$. Entonces:

1. *$Irr(u, K) = Irr(v, K)$.*
2. *$\exists \sigma : K(u) \to K(v)$ isomorfismo sobre K tal que $\sigma(u) = v$*
3. *$\exists \sigma : K(u) \to \overline{K}$ homomorfismo sobre K tal que $\sigma(u) = v$*
4. *$\exists \sigma : \overline{K} \to \overline{K}$ automorfismo sobre K tal que $\sigma(u) = v$*

Demostración. Veamos circulamente las implicaciones.

1. $K(u) \cong \frac{K[X]}{\langle f(X) \rangle} \cong K(v)$. Este isomorfismo deja invariante a K pues la evaluación de una constante es la constante.
2. Basta tomar como codominio $\overline{K}$.
3. Como $\overline{K}$ es la clausura algebraica de K por la invarianza de la clausura mediante extensiones algebraicas también es clausura algebraica de $K(u)$, en particular, la extensión $\frac{\overline{K}}{K(u)}$ es algebraica. En estas condiciones teníamos que se podía extender el homorfismo desde la extensión algebraica $\overline{K}$ hasta la clausura algebraica $\overline{K}$. Pero todo endomorfismo sobre extensiones algebraicas es automorfismo.
4. Trabajamos con la extensión del automorfismo σ a anillos de polinomios $\overline{\sigma}$. Sea $f = Irr(u, K) = \sum a_i X^i$. Entonces
$$0 = \overline{\sigma}(f(u)) = \sum \sigma(a_i)\sigma(u)^i = \sum a_i v^i$$
como este isomorfismo lleva irreducibles en irreducibles pues también $f = Irr(v, K)$.

□

Definición 5.2 (Extensiones conjugadas)**.**
Dos extensiones algebraicas $\frac{F_1}{K}, \frac{F_2}{K}$ son conjugadas si ocurre cualquiera de las condiciones de la siguiente proposición.

Proposición 5.2.
Dadas dos extensiones algebraicas $\frac{F_1}{K}, \frac{F_2}{K}$ son equivalentes:

1. *Existe un isomorfismo $\sigma : F_1 \to F_2$ sobre K.*
2. *Existe un homomorfismo $\sigma : F_1 \to \overline{K}$ sobre K tal que $\sigma(F_1) = F_2$.*
3. *Existe un isomorfismo $\sigma : \overline{K} \to \overline{K}$ sobre K tal que $\sigma(F_1) = F_2$.*

5.2. Extensiones normales

Definición 5.3 (Extensión normal)**.**
Una extensión normal $\frac{F}{K}$ es un subcuerpo de la clausura de K que determina una extensión algebraica y tal que se verifica alguna de las siguientes condiciones.

Proposición 5.3 (Condiciones equivalentes para extensión normal)**.**
Dada una extensión algebraica $\frac{F}{K}$ tal que F un subcuerpo de la clausura de K. Son equivalentes:

1. *Para todo homomorfismo $\sigma : F \to \overline{K}$ sobre K se verifica que $\sigma(F) = F$, es decir, todo homomorfismo de la extensión a la clausura factoriza como automorfismo por la extensión.*
2. *Todo polinomio irreducible sobre K que tiene una raíz en F descompone en factores lineales en $F[X]$.*
3. *F es el cuerpo de descomposición de una familia de polinomios.*

Demostración. Veamos las implicaciones de forma circular:

1. Sea f un irreducible con $u \in F$ raíz. Si f no es lineal entonces tendrá alguna raíz v en un cuerpo extensión. Pero las raíces del mismo irreducible son elementos conjugados sobre K y por tanto existe un automorfismo $\sigma : \overline{K} \to \overline{K}$ sobre K tal que $\sigma(u) = v$.

   $\sigma|_F$ es un homomorfismo y como todo homomorfismo de F a la clausura deja fijo a F, en particular, $v \in F$. Se procede por inducción para demostrar que f descompone en lineales sobre $F[X]$.

2. Dada $u \in F$, por hipótesis, $Irr(u, F)$ tiene todas sus raíces en F. Claramente, F será el cuerpo de descomposición de los polinomios mínimos de sus elementos, no pudiendo estos descomponer en ningún subcuerpo intermedio.

3. Sea S las raíces de la familia de polinomios que tiene a F como su cuerpo de descomposición. Entonces $F = K(S)$.

   Sea $\sigma : F \to \overline{K}$ un homomorfismo sobre K. $\sigma(F) \subseteq F$ ya que $\sigma(K) = K$, de modo que σ extiende a la identidad, y por tanto dado un polinomio f de los generadores del cuerpo de descomposición, $\overline{\sigma}(f) = f$ y si tomo una raíz u de f entonces $\sigma(u)$ es raíz de ese mismo polinomio. Por tanto, σ se puede ver como un endomorfismo en F. Como las extensiones son algebraicas, todo endomorfismo es automorfismo y por tanto $\sigma(F) = F$.

□

Proposición 5.4 (Extensiones normales finitas)**.**
Sea $\frac{E}{K}$ una extensión de cuerpos.

E es el cuerpo de descomposición de un polinomio $p \in K[X] \iff \frac{E}{K}$ es normal y finita.

Demostración. $\Rightarrow$) Si E es un cuerpo de descomposición de un polinomio en K entonces $\frac{E}{K}$ es finita ya que es de generación finita mediante generadores algebraicos y además es normal pues es el cuerpo de descomposición de una familia (con un elemento) de polinomios.

$\Leftarrow$) Si la extensión es finita de nuevo debe ser generada por una colección finita de elementos algebraicos sobre K. Denotemos $Irr(\alpha_i, K)$ al polinomio mínimo de α_i sobre K. Este polinomio es irreducible y tiene una raíz en F por tanto, descompone en F completamente. Entonces basta considerar $f = \prod Irr(\alpha_i, K)$ y ver que su cuerpo de descomposición tiene que ser exactamente igual a E. □

EJEMPLO 5.1: Veamos que $\mathbb{Q}(\sqrt[3]{2})$ no es el cuerpo de descomposición de ningún polinomio de $\mathbb{Q}[X]$.

Tengo que el polinomio x^3-2 es irreducible sobre $\mathbb{Q}[X]$ y tiene una raíz sobre $\mathbb{Q}(\sqrt[3]{2})$, entonces por la proposición anterior, forzaríamos a que X^3-2 descompusiera completamente sobre $\mathbb{Q}(\sqrt[3]{2})$. Pero esto no es posible ya que este cuerpo se queda en $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$ y en particular no contiene a las raíces complejas $\omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$.

Proposición 5.5 (Propiedades de las extensiones normales)**.**
Se verifican las siguientes propiedades:

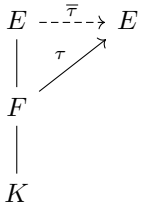
1. *Sea $\frac{E}{K}$ una extensión normal y $\frac{F}{K}$ una extensión algebraica. Entonces la extensión $\frac{EF}{F}$ es una extensión normal.*
2. *Sea $K \subseteq F \subseteq E$ una torre de cuerpos con $\frac{E}{K}$ normal. Entonces $\frac{E}{F}$ es una extensión normal.*
3. *Sean $\frac{F_1}{K}, \frac{F_2}{K}$ dos extensiones normales. Entonces $\frac{F_1F_2}{K}$ es una extensión normal.*
4. *Sea $\frac{F_\lambda}{K}$ con $\lambda \in \Lambda$ una familia de extensiones normales y sea $E = \cap_\lambda F_\lambda$ entonces la extensión $\frac{E}{K}$ es normal.*

Demostración.

1. Si $\sigma : EF \to \overline{F}$ es un homomorfismo sobre F entonces $\sigma(EF) = \sigma(E)\sigma(F) = EF$ y por tanto la extensión $\frac{EF}{F}$ es normal. Obsérvese que lo anterior es valído ya que todo homomorfismo que sale de un cuerpo es monomorfismo y que también hemos utilizado la preservación de la clausura mediante extensiones algebraicas de modo que $\overline{F} = \overline{K}$ y en particular hemos podido utilizar la propiedad de normalidad de E.
2. Sea $\sigma : E \to \overline{F}$ un homomorfismo sobre F. Tenemos que observar que como $\frac{E}{K}$ es normal en particular asumimos que es una extensión algebraica. Esto nos dice que, en particular, $\frac{F}{K}$ es algebraica y gracias a esto podemos aplicar la invarianza de la clausura mediante extensiones algebraicas para deducir que $\overline{F} = \overline{K}$. Entonces $\sigma : E \to \overline{K}$ es un homomorfismo que en particular fija K. Por ser $\frac{E}{K}$ una extensión normal se tiene que verificar que $\sigma(E) = E$ y por tanto, $\frac{E}{F}$ es normal.
3. Si $\sigma : EF \to \overline{K}$ es un homomorfismo sobre K entonces $\sigma(EF) = \sigma(E)\sigma(F) = EF$ y por tanto la extensión $\frac{EF}{K}$ es normal. Obsérvese que lo anterior es valído ya que todo homomorfismo que sale de un cuerpo es monomorfismo.
4. Si $\sigma : \cap F_k \to \overline{K}$ es un homomorfismo sobre K entonces, como la intersección arbitraria de cuerpos es un cuerpo, el homomorfismo es inyectivo y por tanto respecta intersecciones. Por tanto, $\sigma(\cap F_k) = \cap\sigma(F_k) = \cap F_k$ por la normalidad de los F_k.

□

Teorema 5.6 (Extensión de homomorfismos a una extensión normal)**.**
Sea $K \subseteq F \subseteq E$ una torre de cuerpos con $\frac{E}{K}$ normal. Entonces todo homomorfismo $\tau : F \to E$ sobre K se extiende a un automorfismo $\overline{\tau} : E \to E$.



Demostración. Sea $\tau : F \to E$ un homomorfismo. Cambiamos el codominio por $\overline{K}$ y seguimos teniendo un homomorfismo. Pero, ya que $\frac{E}{K}$ es algebraica por ser normal, podemos extender el homomorfismo a $\tau : E \to \overline{K}$. Finalmente, por la normalidad este homomorfismo verifica que $\tau(E) = E$. De modo que tenemos un endomorfismo $\tau : E \to E$ y todo homomorfismo de extensiones algebraicas es un automorfismo. □

5.3. Clausura normal

Definición 5.4 (Clausura normal)**.**
Sea $\frac{F}{K}$ una extensión algebraica, la clausura normal de $\frac{F}{K}$ es una extensión $\frac{E}{K}$ con

$$E = \cap\{H : H \supseteq F \wedge \frac{H}{K} \text{ es normal}\}$$

En otros términos, la clausura normal es la menor extensión normal que contiene a F.

Proposición 5.7 (Existencia y unicidad de la clausura normal)**.**
1. Para toda extensión algebraica $\frac{F}{K}$ existe una clausura normal $\frac{E}{K}$.
2. Dos clasuras normales de de la extensión algebraica $\frac{F}{K}$ están relacionadas mediante un isomorfismo sobre F.

Demostración. 1. La existencia se sigue del de que la intersección que define a la clausura normal es no vacía ya que $\overline{K}$ siempre define una extensión normal utilizando que es algebraica y que todo endomorfismo será un automorfismo.

2. La unicidad se sigue de la unicidad de las clausuras algebraicas. En efecto, si tengo dos clausuras normales E_1, E_2 entonces como son algebraicas existe una extensión sobre K a las clausuras que contengan a E_1, E_2. Sean $\overline{K}_1, \overline{K_2}$ estas clausuras y σ, σ' los respectivos homomorfismos desde los E. Observamos que $\overline{K}_1 \cong \overline{K_2}$ y denotamos por τ al isomorfismo.

Entonces $\sigma(K) = K \wedge \sigma'(K') = K'$, como la normalidad se preserva por isomorfismo tenemos que $\tau(K) \cap K'$ es normal sobre F y como $\tau(K) \cap K' \cap K'$ y K' es una clausura normal, necesariamente $\tau(K) = K'$ (si no no sería la menor). Es decir, tenemos que ambas clausuras son isomorfas. □

Proposición 5.8 (Clausura de una extensión de finita)**.**
Sea $F = K(u_1, \ldots, u_n)$ y $f_i = Irr(u_i, K)$.

La clausura normal de F es el cuerpo de descomposición del polinomio $f = \prod f_i$.

Como consecuencia toda clausura normal de una extensión finita determina una extensión finita.

Demostración. El cuerpo de descomposición del polinomio $\prod f_i$ determina una extensión normal y finita. Por ser finita, la consecuencia esta clara.

Toda clausura normal, debería contener a las raíces de los f_i pues todo polinomio irreducible que tenga sus raíces en la clausura debe descomponer totalmente. Además la clausura normal contiene al cuerpo al que se refiere. En definitiva, el cuerpo de descomposición es la menor extensión normal candidata a ser clausura. □

Claramente, la clausura algebraica determina una extensión normal. El carácter de normalidad se preserva mediante reducciones locales de este concepto.

Proposición 5.9 (Subextensiones de una extensión normal)**.**
Sea $K \subseteq F \subseteq E$ una torre de extensiones algebraicas con $\frac{E}{K}$ una extensión normal. Entonces:

$$\frac{F}{K} \text{ es normal } \iff \forall \sigma : E \to E \text{ sobre } K \text{ verifica que } \sigma(F) = F$$

Demostración. $\Rightarrow$) Dado $\sigma : E \to E$ sobre K se extiende a la clausura y se restringe a F, por la normalidad $\sigma(F) = F$.

$\Leftarrow$) Dado un homomorfismos $\sigma : F \to \overline{K}$ por ser $\frac{E}{K}$ algebraica podemos extenderlo hasta E. Esta extensión $\overline{\sigma}$ verifica que preserva E y en estas condiciones las hipótesis implican que $F = \overline{\sigma}(F) = \sigma(F)$. □

5.4. Polinomio normal

Definición 5.5 (Polinomio normal)**.**
Un polinomio irreducible es normal si ocurre alguna de las condiciones de la siguiente proposición.

Proposición 5.10 (Condiciones equivalentes para que un polinomio sea normal)**.**
Sea $f \in K[X]$ un polinomio irreducible. Las siguientes propiedades son equivalentes:

1. *En toda extensión algebraica F/K con una raíz de f, f descompone en factores lineales.*
2. *El cuerpo de descomposición de f sobre K es $K(u)$ con u una raíz arbitraria de f.*
3. *Todas las raíces de f se expresan como polinomios en una cualquiera de ellas.*

Demostración.

1. Tenemos que en $K(u)/K$ para u una raíz de f es una extensión algebraica que contiene una raíz de f, por tanto, f descompone en factores lineales. Claramente, ninguna extensión intermedia podría ser cuerpo de descomposición pues debería contener a alguna raíz que por la inclusión debería ser u.
2. Como $K(u)$ es el cuerpo de descomposición se sigue que todas las raíces están en $K(u)$ y por tanto, se expresan a priori como expresiones fraccionarias en u. Sin embargo, por las propiedades del polinomio mínimo sabemos que $K(u) = K[u]$ y por tanto, la expresión es en términos polinómicos.
3. Cualquier extensión algebraica con una raíz u contendría a $K(u)$. Como todas las raíces se expresan como polinomios en u la extensión contendría a todas las raíces y entonces f descompodría en polinomios lineales.

□

6. Extensiones separables y cuerpos perfectos

6.1. Característica y derivada

Proposición 6.1.
Sea A un anillo. Entonces existe un único homomorfismo $f : \mathbb{Z} \to A$ tal que $f(1) = 1 \wedge f(n) = n \cdot 1$.

Demostración. Defino $f : \mathbb{Z} \to A$ como $n \to n \cdot 1$. f está bien definido ya que si $n \in \mathbb{N}$ entonces $n \cdot 1$ está de forma natural definiado y si $n \in \mathbb{Z}$ entonces $n1 = (-n)(-1)$ también está naturalmente definido.

Por otro lado, $f(1) = 1 \cdot 1 = 1$ y es un homomorfismo ya que

$$f(n+m) = (n+m) \cdot 1 = n \cdot 1 + m \cdot 1 = f(n) + f(m)$$

Claramente cualquier otro homomorfismo verificando las condiciones sería igual a f. □

Definición 6.1 (Característica de un anillo)**.**
Sea A un anillo. Consideramos el homomorfismo característico $f : \mathbb{Z} \to A$ tal que $n \mapsto n \cdot 1$. Definimos la característica de K como el generador del ideal $Ker(f)$. Lo denotamos por $Car(A)$.

Proposición 6.2 (Propiedades de la característica)**.**
Sea A un anillo. Se verifican las siguientes propiedades:

1. *$Car(A)$ es el menor número entero positivo o nulo n tal que $\forall a \in A. n \cdot a = 0$.*
2. *Si $Car(A) = 0$ entonces $f(\mathbb{Z}) \cong \mathbb{Z}$. Si $n = Car(A) \neq 0$ entonces $f(\mathbb{Z}) \cong \mathbb{Z}_n$ y además $\forall a \in A. na = 0$.*
3. *Si A es un dominio de integridad entonces $Car(A)$ es cero o un número primo.*
4. *Sea A un anillo de característica prima p entonces la aplicación $R(a) = a^p$ es un endomorfismo conocido como endomorfismo de Frobenius.*
5. *Si $f : A \to B$ es un homomorfismo entonces $car(B)|car(A)$.*

Demostración.

1. No puede haber ningún elemento menor que él que anule a todos pues entonces generaría al núcleo.
2. Utilícese el primer teorema de isomorfía y la definición de característica.
3. Si $Car(A) = 0$ hemos acabado. Si $n = Car(A) \neq 0$ entonces si n no fuera primo, $0 = n \cdot 1 = (n_1 n_2) \cdot 1 = (n_1 \cdot 1)(n_2 \cdot 1) \implies n_1 \cdot 1 = 0 \vee n_2 \cdot 1 = 0$ donde hemos utilizado la propiedad asociativa general.
4. Escribamos $(\alpha+\beta)^p = \alpha^p + \beta^p + \sum \binom{p}{i} \alpha p - i\beta^i$ con $1 \leq i \leq p-1$. Claramente, p divide a cada uno de los coeficientes binomiales y como F tiene característica p, se deduce que $(\alpha + \beta)^p = \alpha^p + \beta^p$. Las otras propiedades son triviales.
5. $0 = f(0) = f(1Car(A)) = 1Car(A)$ y como $Car(B)$ debe ser el mínimo que anule a uno, tendrá que ser $Car(B)|Car(A)$.

□

Definición 6.2 (Subanillo característico)**.**
Sea A un anillo y f el homomorfismo característico de A.

El subanillo característico de A, S, es la intersección de todos los subanillos de A. Equivalentemente, S es el menor subanillo que contiene a $f(\mathbb{Z})$.

Proposición 6.3 (Clasificación del subanillo característico)**.**
La característica clasifica al subanillo característico:

1. $Car(A) = 0 \iff \cong \mathbb{Z}$
2. $Car(A) = n > 0 \iff S \cong \mathbb{Z}_n$

Definición 6.3 (Subcuerpo característico)**.**
Sea K un cuerpo y f el homomorfismo característico de K.

El subcuerpo característico de A, C es la intersección de todos los subcuerpos de K. Equivalentemente, C es el menor subcuerpo que contiene a $f(\mathbb{Z})$.

Obsérvese que en la definición anterior, C sería el cuerpo de fracciones del dominio de integridad S, subanillo característico de K.

Proposición 6.4 (Clasificación del subcuerpo característico)**.**
La característica clasifica al subcuerpo característico:

1. $Car(K) = 0 \iff C \cong \mathbb{Q}$
2. $Car(K) = p \neq 0 \iff C \cong \mathbb{Z}_p$ *con p un entero primo positivo.*

Definición 6.4 (Derivada de un polinomio)**.**
La derivada de un polinomio $f = \sum a_i X^i$ es $Df = \sum i a_i X^{i-1}$

Definición 6.5 (Multiplicidad de una raíz)**.**
Sea $f \in K[X]$ un polinomio. $u \in F$ una raíz de f en alguna extensión F tienen multiplicidad k si $f = (X-u)^k f_1$ con $f_1(u) \neq 0$.

Decimos que u es una raíz simple si $k = 1$ y que u es una raíz múltiple si $k > 1$.

6.2. Separabilidad

Proposición 6.5 (La separabilidad es invariante frente al cuerpo de descomposición)**.**
La multiplicidad de las raíces de un polinomio no depende del cuerpo de descomposición.

Demostración. Supongamos que $f \in K[X]$ es un polinomio no constante y descompone como

$$f(X) = \prod (X - \alpha_i)^{m_i} = \prod (X - \beta_i)^{n_i}$$

donde se entiende que las raíces son distintas y los exponentes son sus multiplicidades.

Recordemos que los cuerpos de descomposición son isomorfos por un isomorfismo τ sobre K. La extensión canónica $\overline{1_K}$ de la identidad a polinomios da la identidad. Por tanto, τ, que extiende a K y es isomorfismo debe llevar las raíces $\{\alpha_i\}$ en raíces $\{\alpha_i\}$. Pero τ es inyectiva y tenemos sobre las raíces, que forman un conjunto finito, una aplicación inyectiva. Por tanto debe ser sobreyectiva. Lo que se tiene es una permutación de las raíces.

Que la multiplicidad no varía se deduce de que el homomorfismo extendido a polinomios no varía grados. □

Lema 6.6 (Criterio de raíces simples)**.**
Sea $f \in K[X]$ un polinomio no constante.

Las raíces de f son todas simples $\iff$ f, Df son primos relativos.

Demostración. $\Rightarrow$) Si todas las raíces de $f(X)$ son simples, en un cuerpo de descomposición:

$$f(X) = a\prod_{i=1}^{r}(X-\alpha_i) \text{ con } \alpha_i \text{ distintos y } Df(X) = a\sum_{i=1}^{r}(X-\alpha_1)\dots(X-\alpha_{i-1})(X-\alpha_{i+1})\dots(X-\alpha_r)$$

Es claro que como $K[X]$ es un DFU, los polinomios de grado 1 determinan clases de asociación irreducibles distintas. Recordando que $mcd(f,g) = \prod_{p\in\mathcal{P}} p^{min(e(p,f),e(p,g)}$ con $\mathcal{P}$ un conjunto de representantes de los irreducibles para la relación de asociación, bastará ver que ningún factor de f es factor de Df. Esto es sencillo ya que cada $(X-\alpha_i)$ divide a todos los sumandos de $Df(X)$ salvo a uno que no puede dividir porque no coincide con ninguno de los factores.

En consecuencia, $mcd(f, Df) = 1$.

$\Leftarrow$) Se procede por contrarrecíproco. Supongamos que f tiene una raíz múltiple α de multiplicidad $m \geq 2$ y sea $d(X) = mcd(f(X), Df(X))$. En el cuerpo de descomposición podemos escribir:

$$f(X) = (X-\alpha)^m g(X) \text{ y } Df(X) = (X-\alpha)^m Dg(X) + m(X-\alpha)^{m-1}g(X)$$

Por tanto, en el cuerpo de descomposición $(X-\alpha)$ es un factor común de f y Df, con lo que $d(X) \neq 1$. Bastaría entonces con observar que el máximo común divisor de dos polinomios no depende del cuerpo extensión. Para ello observaremos que f, g se escriben del mismo modo en la extensión (aunque sean factorizables) y por tanto, el algoritmo de Euclides no varía, obteniéndose en particular los mismos resultados. □

Lema 6.7 (Multiplicidad de las raíces de un irreducible)**.**
Todas las raíces de un irreducible tienen la misma multiplicidad.

Demostración. La prueba aparece en el libro de Gallian. Básicamente, tenemos un polinomio $f \in K[X]$ irreducible y nos vamos a un cuerpo de descomposición. Sabemos que dos cuerpos de descomposición son isomorfos y como corolario obtuvimos que dadas dos raíces de un polinomio irreducible (para que la extensión de la identidad me de el mismo polinomio en la imagen) existirá un isomorfismo del cuerpo de descomposición que me lleve una raíz en otra. Sea ϕ este isomorfismos entonces si $f(X) = (X-\alpha)^m g(X)$:

$$f(X) = \phi(f(X)) = (X-\beta)^m \phi(g(X))$$

Esto prueba que la multiplicidad de α es menor o igual que la multiplicidad de β. Intercambiando los papeles de α, β se obtiene la otra desigualdad. □

Definición 6.6 (Separabilidad)**.**
Sea K un cuerpo.

1. Un polinomio $p \in K[X]$ es separable si sus factores irreducibles sobre K tienen todas sus raíces simples.
2. Un elemento algebraico u sobre un cuerpo K es separable si $Irr(u, K)$ no tiene raíces múltiples.

3. Una extensión algebraica $\frac{F}{K}$ es separable si todos los elementos de F son separables sobre K.

Corolario 6.8 (Separabilidad de irreducibles según la característica)**.**
Sea K un cuerpo.

1. *Si $Car(K) = 0$ entonces todo irreducible no constante es separable.*
2. *Si $Car(K) = p \neq 0$ con p un número primo positivo y f un irreducible no constante entonces:*
   a*) f es separable $\iff Df \neq 0$.*
   b*) f no es separable $\iff f(X) = g(X^p)$ es un polinomio en X^p.*

Demostración. 1. Sea f un polinomio irreducible sobre un cuerpo de característica 0. Por ser irreducible $mcd(f, Df) = Df$ o $mcd(f, Df) = 1$. El primer caso, no puede darse pues entonces $Df|f$ y como Df es de grado menor tendríamos una factorización propia de f, de modo que no sería irreducible. En el segundo caso, tendríamos por el criterio de raíces simples que f es separable.

2. $\Leftarrow$) Si $Df \neq 0$ entonces $mcd(f, Df) = f, 1$ por ser f irreducible. Pero f no puede dividir a Df por ser f de grado mayor. Por tanto, $mcd(f, Df) = 1$ y las raíces son simples.

   $\Rightarrow$) Por contrarrecíproco, si $Df = 0$ entonces $mcd(f, Df) = mcd(f, 0) = f$ y como f es irreducible se tiene que las raíces f no son todas simples, esto es, que existe al menos una raíz múltiple.

   Para ver que $f = g(X^p)$ escribimos $f = \sum a_i X^i$ y $Df = \sum i a_i X^{i-1}$. Como $Df = 0$ tendremos que $ia_i = 0$. Como $K[X]$ es un dominio de integridad de característica p para cada índice tal que $p \nmid i$ se tendría que $a_i = 0$ y entonces f se escribe como $f = a_0 + a_p(X^p) + \ldots + a_{p^r}(X^p)^r$.

   Recíprocamente la derivada de este polinomio es 0 ya que todos los monomios quedan afectados por un múltiplo de p y la característica anula a todos los elementos del anillo.

□

Damos ahora otra caracterización de la separabilidad para cuerpos de característica prima.

Teorema 6.9 (Caracterización de separabilidad en característica prima)**.**
Sea K un cuerpo de característica prima p no nula.

Todo irreducible no constante es separable $\iff$ el endomorfismo de Frobenius es un automorfismo.

Demostración. Veamos cada implicación:

$\Rightarrow$) Consideramos $a \in K$ y el polinomio $f = X^p - a$. Si α es una raíz de f en un cuerpo de descomposición F, entonces en ese cuerpo f debe descomponer como $f = (X - \alpha)^p$ ya que estamos en característica p. Por tanto, cada factor irreducible sobre K de f tiene también una única raíz α que a priori podría ser múltiple. Pero por hipótesis, debe ser simple y el único factor irreducible de f resulta ser $X - \alpha$. Por tanto, $\alpha \in K$ y $a = \alpha^p$ de donde el endomorfismo de Frobenius es sobreyectivo y por tanto es automorfismo.

$\Leftarrow$) Por reducción al absurdo, si f es irreducible no constante con $Df = 0$ entonces tiene raíces múltiples y en particular $f = g(X^p)$.

Escribamos $g = \sum b_i X^i$. Entonces, si el endomorfismo de Frobenius fuera automorfismo entonces $b_i = c_i^p$ y en particular $f = (\sum c_i X^i)^p$ de modo que no sería irreducible. Esto es una contradicción. Por tanto, $Df \neq 0$ y todas las raíces son simples. □

Establecemos ahora un lema que permite descomponer torres separables para dar un ejemplo extra de cuerpos perfectos. Posteriormente daremos la otra implicación.

Proposición 6.10 (Descomposición de torres separables y algebraicas)**.**
Sea $E \supseteq F \supseteq K$ una torre algebraica de cuerpos.

Si $\frac{E}{K}$ separable entonces $\frac{E}{F}, \frac{F}{K}$ son separables.

Demostración. F/K es separable ya que cada elemento $\alpha \in F$ está en E y por tanto es separable sobre K.

Sea ahora $\beta \in E$ entonces $Irr(\beta, F)|Irr(\beta, K)$ y como $Irr(\beta, K)$ es separable, también lo será $Irr(\beta, F)$. Por tanto, β es separable sobre F. □

6.3. Cuerpos perfectos

Definición 6.7 (Cuerpo perfecto)**.**
Un cuerpo K es perfecto si se cumplen alguna de las condiciones de la siguiente proposición.

Proposición 6.11 (Criterios de cuerpo perfecto)**.**
Sea K un cuerpo. Las siguientes condiciones son equivalentes:

1. *Todo polinomio $p \in K[X]$ es separable.*
2. *Toda extensión algebraica sobre K es separable.*
3. *Toda extensión finita sobre K es separable.*
4. *$Car(K) = 0 \vee Car(K) = p$ prima y el endomorfismo de Frobenius es sobreyectivo.*

Demostración. Vamos a ver de forma circular, $1, 2, 3$ y luego $1 \iff 4$.

1. Si F/K es una extensión algebraica entonces para cada $\alpha \in F$, $Irr(\alpha, K)$ es un polinomio separable sobre K. Luego α es un elemento separable sobre K y por tanot F/K es separable.
2. Ya que toda extensión algebraica es separable.
3. Si f es un polinomio irreducible no constante y F es su cuerpo de descomposición entonces F/K es una extensión finita ($[F : K] \leq gr(f)!$) y por tanto es separable. Como consecuencia, cada raíz de f es separable y por tanto, f es un polinomio separable.
4. Veamos que $1 \iff 4$. Basta observar que la característica de un dominio de integridad es 0 o prima no nula. Si $Car(K) = 0$ entonces todo polinomio es separable y si $Car(K) = p$ entonces todo polinomio es separable si y sólo si el endomorfismo de Frobenius es sobreyectivo (ya que siempre es inyectivo por nacer en un cuerpo).

□

Proposición 6.12 (Ejemplos de cuerpos perfectos)**.**
Los siguientes cuerpos son cuerpos perfectos:

1. *Los cuerpos de característica 0.*
2. *Los cuerpos finitos.*
3. *Los cuerpos algebraicamente cerrados.*

4. *Las extensiones algebraicas de cuerpos perfectos.*
5. *Los cuerpos de característica prima no nula si y sólo si el endomorfismo de Frobenius es automorfismo.*

Demostración. 1. Véase los criterios de cuerpo perfecto.

2. En cuerpos finitos la característica siempre es un primo no nulo y además el endomorfismo de Frobenius que debe de ser inyectivo por salir de un cuerpo, será sobreyectiva por la finitud del cuerpo. Esto nos da que deben ser cuerpos perfectos.
3. En un cuerpo algebraicamente cerrado, los irreducibles son los lineales. Estos polinomios no pueden tener más que una raíz simple y por tanto, todo polinomio es separable.
4. Supongamos que K es un cuerpo perfecto y que F/K es una extensión algebraica. Para ver que F es un cuerpo perfecto tomamos cualquier extensión algebraica de E/F. Tenemos que E/K es algebraica y por tanto separable. Por la descomposición de torres separables y algebraicas (en un sentido), tenemos que E/F es separable. Como E/K es una extensión algebraica arbitraria tenemos que F es perfecto.

□

Ejemplo 6.1: $\mathbb{F}_p(t)$ con t transcendente no es perfecto.

6.4. Extensiones separables

Ejercicio 6.1: Buscar una extensión normal que no sea separable.

Vamos a contar homomorfismos de un cuerpo K sobre él mismo a su clausura, lo que nos será útil en la siguiente sección.

Definición 6.8 (Grado separable de un cuerpo)**.**
Sea $\overline{K} \supseteq F \supseteq K$ una torre de cuerpos.

El grado separable de F sobre K es el cardinal del conjunto de homomorfismos de F en $\overline{K}$ sobre K, esto es, $[F:K]_s = |\{\sigma : F \to \overline{K} \text{ sobre K }\}|$

Proposición 6.13 (Grado separable en torres algebraicas)**.**
Sea $K \subseteq F \subseteq E \subseteq \overline{K}$ una torre algebraica de cuerpos. Entonces:

$$[E:K]_s = [E:F]_s[F:K]_s$$

Demostración. Realizamos la prueba en cuatro pasos.

1. Sea τ_i los homomorfismos de $E \to \overline{K}$ sobre F y sean σ_i los homomorfismos de F en $\overline{K}$ sobre K. Sabemos que podemos extender los σ_i a la clausura $\overline{K}$ obteniendo unos endomorfismos $\overline{\sigma_i}$ que serán automorfismos puesto que todo endomorfismo de extensiones algebraicas es automorfismo. Entonces $\overline{\sigma_i}\tau_i$ serán homomorfismos $E \to \overline{K}$ sobre K.
2. Vemos que son todos distintos. En efecto, si $\overline{\sigma_i}\tau_j = \overline{\sigma_h}\tau_k$ entonces, para cada $f \in F$:

   $$\sigma_i(f) = \overline{\sigma}\tau(f) = \overline{\sigma_h}\tau_k(f) = \sigma_h(f)$$

   Por tanto, los σ_i son iguales sobre F y tendríamos que $\overline{\sigma_i} = \overline{\sigma_h}$ y entonces por ser cada $\overline{\sigma_i}$ automorfismo tendríamos que $\tau_j = \tau_k$.

Esto demuestra que $[E:K]_S \geq [E:F]_S[F:K]_S$.

3. Veamos que todo homomorfismo $E \to \overline{K}$ sobre K es de esta forma. Sea σ un homomorfismo de esta familia. Podemos restrigir $\sigma|_F$ y a partir de este construir una extensión a la clausura τ que como antes será automorfismo. También podemos extender los σ a la clausura obteniendo $\overline{\sigma}$. Como $\tau|_F = \sigma|_F$ tendríamos que $\overline{\sigma} \circ \tau^{-1}$ deja fijo a F entonces los homomorfismos buscados son $\overline{\sigma} \circ \tau^{-1}|_E$ y $\sigma|_F$.

4. Además son todos distintos ya que si $\sigma|_F = \sigma'|_F$ entonces las extensiones τ las hemos tomado iguales. Veamos que esto no puede pasar. Si ocurriese, $\sigma \circ \tau^{-1} = \sigma' \circ \tau^{-1}|_E$ y como $\tau - 1$ es sobreyectiva entonces $\overline{\sigma}|_E = \overline{\sigma}'|_E$ y por tanto $\sigma = \sigma'$ (revisar).

   Esto demuestra que $[E:K]_S \leq [E:F]_S[F:K]_S$.

□

Proposición 6.14 (Relación entre grado y grado separable en extensiones finitas)**.**
En el ambiente finito se verifican los siguientes resultados:

1. *Sea $\frac{E}{K}$ una extensión finita, entonces $[E:K]_s \Big| [E:K]$. En particular, $[E:K]_s \leq [E:K]$.*
2. *Sea $K \subseteq F \subseteq E$ una torre de cuerpos con $\frac{E}{K}$ finita. Entonces:*

$$[E:K]_s = [E:K] \iff [E:F]_s = [E:F] \wedge [F:K]_s = [F:K]$$

3. *Sea $\frac{E}{K}$ una extensión finita entonces es separable $\iff [E:K]_s = [E:K]$.*

Demostración. 1. Una extensión es finita si y sólo si es de generación finita por generados algebraicos. Nos aprovechamos de esto para proceder por distinción de casos.

   a) Caso simple: sea $K(u)$ la extensión con polinomio $Irr(u,K)$ de grado n. Ya habíamos demostrado en las herramientas previas a los cuerpos de descomposición que el número de homomorfismos de $K(u)$ a una extensión era el número de raíces en esa extensión (considerando $\sigma = Id$). Como la clausura algebraica contiene todas las raíces y todas las raíces de un polinomio irreducible tienen la misma multiplicidad se tendrá que si llamamos m a esta multiplicidad, el número de homomorfismos a la clausura desde $K(u)$ será el número de raíces, esto es, $\frac{n}{m}$.

   b) Caso compuesto: podemos aplicar inducción sobre el grado de la extensión. Gracias a nuestro estudio del grado separable en torres. Tendremos que:

$$[E:K]_S = [E:K(u)]_S[K(u):K]_S | [E:K(u)][K(u):K] = [E:K]$$

   Donde se ha utilizado la hipótesis de inducción y el caso simple.

2. Razónese a partir de la siguiente cadena:

$$[E:K]_S = [E:F]_S[F:K]_S \leq [E:F][F:K] = [E:K]$$

   De aquí está claro que se da la implicación izquierda. La implicación derecha se da por consideraciones de divisibilidad si llamamos $a = [E:F]_S, b = [F:K]_S, c = [E:F], d = [F:K]$ entonces tenemos que $a|b \wedge c|d$ pero en la implicación derecha se da también la igualdad $ac = bd$ y por tanto, $b|a \wedge c|d$ esto me dice que son asociados, esto es, $a \sim b, c \sim d$ y como son positivos y enteros tienen que ser iguales.

3. $\Rightarrow$) Sabemos que siempre $[E:K]_S \leq [E:K]$. Procedemos por inducción sobre $n = [E:K]$.

   Si $n = 1$ entonces como tenemos que la identidad es un homomorfismo a la clausura tendremos $[E:K]_S = [E:K]$. Supongamos $n > 1$, entonces tomando una extensión $[F:K] = 1$ entonces para $\alpha \in F \setminus K$, llamando $f(X) = Irr(\alpha, K)$ con $gr(f) = m$, tenemos que $[F:K(\alpha)] = \frac{n}{m}$ y por hipótesis de inducción $[F:K(\alpha)] = \frac{n}{m}$.

   Como α es separable sobre K, f tiene exactamente m raíces y por tanto, $[K(\alpha):K] = m$, por el grado separable en torres tendremos que $[F:K] = n$ como queríamos.

4. Si F/K es una extensión finita de grado n que no es separable, entonces existe $\alpha \in F$ tal que $Irr(\alpha, K)$ no es separable sobre K, es decir tiene raíces múltiples. Por tanto, el número de raíces distintas $m_0 < gr(f) = m$. Además $[K(\alpha):K] = m_0 < m$. Tenemos que, $[F:K(\alpha)]_S \leq [F:K(\alpha)] = \frac{n}{m}$ y por tanto

   $$n = [F:K]_S = [F:K(\alpha)][K(\alpha):K] < \frac{n}{m}m = n$$

   Esto es una contradicción.

□

Proposición 6.15 (Descomposición de torres separables y algebraicas revisitada en el caso finito)**.**
Sea $E \supseteq F \supseteq K$ una torre finita de cuerpos.

$\frac{E}{K}$ es separable $\iff$ $\frac{E}{F}, \frac{F}{K}$ son separables.

Demostración. $\Rightarrow$) Toda extensión algebraica.

$\Leftarrow$) En torres finita la separabilidad equivale a la separabilidad de las intermedias. □

Corolario 6.16 (Extensiones algebraicas generadas por elementos separables)**.**
Sea $E = K(\alpha_1, \ldots, \alpha_n)$ una extensión algebraica.

E/K es separable $\iff$ los elementos α_i son separables.

Para extender estos resultados véase Lang, a partir de la página 241.

7. Teoría de Galois finita

7.1. Automorfismos de extensiones de cuerpos

Definición 7.1.
Sean $\frac{F}{K}, \frac{E}{K}$ extensiones de cuerpos.

$Hom(F, E)$ es el conjunto de los homomorfismos de cuerpos entre F y E.

$Hom_K(F, E)$ es el conjunto de homomorfismos de K-espacios vectoriales entre F y E.

Proposición 7.1.
Sean $\frac{F}{K}, \frac{E}{K}$ extensiones de cuerpos.

1. $Hom(F, E) \subseteq Hom_K(F, E)$
2. $Hom_K(F, E)$ *tiene estructura de E-espacio vectorial.*

Demostración. 1. Recordemos que $\frac{E}{K}, \frac{F}{K}$ son K-espacios vectoriales. Entonces las propiedades de homomorfismo de cuerpo me dan las propiedades de homomorfismo de espacios vectoriales.

2. La suma es la suma convencional de homomorfismos $(\phi + \psi)(x) = \phi(x) + \psi(x)$ y el producto por escalares de E es de forma natural $e\phi(x) = e \cdot \phi(x)$.

□

Lema 7.2 (Lema de independencia de Dedekind)**.**
Dados $\frac{F}{K}, \frac{E}{K}$ dos extensiones de cuerpos y $\mathcal{F} \subseteq Hom(F, E)$.

$\mathcal{F}$ es linealmente independiente en $Hom_K(F, E)$ $\iff$ todos sus elementos son distintos.

Demostración. $\Rightarrow$) Si hubiera dos iguales, serían linealmente dependientes.

$\Leftarrow$) Lo que se prueba a continuación es que todo conjunto de homomorfismos de un grupo G en el grupo de las unidades de un cuerpo F^* donde los homomorfismos son distintos entonces son linealmente independientes.

Desde este resultado, para nuestra familia de homomorfismos de cuerpos $F \to E$ tenemos que cuando son restringidos a homomorfismos $F^* \to E^*$ son linealmente independientes. La clave es entonces que como todo homomorfismo que nace en un cuerpo es inyectivo esta restricción tiene sentido pues no hay ningún elemento no nulo que vaya al cero. Finalmente, si agregamos el 0, como todos los homomorfismos valdrían cero esto no cambia que los homomorfismos sean independientes o no.

Supongamos que son todos distintos. Y procedamos por inducción sobre el número de elementos n.

Si $n = 1$ entonces el conjunto $\{\sigma_1\}$ es linealmente independiente. Si $n > 1$ procedemos por inducción fuerte asumiendo que cada subconjunto de menos de n elementos es linealmente independiente.

Consideremos una familia $\{\sigma_1, \ldots, \sigma_n\} \subseteq \{\sigma_i : i \in I\}$ y una combinación lineal igualada a 0, $\sum_{i=1}^{n} e_i\sigma_i = 0$ con $e_i \in E$, queremos ver que todos los $e_i = 0$.

Como son todos distintos, en particular $\sigma_1 \neq \sigma_n$. Sea $y \in F^*$ tal que $\sigma_1(y) \neq \sigma_n(y) \neq 0$. Apliquemos la ecuación anterior a x, xy:

$$\sum_{i=1}^{n} e_i\sigma_i(x) = 0$$

$$\sum_{i=1}^{n} e_i\sigma_i(xy) = \sum_{i=1}^{n} e_i\sigma_i(x)\sigma_i(y) = 0$$

Multiplicando por $\sigma_n(y)^{-1}$ se obtiene que

$$\sum_{i=1}^{n-1} e_i\sigma_i(x)\sigma_i(y)\sigma_n(y)^{-1} + e_n\sigma_n(x) = 0$$

Restando ambas ecuaciones se tendrá para todo x que:

$$\sum_{i=1}^{n-1}(e_i - e_i\sigma_i(y)\sigma_n(y)^{-1})\sigma_i(x) = 0$$

y por tanto:

$$\sum_{i=1}^{n-1}(e_i - e_i\sigma_i(y)\sigma_n(y)^{-1})\sigma_i = 0$$

Como el conjunto $\{\sigma_1, \ldots, \sigma_{n-1}\}$ son independientes por hipótesis, tendremos que todos los coeficientes son nulos, en particular el primero:

$$e_1 - e_1\sigma_1(y)\sigma_n(y)^{-1} = e_1(1 - \sigma_1(y)\sigma_n(y)^{-1}) = 0 \implies e_1 = 0 \vee \sigma_1(y) = \sigma_n(y) \implies e_1 = 0$$

Y por tanto nos queda una combinación lineal $\sum_{i=2}^{n} e_i\sigma_i = 0$ que por hipótesis son independientes y por tanto los e_i son todos nulos. Como queríamos. □

Corolario 7.3 (Acotación del número de homomorfismos entre extensiones de cuerpos)**.**
Dadas $\frac{F}{K}, \frac{E}{K}$ dos extensiones de cuerpos.

Si $\frac{F}{K}$ es una extensión finita entonces $|Hom(F, E)| \leq [F : K]$.

En particular, $|Aut(F)| \leq [F : K]$.

Demostración. Por reducción al absurdo, supongamos que $\{\sigma_i\}_{1\leq i\leq n+1} \subseteq Hom(F, E)$. Como la extensión es finita tenemos una base $\{f_i\}_{1\leq i\leq n}$ de F como K-espacio vectorial. Para ver que los elementos σ_i no son distintos basta ver que no son linealmente independientes por el lema de Dedekind.

Supongamos que $\sum_{i=1}^{n+1} e_i\sigma_i = 0$ aplicando esta ecuación funcional a la base anterior obtendríamos n ecuaciones indexadas por j de la forma $\sum_{i=1}^{n+1} e_i\sigma_i(f_j) = 0$. En particular, los e_i son una solución del sistema de n ecuaciones y $n + 1$ incógnitas $\sum_{i=1}^{n+1} X_i\sigma_i(f_j) = 0$. Dado que el sistema es homógeneo, existe una solución no trivial. Esto me dice que los correspondientes e_i me dan la dependencia lineal de los σ_i y por tanto, tiene que haber repetidos entre los σ_i. Como queríamos. □

Definición 7.2 (Cuerpo fijo por un subgrupo de automorfismos)**.**
Sea E un cuerpo y $G \leq Aut(E)$ un subgrupo del grupo de automorfismos de E. El cuerpo fijo de E por G es:

$$E^G = \{u \in E : \forall\sigma \in G.\sigma(u) = u\}$$

Teorema 7.4 (Teorema de Artin)**.**
Sea E un cuerpo y $G \leq Aut(E)$ un subgrupo finito del grupo de automorfismos de E entonces E^G es un subcuerpo de E y $[E : E^G] = |G|$.

Demostración. Claramente, E^G es un subcuerpo por la definición de homomorfismo de cuerpos ya que sería un cuerpo con las operaciones heredadas de E. También se podría comprobar que es un cuerpo con las operaciones de suma, producto e inversos no nulos.

Por el lema de Dedekind, como $G \subseteq Hom_{E^G}(E, E)$ tendríamos que $|G| \leq [E : E^G]$ (si el grado es infinito, entonces claramente también se verifica la desigualdad).

Para la otra desigualdad procedemos por reducción al absurdo, si σ_i son los n elementos de G y suponemos que tenemos $n+1$ elementos independientes $e_i \in E$ sobre E^G, entonces el sistema $\sum_{i=0}^{n} \sigma_j(e_i)X_i = 0$ tiene n ecuaciones y $n+1$ incógnitas, será compatible indeterminado y tendrá solución no trivial en E para las incógnitas, s_i. Imponemos que sea la solución que tenga el menor número de términos distintos de cero. Como podemos reetiquetar las incógnitas podemos suponer que $\forall 1 \leq i \leq t.s_i \neq 0$ y $\forall t+1 \leq i \leq n+1.s_i = 0$. Queda un primer sistema $\sum_{i=0}^{n} \sigma_j(e_i)s_i = 0$.

Por ser G un grupo finito es claro que $\sigma\sigma_i$ nos dan todos los automorfismo del grupo, de modo que al aplicar $\sigma \in G$ nos quedan los sistemas $\sum_{i=0}^{n} \sigma(\sigma_j(e_i))\sigma(s_i) = 0$ y queda un segundo sistema $\sum_{i=0}^{n} \sigma_j(e_i)\sigma(s_i) = 0$.

Tomando el primer sistema multiplicado por $\sigma(s_0)$ y restando el segundo sistema multiplicado por s_0 nos queda $\sum_{i=1}^{n}[\sigma_j(e_i)s_i\sigma(s_0) - \sigma_j(e_i)\sigma(s_i)s_0] = 0$ y agrupando, $\sum_{i=0}^{n} \sigma_j(e_i)[s_i\sigma(s_0) - \sigma(s_i)s_0] = 0$.

Si llamamos $\overline{s_i} = s_i\sigma(s_0) - \sigma(s_i)s_0$ obtenemos una solución para cada $\sigma \in G$ donde los términos a partir del $t+1$ son nulos, pero también es nulo $\overline{s_0}$. Como tienen menos términos nulos, necesariamente deben ser nulas por las hipótesis. Pero entonces para cada $\sigma \in G$ tenemos que $\sigma(s_i/s_0) = s_i/s_0$ y por tanto $s_i/s_0 \in E^G$.

En particular, lo anterior ocurre para la identidad y entonces la primera ecuación del primer sistema da $\sum_{i=0}^{t} e_i s_i = 0$ de donde $e_0 = -\sum_{i=1}^{t}(s_i/s_0)e_i$ de modo que e_0 es una combinación lineal con coeficientes en E^G de e_i. Esto contradice la independencia lineal de los e_i. □

7.2. Extensiones de Galois

Definición 7.3 (Extensión finita de Galois)**.**
Una extensión finita $\frac{E}{K}$ es una extensión de Galois si existe un subgrupo $G \leq Aut(E)$ tal que $K = E^G$. En su caso, al subgrupo G se le llama grupo de Galois de la extensión y se le denota por $Gal(\frac{E}{K})$.

Proposición 7.5 (Caracterización de las extensiones de Galois finitas)**.**
Sea $\frac{E}{K}$ una extensión finita. Son equivalentes:

1. *$\frac{E}{K}$ es una extensión de Galois.*
2. *$\frac{E}{K}$ es normal y separable.*
3. *E es el cuerpo de descomposición de un polinomio separable sobre K.*

Demostración. Veamos primeramente 1 $\iff$ 2 y luego 2 $\iff$ 3

1. Supongamos que $\frac{E}{K}$ es de Galois con $Gal(\frac{E}{K}) = G$. Cada uno de estos automorfismos sobre K se pueden extender como homomorfismos a la clausura $\overline{K}$. Por tanto, el

$$[E : K]_S \geq |G| = [E : K] \geq [E : K]_S$$

Hemos utilizado que todo automorfismo se puede extender a la clausura mediante extensiones algebraicas, el lema de Artin y que el grado separable en extensiones finitas es menor que el grado de la extensión.

Como, $[E:K]_S = [E:K]$ y como la extensión es finita, debe ser separable. Como $[E:K]_S = |G|$, todos los homomorfismos que puede enviar a la clausura algebraica son automorfismos y en particular tenemos que $\sigma(E) = E$ para esos automorfismos de modo que las extensiones son normales.

2. Supongamos que $\frac{E}{K}$ es normal y separable. Por ser separable y finita, $[E:K]_S = [E:K]$ y por ser normal tendremos que cada homomorfismo σ a la clausura verifica que $\sigma(E) = E$.

   Si restringimos el codominio, a E tenemos que el número de endomorfismos en E sobre K es $[E:K]$ y como todo endomorfismo entre extensiones algebraicas es automorfismo tendremos que $|Aut(\frac{E}{K})| = [E:K]$ esto es que el número de automorfismos de E sobre K está dado por $[E:K]$. Nadie ha demostrado hasta ahora que estos fijen sólo a K sino que podrían fijar más elementos. Esto no ocurre gracias al teorema de Artin que nos dice que $[E : E^{Aut(\frac{E}{K})}] = [E:K]$ y por el teorema del grado tenemos que $[E^{Aut(\frac{E}{K})} : K] = 1$ y por tanto $Gal(\frac{E}{K}) = E^{Aut(\frac{E}{K})}$.

3. Como la extensión es normal y finita, necesariamente debe ser el cuerpo de descomposición de algún polinomio $f \in K[X]$. Dado que la extensión es separable, f será separable sobre K.

4. Si E es el cuerpo de descomposición de un polinomio $f \in K[X]$ separable sobre K entonces la extensión es finita y normal. Además como f es separable, el cuerpo de descomposición que genera también es separable.

□

El siguiente resultado muestra que como extensiones normales, las extensiones de Galois no son una clase distinguida de extensiones en general ya que las subextensiones no son siempre de Galois.

Proposición 7.6 (Extensiones de Galois en torres)**.**
Supongamos que $\frac{E}{K}$ es una extensión de Galois y $K \subseteq F \subseteq E$ entonces $\frac{E}{F}$ es de Galois.

Demostración. Como $\frac{E}{K}$ es de Galois, entonces es normal y separable. Por ser normal, la extensión $\frac{E}{F}$ es normal y por ser separable, las extensiones $\frac{E}{F}, \frac{F}{K}$ son separables. Por tanto, $\frac{E}{F}$ es una extensión de Galois. □

7.3. Conexión de Galois

Definición 7.4 (Subgrupo de automorfismos que fijan un subcuerpo)**.**
Sea E un cuerpo y $F \subseteq E$ un subcuerpo. El subgrupo de automorfismos de E que fijan F es:

$$G^F = \{\sigma \in G : \forall x \in F.\sigma(x) = x\}$$

Definición 7.5 (Correspondencia de Galois)**.**
Sea E un cuerpo y $G \leq Aut(E)$ un subgrupo de su grupo de automorfismos. Sea $H(E)$ el conjunto de subcuerpos de E y $S(E)$ al conjunto de subgrupos de G.

Consideremos las aplicaciones $G^{(\cdot)} : H(E) \to S(E)$ tal que $G \to G^F$ y $E^{(\cdot)} : S(E) \to H(E)$ con $H \to E^H$. Al par $(G^{(\cdot)}, E^{(\cdot)})$ se le llama conexión de Galois entre $H(E)$ y $S(E)$.

Proposición 7.7 (Propiedades de las conexiones de Galois)**.**
Sean F, F_1, F_2 subcuerpo intermedios de la extensión de cuerpos $\frac{E}{K}$ y sean H, H_1, H_2 subgrupos del grupo de Galois $G = Gal(\frac{E}{K})$ entonces:

1. $F_1 \subseteq F_2 \implies G^{F_1} \geq G^{F_2} \wedge H_1 \leq H_2 \implies E^{H_1} \subseteq E^{H_2}$
2. $F \subseteq E^{G^F} \wedge H \leq G^{E^H}$
3. $E^{G^{E^H}} = E^H \wedge G^{E^{G^F}} = G^F$

Demostración. 1. Si $F_1 \subseteq F_2$ entonces para cada $\sigma \in G^{F_2}$ se tiene que para cada $x \in F_2$, $\sigma(x) = x$, luego en particular para cada $x \in F_1$ se tendrá que $\sigma(x) = x$ y por tanto, $\sigma \in G^{F_1}$.

Si $x \in E^{H_2}$ entonces para cada $\sigma \in H_2$ se verifica que $\sigma(x) = x$ y como $H_1 \leq H_2$ entonces para cada $\sigma \in H_1 \leq H_2$ se tendrá que $\sigma(x) = x$ y por tanto, $x \in E^{H_1}$.

2. Si $x \in F$ entonces para cada $\sigma \in G^F$ se tiene que $\sigma(x) = x$ y esto ocurre si y sólo si $x \in E^{G^F}$.

   Si $\sigma \in H$ entonces para cada $x \in E^H$ se verifica que $\sigma(x) = x$ y esto ocurre si y sólo si $\sigma \in G^{E^H}$.

3. Aplicando 2. tenemos que $E^H \subseteq E^{G^{E^H}}$ y también tenemos que $H \subseteq G^{E^H}$ y por la propiedad 1. se tiene la igualdad. La otra es análoga.

□

Nuestro objetivo es dar subcuerpos F de E y subgrupos H de G tales que $G^{E^H} = H$ (C1) y $E^{G^F} = F$ (C2). El siguiente teorema muestra que existe una biyección entre los cuerpos que verifican (C2) y los grupos que verifican (C1) y que ambos conjuntos forman subretículos de los retículos de cuerpos y de los retículos de automorfismos. Para remarcar el hecho de que estamos estudiando subretículos hagamos previamente la siguiente observación:

Proposición 7.8.
Sea E/K una extensión finita de Galois con grupo de Galois $G = Gal(E/K)$. Entonces se verifica que:

1. $K = E^G$
2. *G es el único subgrupo de $Aut(E)$ tal que $K = E^G$.*

Como consecuencia, dada una extensión finita E/K, es de Galois $\iff K = E^G$ con $G = Aut(E/K) \subseteq Aut(E)$.

Demostración. Lo único que hay que desmostrar es que sólo hay un subgrupo de los automorfismos que fija a K. Si H fuera otro subgrupo que fija K, debería estar contenido en G y entonces por el teorema de Artin $|H| = [E : E^H] = [E : K] = |G|$ luego ambos deben ser iguales. □

Teorema 7.9 (Teorema fundamental de la teoría de Galois)**.**
Sea $\frac{E}{K}$ una extensión de Galois finita con $G = Gal(\frac{E}{K})$ y consideremos la conexión de Galois dada por $(G^{(\cdot)}, E^{(\cdot)})$ entre $H(E/K)$ y $S(G)$ entonces:

1. *La conexión de Galois es una biyección entre $H(E/K)$ y $S(G)$.*
2. *La conexión invierte el orden:*

   a) $F_1 \subseteq F_2 \iff G^{F_1} \geq G^{F_2}$

   b) $H_1 \leq H_2 \iff E^{H_1} \supseteq E^{H_2}$

3. *La conexión de Galois es un antiisomorfismo de retículos tal que:*

   a) $G^{F_1F_2} = G^{F_1} \cap G^{F_2}$

   b) $G^{F_1 \cap F_2} = G^{F_1} \vee G^{F_2}$

   c) $E^{H_1 \vee H_2} = E^{H_1} \cap E^{H_2}$

   d) $E^{H_1 \cap H_2} = E^{H_1}E^{H_2}$

   En particular, si $F_1/K, F_2/K$ *son extensiones intermedias entonces*

   a) $Gal(E/F_1F_2) = Gal(E/F_1) \cap Gal(E/F_2)$

   b) $Gal(E/(F_1 \cap F_2)) = Gal(E/F_1) \vee Gal(E/F_2)$

4. *Dos extensiones* $F_1/K, F_2/K$ *son conjugadas si existe* $\sigma \in Gal(E/K)$ *tal que* $\sigma(F_1) = F_2$ *y sus correspondientes subgrupos* H_1, H_2 *serán conjugados si existe* $\sigma \in G.H_1 = \sigma H_2 \sigma^{-1}$. *Entonces se verifica:*

   F_1/K *y* F_2/K *son conjugadas* $\iff$ H_1 *y* H_2 *son conjugados en* G.

   Como consecuencia,

   F/K *es una extensión de Galois* $\iff$ $Gal(E/F)$ *es un subgrupo normal de* G. *Además:*

   $$Gal(F/K) \cong G/Gal(E/F)$$

5. *Para una extensión intermedia* $K \subseteq F \subseteq E$, *si* $Gal(E/F) = H$ *y notamos por* $(G : H)$ *al índice del subgrupo* H *en* G *(el número de clases laterales a izquierda o derecha) entonces:*

   Para $H \leq G$ *se verifica* $|H| = [E : F]$ *y* $(G : H) = [F : K]$.

Ver proposiciones sobre

8. Elementos primitivos

Definición 8.1 (Elemento primitivo y extensiones simples)**.**
Sea F/K una extensión de cuerpos.

$a \in F$ es primitivo para F/K si $F = K(\alpha)$ en cuyo caso se dice que F/K es una extensión simple.

Teorema 8.1 (Teorema de Steinitz o del elemento primitivo)**.**
Sea F/K una extensión finita.

F/K es simple $\iff$ Existe un número finito de cuerpos intermedios.

Demostración. $\Rightarrow$) Sea $F = K(\alpha)$ y $K \subseteq L \subseteq F$ un cuerpo intermedio. Sea $f = Irr(\alpha, K)$ y $g = Irr(\alpha, L)$ donde sabemos por la introducción del polinomio mínimo que $g|f$. Esto nos dice que las extensiones intermedias tienen como polinomio mínimo para α un factor del polinomio mínimo de la extensión total. Además, observamos que los coeficientes del polinomio mínimo sobre un cuerpo, por definición deben de pertenecer al cuerpo.

Entonces sea L un extensión intermedia cualquiera, por lo anterior $g|f$. Tomemos una segunda extensión generada por los coeficientes de g, E. Entonces claramente, $E \subseteq L$ y $g = Irr(\alpha, E)$ ya que si $Irr(\alpha, E)$ fuera de grado menor entonces g también sería de grado menor. Pero $[K(\alpha) : E] = gr(Irr(\alpha, E)) = gr(Irr(\alpha, L)) = [K(\alpha) : E]$, de donde $E = L$. En consecuencia, hay un número finito de cuerpos intermedios, uno por cada factor de f.

$\Leftarrow$) Distiguimos casos, según la cardinalidad de K.

- Si K es finito, entonces la extensión finita da un cuerpo F finito (recuérdese el carácter vectorial de las extensiones). Pero sabemos que el grupo de las unidades de un cuerpo finito es cíclico y por tanto, bastará con dar un generador del cíclo para la extensión.
- Como la extensión es finita, tiene que ser de generación finita. Bastará probar que $K(a, b)$ es simple y luego procederíamos por inducción para probar el resto.

  Utilizando la hipótesis de que sólo puede haber un número finito de cuerpos intermedios es claro que entre los de la forma $K(a + bx)$ con $x \in K$ debe haber repetidos ya que el cardinal de K es infinito. Sean $x, y \in K$ con $x \neq y$ tales que $K(a + bx) = K(a + by)$, entonces elemento $b = \frac{(a+bx)-(a+by)}{x-y} \in K(a + bx) = K(a + by)$ de modo que $K(a + bx) \subseteq K(a, b)$ y siempre se tenía que $K(a, b) \subseteq K(a + bx)$. Por tanto, $K(a, b) = K(a + bx)$ y tenemos que la extensión es simple.

□

Proposición 8.2 (Ejemplos de extensiones primitivas)**.**
Los siguientes son ejemplos de extensiones simples:

1. *Toda subextensión de una extensión de Galois finita.*
2. *Toda extensión separable finita.*

Demostración. 1. Sea F/K subextensión de E/K una extensión de Galois finita. Por ser E/K finita, el grupo de Galois es finito. Y por tanto, existe un número finito de subgrupos que pueden dar cuerpos intermedios entre F y K.

2. Como la extensión es finita, en particular es algebraica y por tanto, existe una clausura normal, E/K. De exte modo, nuestra extensión F/K es una subextensión de la extensión de Galois E/K y por tanto sera simple.

□

Una vez determinado cuando una extensión es simple y presentados algunos ejemplos, damos criterios en ciertas situaciones para reconocer a los elementos primitivos.

Proposición 8.3 (Elementos primitivos en extensiones de Galois)**.**
Sea E/K una extensión de Galois y $\alpha \in E$.

α es primitivo $\iff$ los conjugados de α son distintos.

Demostración. $\Rightarrow$) Si α es primitivo, □

9. Cuerpos finitos

9.1. Resultados generales

Teorema 9.1 (Caracterización de los cuerpos finitos)**.**
1. Si K es un cuerpo finito, entonces su $|K| = p^n$ con p un número primo que es la característica del cuerpo y $n \geq 1$.

2. Teorema de Moore: para cada primo p y cada $n \geq 1$ existe un único cuerpo de orden p^n salvo isomorfismo, este es, el cuerpo de descomposición del polinomio $X^{p^n} - X$ sobre $\mathbb{F}_p$.

Demostración. Si K es finito, necesariamente su característica ha de ser un número primo y por tanto por el primer teorema de isomorfía $Img(f) \cong \mathbb{Z}_p$ es un subcuerpo de K. Subcuerpo que denotaremos por $\mathbb{F}_p$.

Ahora, K tiene estructura de espacio vectorial sobre $\mathbb{F}_p$ y dado que K es finito, considerando todos los elementos de K como vectores del espacio vectorial sobre $\mathbb{F}_p$, claramente, K es finitamente generado por sus elementos. Sabemos del álgebra lineal que todo espacio vectorial finitamente generado tiene una base. El cardinal de esta base nos dará la dimensión n y todo vector de K se expresa de forma en función de n vectores. Por tanto, hay exactamente p^n elementos en K.

2. La prueba de la unicidad nos dará pista para demostrar la existencia. Demostremos la unicidad. Sea K un cuerpo con p^n. Consideremos el grupo de los unidades $U = K \setminus \{0\}$. Este grupo tiene $p^n - 1$ elementos y por el teorema de Lagrange, tenemos que $\forall \alpha \in U . \alpha^{p^n - 1} = 1$. Por tanto, los elementos de este grupo son raíces del polinomio $X^{p^n-1} - 1$. Por tanto, los elementos de K son las raíces del polinomio $f = X^{p^n} - X$ que podemos ver como un polinomio en $K[X]$. La unicidad se sigue de la unicidad del cuerpo de descomposición para un polinomio.

Para ver la existencia, demostramos que el cuerpo de descomposición para f tiene exactamente p^n elementos. Como $f' = -1$ tenemos que f, f' no tienen raíces comunes y por tanto, no hay raíces múltiples de f, en consecuencia el cuerpo de descomposición contiene exactamente p^n raíces (esto es lo mismo que decir que el polinomio es separable). Para terminar la prueba, necesito ver que el conjunto de dichas raíces es un subcuerpo del cuerpo de descomposición. En efecto, tenemos las siguientes propiedades, sean u, v raíces de f entonces:

1. $(u+v)^{p^n} - (u+v) = u^{p^n} - u + v^{p^n} - v = 0$
2. $(uv)^{p^n} - uv = u^{p^n} v^{p^n} - uv = 0$
3. $(-u)^{p^n} - (-u) = 0$
4. $(u^{-1})^{p^n} - u^{-1} = 0$
5. $(1)^{p_n} - 1 = 0$

□

Definición 9.1 (Cuerpos finitos o de Galois)**.**
El cuerpo de Galois con q elementos es el único cuerpo con $q = p^n$ elementos, con p un número primo. Lo notaremos por $\mathbb{F}_q$.

Proposición 9.2 (Subgrupo multiplicativo finito de un cuerpo es cíclico)**.**
Sea F un cuerpo arbitrario y G un subgrupo finito de $F^x = F \setminus \{0\}$. Entonces, G es cíclico.

En particular, si F es finito, su grupo de unidades es cíclico.

Demostración. Sea G un subgrupo finito de F.

Ya que G es un grupo finito que será abeliano pues estamos asumiendo que los cuerpos tienen producto conmutativo. Por la clasificación de los grupos abelianos finitos mediante factores invariantes, tenemos que $G \cong \prod_{i=1}^{r} C_{n_i}$ con $\forall 1 \leq i < r.n_i | n_{i+1}$.

Observemos que $mcm(n_i) = n_r$ y como para cada $a_i \in C_{n_i}$ se verifica que $a_i^{n_i} = 1$, también se verificará que $a_i^{n_r} = 1$. Por tanto, cualquier $a \in G$ verificará que $a^{n_r} = 1$. Por tanto, a será raíz de $X^{n_r} - 1$, que como mucho tiene n_r raíces, esto me dice que $|G| \leq n_r$. Pero por el isomorfismo tendría que ser $|G| = \prod_{i=1}^{r} n_i = n_r$, de donde necesariamente todos los $n_i = 1$ salvo el último y tenemos que $G \cong C_{n_r}$. □

Teorema 9.3 (Estudio de la extensión $\mathbb{F}_q/\mathbb{F}_p$)**.**
Sea p un número primo y $q = p^n$ tenemos que:

1. *$\mathbb{F}_q/\mathbb{F}_p$ es una extensión de Galois.*
2. *$Gal(\mathbb{F}_q/\mathbb{F}_p)$ es un grupo cíclico de orden n generado por el automorfismo de Frobenius.*

Demostración.

1. Como por el teorema de Moore, $\mathbb{F}_q$ es el cuerpo de descomposición del polinomio $X^q - X$, la extensión es normal y finita.

   Como $\mathbb{F}_p$ es cuerpo finito, es perfecto. Como toda extensión finita de un cuerpo perfecto es separable, resulta que $\mathbb{F}_q/\mathbb{F}_p$ es separable.

   En consecuencia, la extensión es de Galois.

2. Comencemos observando que por el teorema de Artin, $n = [\mathbb{F}_q : \mathbb{F}_p] = |Gal(\mathbb{F}_q/\mathbb{F}_p)|$.

   Como $\mathbb{F}_q$ es un cuerpo finito, es perfecto. Como $Car(\mathbb{F}_q) = p$ necesariamente, el homomorfismo de Frobenius ϕ es sobreyectivo. Y siempre es monomorfismo puesto que sale de un cuerpo. Por tanto, ϕ es automorfismo. Además, fija $\mathbb{F}_p$ ya que $\phi(a) = a^p = a$, pues por el teorema de Moore $\mathbb{F}_p$ es el conjunto de las raíces de $X^p - X$. Por tanto, $\phi \in Gal(\mathbb{F}_q/\mathbb{F}_p)$.

   Para $0 \leq i < n$, $\phi^i \in Gal(\mathbb{F}_q/\mathbb{F}_p)$ y $\alpha \in \mathbb{F}_q$, tendríamos por inducción:

   $$\phi^i(\alpha) = \phi\phi^{i-1}(\alpha) = \phi(\alpha^{p^{i-1}}) = \phi(\alpha^{p^{i-1}}) = \alpha^{p^i}$$

   Pero los ϕ^i son distintos ya que si $\phi^i = \phi^j$ con $i > j$ entonces $\phi^{i-j} = 1$ y entonces:

   $$\alpha = 1(\alpha) = \phi^{i-j}(\alpha) = \alpha^{p^{i-j}}$$

   y entonces todo elemento de $\mathbb{F}_q$ sería raíz del polinomio $X^{p^{i-j}} - X$ que tiene un máximo de $p^{i-j} < p^n$ raíces. Esto daría un subcuerpo intermedio que sería cuerpo de descomposición de $X^{p^n} - X$ en contradicción de la definición de cuerpo de descomposición.

□

Proposición 9.4 (Retículo de subcuerpos de un cuerpo finito)**.**
Si denotamos por $Sub(F)$ a los subcuerpos de F tendremos:

$Sub(\mathbb{F}_{p^n}) = \{\mathbb{F}_{p^m} : m | n\}$

Demostración. Veamos la igualdad de conjuntos por doble inclusión.

$\subseteq$) Supongamos que $\mathbb{F}_{q^m}$ es isomorfo a un subcuerpo de $\mathbb{F}_{p^n}$ entonces la aplicación inclusión de $\mathbb{F}_{q^m}$ en $\mathbb{F}_{p^n}$ debe ser un homomorfismo. Por las propiedades de la característica $p|q$ y como ambos son primos necesariamente $p = q$.

Por el teorema del grado como tenemos la torre $\mathbb{F}_p \subseteq \mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ se tendrá que

$$n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}]m$$

y por tanto $m|n$.

$\supseteq$) Supongamos que $m|n$ con $n = md$. Por lo anterior, $Gal(\mathbb{F}_{p^n}/\mathbb{F}_p)$ es cíclico de orden n y generado por el automorfismo de Frobenius ϕ.

Recordando el retículo de subgrupos de un grupo cíclico tiene que existir un único subgrupo H de orden d que será cíclico y por tanto estará generado por ϕ^m.

Utilización la conexión de Galois H se corresponde con el subcuerpo $E = (\mathbb{F}_{p^n})^H$. Observemos que como H es subgrupo de un cíclico, que es abeliano, H debe ser normal y esto implica qque $E/\mathbb{F}_p$ es de Galois y $Gal(E/\mathbb{F}_p) \cong Gal(\mathbb{F}_{p^n}/\mathbb{F}_p)/Gal(\mathbb{F}_{p^n}/E)$ que tiene orden $n/d = m$ de donde $E = \mathbb{F}_{p^m}$ y por tanto, tenemos la implicación y la consecuencia del enunciado. □

Corolario 9.5 (Estudio de las extensiones finitas intermedias)**.**
Sea p un número primo y $n, m \in \mathbb{N}$ con $m|n$, tenemos que:

1. *$\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ es una extensión de Galois.*
2. *$Gal(\mathbb{F}_{p^n}/\mathbb{F}_{p^m}) \cong \langle \phi^m \rangle$*

Demostración. Es consecuencia de la demostración de la inclusión a la derecha del teorema anterior. □

9.2. Polinomios irreducibles sobre cuerpos finitos

9.2.1. Motivación

Como motivación al estudio de los polinomios irreducibles sobre cuerpos finitos veamos cómo se puede construir cualquier cuerpo finito a partir de ellos:

Proposición 9.6 (Construcción de cuerpos finitos con polinomios irreducibles)**.**
Sea $m \in \mathbb{F}_p[X]$ un polinomio irreducible entonces $\mathbb{F}_{p^n} \cong \frac{\mathbb{F}_i[X]}{\langle m \rangle}$.

Demostración. Como $\mathbb{F}_p[X]$ es un DIP, los ideales maximales deben ser los elementos generados por irreducibles. Como m es irreducibles, $\langle m \rangle$ es maximal y por tanto, $\frac{\mathbb{F}_i[X]}{\langle m \rangle}$ es un cuerpo.

Para ver el número de elementos del cuerpo, observamos que cada clase $[a] \in \frac{\mathbb{F}_i[X]}{\langle m \rangle}$ tiene un único representante r tal que $[r] = [a]$ y $gr(r) < gr(m)$. Esto lo da la unicidad del resto en el algoritmo de la división. Por otro lado, es claro que cualquier polinomio r con $gr(r) < gr(m)$ nos da una clase del cociente. La unicidad garantiza que ambos conjuntos son biyectivos y por tanto, el cuerpo contiene p^n elementos.

Por el teorema de Moore se tiene que salvo isomorfismo hay un sólo cuerpo con p^n elementos y de aquí se concluye el enunciado. □

9.2.2. Cálculo del número de polinomios irreducibles

Vamos a empezar determinando el número de polinomios irreducibles de grado fijo que hay de grado m. Claramente, este número es finito para cada m. Además, podemos limitarnos a calcular el número de representates de las clases irreducibles para la relación de asociados. Posteriormente, si quisieramos calcular todos los irreducibles bastaría multiplicar el resultado por el número de unidades. Como hay $|K|-1$ unidades (se quita el cero) en $K[X]$ bastaría multiplicar por $|K|-1$.

Sea $N_m = \{f \in \mathbb{F}_p[X] : \text{f es mónico irreducible de grado m}\}$

Ejemplo 9.1 (Cálculo de $|N_1|$): En $\mathbb{F}_p[X]$ los polinomios mónicos lineales son de la forma $x-a$ con $a \in \mathbb{F}_p[X]$ y son todos irreducibles. Por tanto, $|N_1| = p$.

Teorema 9.7 (Polinomios irreducibles de $\mathbb{F}_p$)**.**
Los factores irreducibles de $X^{p^n} - X$ en $\mathbb{F}_p[X]$ son exactamente los polinomios irreducibles de $\mathbb{F}_p[X]$ con grado divisor de n. En particular,

$$X^{p^n} - X = \prod_{f \in N_m, m|n} f$$

y por tanto, $\sum_{m|n} m|N_m| = p^n$.

Demostración. $\Rightarrow$ Si g es un factor irreducible de $X^{p^n} - X$ entonces vemos claramente que su grado divide a n. En efecto, g tendrá alguna raíz α y α también es raíz de $X^{p^n} - X$ pues g es factor de él. Por tanto, tenemos la siguiente torre de cuerpos $\mathbb{F}_{p^n} \supseteq \mathbb{F}_p(\alpha) \supseteq \mathbb{F}_p$. Por el teorema del grado, $gr(g) = [\mathbb{F}(\alpha) : \mathbb{F}_p]|[\mathbb{F}_{p^n} : \mathbb{F}_p]$.

$\Leftarrow$ Los irreducibles de grado divisor de n son factores. En efecto, sea g un irreducible de grado m con $m|n$. Si tomo una raíz α de g en algún cuerpo de descomposición, observo que $\mathbb{F}_p(\alpha) \cong \mathbb{F}_{p^m}$ y como $m|n$ tenemos que $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$, esto es, las raíces están contenidas en las raíces de $X^{p^n} - X$ y entonces claramente $g|f$.

Para obtener la descomposición en irreducibles, razonamos del siguiente modo. Por lo anterior, los factores son irreducibles con grado divisor. Cada factor puede aparecer únicamente una vez ya que si apareciera dos veces entonces teniendo en cuenta que, por el teorema de Moore, $X^{p^n} - X$ tiene p^n raíces distintas obtendríamos menos raíces de las necesarias puesto que no habría una por cada unidad del grado. Además, como $X^{p^n} - X$ es mónico podemos tomar los factores también como polinomios mónicos.

En resumen, podemos escribir

$$X^{p^n} - X = \prod_{f \in N_m, m|n} f$$

Tomando grados en ambos miembros obtenemos la fórmula del enunciado. □

Corolario 9.8 (Cálculo con n primo)**.**
Si n es un número primo entonces $|N_n| = \frac{p^n - p}{n}$

Demostración. Obsérvese que $\sum_{m|n} m|N_m| = p^n$ y como n es primo tenemos que $|N_1| + n|N_n| = p^n$. Pero $|N_1| = p$ y se sigue la igualdad del enunciado. □

Combinamos lo anterior para n no primo:

Ejemplo 9.2 (Cálculo de $|N_4|$): Por el corolario, $|N_2| = \frac{p^2-p}{2}$ y por el teorema:

$$p^4 = |N_4| = |N_1| + 2|N_2| + 4|N_4| = p + 2\frac{p^2-p}{2} + 4|N_4| \implies |N_4| = \frac{p^4-p^2}{4}$$

Vamos a generalizar esta fórmulas para cualquier grado:

Definición 9.2 (Función de Mobius)**.**

$$\mu(n) = \begin{cases} 1 & n = 1 \\ (-1)^s & n = \prod_{i=1}^{s} p_i \text{ para primos distintos } p_i \\ 0 & \text{en otro caso} \end{cases}$$

Teorema 9.9 (Fórmula de Gauss)**.**
Sea p un número primo y $N_n = \{f \in \mathbb{F}_p[X] : f$ es mónico irreducible de grado $n\}$. Se tiene que:

$|N_n| = \frac{1}{n}\sum_{m|n} \mu(m) p^{\frac{n}{m}}$

Demostración. La siguiente prueba se encuentra en [7].

Se procede por inducción sobre n.

Si $n = 1$ entonces el polinomio $x - a$ es irreducible en $\mathbb{F}_p$ para cualquier a por tanto, $|N_1| = p = \mu(1)p$.

Si $n > 1$ y definimos R_n como el conjunto de las raíces de los polinomios de N_n. Podemos observar que dichas raíces pertenecen a $\mathbb{F}_{p^n}$ gracias al teorema que da los polinomios irreducibles sobre $\mathbb{F}_p$. Como las raíces en este cuerpo son todas distintas por el teorema de Moore, se deduce que $|R_n| = n|N_n|$. El problema se reduce a calcular este $|R_n|$. Pongamos $n = \prod_{i=1}^{k} p_i^{e_i}$. Observamos que:

$R_n = \{\alpha \in \mathbb{F}_{p^n} : [\mathbb{F}_p(\alpha) : \mathbb{F}_p] = n\} = \{\alpha \in \mathbb{F}_{p^n} : \alpha$ no contenido en ningún subcuerpo maximal de $\mathbb{F}_{p^n}\} = \mathbb{F}_{p^n} \setminus \cup_i \mathbb{F}_{p^{n/p_i}}$

Finalmente, se utiliza el principio de inclusión-exclusión obteniéndose:

$$|R_n| = p^n - |\cup_i \mathbb{F}_{p^{n/p_i}}| = p^n - (\sum_{i=1}^{k} p^{n/p_i}) + (\sum_{i,j=1,i<j}^{k} p^{n/p_i p_j}) - \ldots + (-1)^k p^{n/\prod p_i}$$

Recordando la expresión de la función de Mobius:

$$\mu(1)p^{n/1} + \sum_{p_i|n} \mu(p_i)p^{n/p_i} + \ldots \mu(\prod p_i)p^{n/\prod p_i}$$

Obsérvese que para cualquier otro divisor $\mu(d) = 0$. □

Si se quieren los irreducibles no necesariamente mónicos bastaría multiplicar por $p - 1$.

Ejemplo 9.3 (Cálculo de $|N_6|$):

$$|N_6| = \frac{1}{6}\sum_{m|6} \mu(m)p^{\frac{6}{m}} = \frac{1}{6}\Big(\mu(1)p^6 + \mu(2)p^3 + \mu(3)p^2 + \mu(6)p\Big) = \frac{1}{6}(p^6 - p^2 - p^3 + p)$$

La fórmula anterior nos confirma que existen polinomios irreducibles de cualquier grado sobre $\mathbb{F}_p$ cosa que no ocurre por ejemplo en $\mathbb{R}$. Recordemos que todo polinomio no constante con coeficientes en $\mathbb{R}$ admite una raíz en $\mathbb{C}$. Se observa que un polinomio con coeficientes en $\mathbb{R}$ que admita una raíz compleja, también admite su conjugada. Pero entonces, si χ es tal raíz, $(x - \chi)(x - \overline{\chi}) = x^2 - (2Re(\chi))x + N(\chi)$ sería un factor con coeficientes reales del polinomio. Esto es, los únicos polinomios irreducibles sobre $\mathbb{R}$ son de grado 1 o 2.

Corolario 9.10 (Los cuerpos finitos tienen irreducibles de cualquier grado)**.**
$\forall n \geq 1. |N_n| > 0$

Demostración.

$$N_n \geq \frac{1}{n}\sum_{m|n}\mu(\frac{n}{d})p^d \geq \frac{1}{n}\Big(p^n - \sum_{i=0}^{m-1} p^i\Big) = \frac{1}{n}\Big(p^n - \frac{p^n-1}{p-1}\Big)$$

Pero dado que $p \geq 2$, imponer que el último término sea mayor que cero equivale a que:

$$p^{n+1} \geq 2p^n > 2p^n - 1$$

que es siempre cierto. □

9.2.3. Algoritmo de Berlekamp

Dado un polinomio $f \in \mathbb{F}_p[X]$ queremos dar un algoritmo para determinar si es irreducible.

Sea $f \in \mathbb{F}_p[X]$ un polinomio de grado $n > 1$ (los de grado 1 son todos irreducibles). Si el polinomio tiene raíces múltiples en un cuerpo de descomposición, no puede ser irreducible ya que, $\mathbb{F}_p$ es un cuerpo perfecto, y por tanto, los irreducibles son separables. En consecuencia, asumamos que f no tiene raíces múltiples en un cuerpo de descomposición.

Sea $R = \frac{\mathbb{F}_p[X]}{\langle f\rangle}$ el cuerpo que define f. Ya vimos que todo elemento de R se puede escribir como $\Big(\sum_{i=0}^{n-1} a_i X^i\Big) + \langle f\rangle$ con $a_i \in \mathbb{F}_p$. Podemos ver R como un espacio vectorial de dimensión n sobre $\mathbb{F}_p$. En estas condiciones tenemos el análogo al endomorfismo de Frobenius, $T : R \to R$ tal que $T(g + \langle f\rangle) = g^p + \langle f\rangle$. Este endormofismo:

- Está bien definido. Pues si $g + \langle f\rangle = h + \langle f\rangle$ entonces $g = h + fB$ para $B \in \mathbb{F}_p[X]$ y por tanto por el binomio de Newton:

  $$g^p = (h + fB)^p = h^p + f^pB^p = h^p + ff^{p-1}B^p$$

  de modo que $g^p + \langle f\rangle = h^p + \langle f\rangle$.

- Es lineal. Es decir $T(\alpha u + \beta v) = \alpha T(u) + \beta T(v)$ donde u, v son los vectores de coeficientes de los polinomios que representan. De nuevo el truco consiste en aplicar la estrategia del apartado anterior. Si $u = (u_1, \ldots, u_n)$ y $v = (v_1, \ldots, v_n)$ entonces $T(u) = (u_1^p, \ldots, u_n^p)$ y $T(v) = (v_1^p, \ldots, v_n^p)$ de donde se sigue fácilmente el resultado.

Claramente la identidad $1_R : R \to R$ también es lineal.

Teorema 9.11 (Principio del algoritmo de Berlekamp)**.**
Sea $f \in \mathbb{F}_p[X]$ un polinomio de grado $n > 1$, y $R = \frac{\mathbb{F}_p[X]}{\langle f\rangle}$. Entonces, f es irreducible si y sólo la aplicación lineal $T - 1_R : R \to R$ tiene rango $n - 1$.

Demostración. $\Rightarrow$) Si f es irreducible entonces R es un cuerpo y T sería el endomorfismo de Frobenius del cuerpo. Por tanto:

$$Ker(T) = \{\alpha \in R : \alpha^p = \alpha\} = \mathbb{F}_p \implies dim(Ker(T)) = 1 \implies rg(T) = dim(Img(T)) = n - 1$$

$\Leftarrow$) Por contrarrecíproco, si f es reducible entonces $f = gh$ con $g, h \in \mathbb{F}_p[X]$ con $gr(g), gr(h) \leq gr(f)$. Además, como f no tiene raíces múltiples, g, h en el cuerpo de descomposición factorizan en lineales

que no tienen factores comunes y por tanto, son primos relativos. Como el máximo común divisor no depende del cuerpo extensión, deducimos que f, g son primos relativos en $\mathbb{F}_p$. Por el teorema de Bézout, $\exists A, B \in \mathbb{F}_p[X].Ag + Bh = 1$. Vamos a ver que:

$$Ag, Bh \in Ker(T - 1_R) \iff (Ag)^p - Ag, (Bh)^p - Bh \in \langle f \rangle$$

Usando el teorema del binomio y que $f = gh$, tenemos que

$$(Ag)^p = Ag(1 - Bh)^{p-1} = Ag(1 - (p-1)Bh + \ldots + (-1)^{p-1}(Bh)^{p-1}) =$$

$$= Ag - gh(p-1)AB + \ldots + gh(-1)^{p-1}AB^{p-1}h^{p-2} \equiv Ag \ mod(f)$$

como queríamos demostrar. Finalmente, probamos que $Ag + \langle f \rangle, Bh + \langle f \rangle$ son linealmente independientes en R con lo que $Ker(T - 1_R) \geq 2$ o equivalentemente $rg(T - 1_R) \leq n - 2$. Veamos que cualquier combinación igualada a cero es trivial:

$$\exists a, b \in \mathbb{F}_p, C \in \mathbb{F}_p[X].aAg + bBh = ghC$$

pero como $mcd(g, h) = 1$, se deduce que $g|bB$ y $h|aA$. Pero al ser $Ag + Bh = 1 \implies mcd(g, B) = gcd(h, A) = 1$ y por el lema de Euclides, $g|b \wedge h|a$ por grados, necesariamente, $a = b = 0$ □

Veamos ahora un ejemplo de aplicación del teorema anterior:

Ejemplo 9.4 (Aplicación del principio de Berlekamp): Dado el polinomio $f = X^5 + X^4 + 1 \in \mathbb{F}_2[X]$. Determinar si es irreducible.

1. El polinomio no tiene raíces múltiples pues $gcd(f, f') = gcd(X^5 + X^4 + 1, 5X^4) = 1$.
2. $R = \frac{\mathbb{F}_2[X]}{\langle f \rangle}$ es un espacio vectorial sobre $\mathbb{F}_2$ de dimensión 5, con base $1, x, x^2, x^3, x^4 + \langle f \rangle$.
3. Calculamos la expresión de T a partir de las imágenes de los vectores de la base $T(1) = 1, T(x) = x^2, T(x^2)) = x^4, T(x^3) = x^6 = 1 + x + x^4, T(x^4) = x^8 = 1 + x + x^2 + x^3 + x^4$.
4. La matriz de $T - 1_R$ es:

$$T - 1_R = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix} - \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

5. Esta matriz tiene rango como mucho tres ya que la primera columna es cero y las tres últimas suman cero (estamos en característica 2). Como $3 < 4 = gr(f) - 1$ deducimos que f es reducible.

10. Extensiones ciclotómicas. Raíces de la unidad

10.1. Raíces de la unidad

Definición 10.1 (Raíces n-ésimas de la unidad)**.**
Dado un cuerpo K y una clausura algebraica $\overline{K}$.

Las raíces n-ésimas de la unidad son las raíces del polinomio $X^n - 1$ en $\overline{K}$.

Proposición 10.1 (Condición para que las raíces n-ésimas de la unidad sean distintas)**.**
Sea K un cuerpo.

Las raíces n-ésimas de la unidad son todas distintas si y sólo si $Car(K) \nmid n$. En particular, si la característica es cero.

Si $0 \neq p = Car(K)|n$ entonces si $n = mp^r$ existen m raíces n-ésimas de la unidad distintas y todas tienen multiplicidad p^r.

Demostración. Las raíces serán distintas si y sólo si $X^n - 1$ no tiene raíces mútiples. Por el criterio de las raíces simples, esto ocurre cuando $mcd(f, Df) = 1$. En nuestro caso, cuando $mcd(X^n - 1, nX^{n-1}) = 1$. Distinguimos tres casos. Si $0 \neq p = Car(K)|n$ entonces claramente $mcd(X^n - 1, nX^{n-1}) = mcd(X^n - 1, 0) = X^n - 1 \neq 1$. Si $Car(K) = 0 \vee p = Car(K) \nmid n$ entonces el polinomio nX^{n-1} tiene grado $n - 1$ y el único irreducible que lo divide es X como X no divide a $X^n - 1$ se deduce que ambos son primos relativos.

Si $0 \neq p = Car(K)|n$ entonces el criterio de la derivada nos dice que existen raíces múltiples. En particular, como $p \neq 0$ tenemos el endomorfismo de Frobenius, que nos dice que si $n = mp^r$ entonces $X^n - 1 = (X^m - 1)^{p^r}$ de modo que aplicando el caso anterior existen m raíces n-ésimas de la unidad distintas y tienen multiplicidad p^r. □

En lo sucesivo asumiremos que existen n raíces n-ésimas distintas de la unidad. Suponemos también que el cuerpo K es fijo.

Proposición 10.2 (Raíces n-ésimas como subgrupo cíclico)**.**
Las raíces n-ésimas de la unidad forman un subgrupo cíclico de orden n del grupo multiplicativo de $\overline{K}$ que denotamos μ_n.

Demostración. Para ver que es un subgrupo tomo a, b raíces n-ésimas. Entonces $(ab^{-1})^n = a^n b^{-n} = 1$ de donde ab^{-1} también es una raíz n-ésima de la unidad. Además, el subgrupo es cíclico pues todo subgrupo finito del grupo multiplicativo de un cuerpo es cíclico como ya vimos en cuerpos finitos. □

Definición 10.2 (Raíz n-ésimas primitiva de la unidad)**.**
Una raíz n-ésima primitiva de la unidad es un generador del grupo de las raíces n-ésimas de la unidad.

Proposición 10.3 (Retículo de raíces n-ésimas)**.**
$Sub(\mu_n) = \{\mu_d : d|n\}$. Además, si a es una raíz n-ésima primitiva, esto es, $\mu_n = \langle a \rangle$ entonces $a^{n/d}$ es una raíz d-ésima primitiva de la unidad, esto es, $\mu_d = \langle a^{n/d} \rangle$.

Demostración. Esta proposición es la clasificación de los grupos cíclicos de orden finito, que se tiene de la teoría de grupos. □

10.2. Extensiones ciclotómicas

Definición 10.3 (Extensión ciclotómica)**.**
Una extensión ciclotómica de K es un cuerpo de descomposición sobre K de un polinomio del tipo $X^n - 1$. Equivalentemente, es una extensión simple generada por una raíz n-ésima primitiva de la unidad.

Teorema 10.4 (Estructura de Galois de una extensión ciclotómica)**.**
Sea F/K una extensión ciclotómica generada por el polinomio $X^n - 1$ y sea ξ raíz n-ésima primitiva de la unidad. Entonces:

1. *F/K es una extensión de Galois.*
2. *$Gal(F/K) \cong H \leq U(\mathbb{Z}_n)$ mediante el isomorfismo $\sigma \mapsto i$ tal que $\sigma(\xi) = \xi^i$.*
3. *$|Gal(F/K)||\phi(n)$.*

Demostración.

1. F/K es una extensión normal por ser el cuerpo de descomposición del polinomio $X^n - 1$ sobre K. Hemos asumido además que las raíces de $X^n - 1$ son distintas. En particular, también lo son las raíces de sus factores irreducibles, esto es, el polinomio es separable. Como el cuerpo de descomposición está formado por sus raíces, necesariamente, la extensión es separable. Por tanto, es de Galois.

2. Tenemos que $\sigma \in Gal(F/K)$ queda determinado por su valor sobre ξ. Queremos ver que si $\sigma(\xi) = \xi^i$ entonces $i \in U(\mathbb{Z}_n)$.

   En efecto, si tomamos j tal que $\sigma^{-1}(\xi) = \xi^j$ entonces $\xi = (\sigma\sigma^{-1})(\xi) = \xi^{ji}$. Como ξ tiene orden n, esta ecuación se formula de manera equivalente como $ij = 1$ en $\mathbb{Z}_n$ y por tanto $i, j \in U(\mathbb{Z}_n)$ como queríamos.

   Por tanto, la aplicación dada en el enunciado está bien definida. Además es un homomorfismo de grupos ya que si $\tau \in Gal(F/K)$ viene dada por $\tau(\xi) = \xi^k$ entonces $\sigma \circ \tau(\xi) = \xi^{ik}$.

   Además, si $\sigma \in Ker$ entonces $\sigma(\xi) = \xi^i = \xi$ de modo que $\sigma = Id_F$ y por tanto, tenemos un monomorfismo. Por el primer teorema de isomorfía, $Gal(F/K) \cong Im \leq U(\mathbb{Z}_n)$.

3. Es consecuencia del teorema de Lagrange y de que $\phi(n) = |U(\mathbb{Z}_n)|$.

□

10.3. Polinomios ciclotómicos

Definición 10.4 (Polinomio ciclotómico)**.**
Sea F/K una extensión ciclotómica.

El n-ésimo polinomio ciclotómico en K es $\Phi_n(X) = \prod(X - a_i)$ con a_i las raíces n-ésimas primitivas de la unidad en F.

Proposición 10.5 (Propiedades de los polinomios ciclotómicos)**.**
Se verifican las siguientes propiedades:

1. *$X^n - 1 = \prod_{d|n} \Phi_d(X)$*

2. *Los coeficientes de $\Phi_n(X)$ pertenecen al cuerpo característico de K. Si $Car(K) = 0$ entonces pertenecen a $\mathbb{Z}$. Además, $gr(\Phi_n(X)) = \phi(n)$ y $\Phi_n(X)$ es mónico.*
3. *Cálculo del n-ésimo polinomio ciclotómico: $\Phi_n(X) = \frac{X^n-1}{\prod_{d|n \wedge d \neq n} \Phi_d(X)}$*
4. *Fórmula de Gauss: $\Phi_n(x) = \prod_{d|n}(x^d - 1)^{\mu(n/d)}$*

Demostración. 1. Escribimos $\phi_d(X) = \prod X - \xi_i$ con ξ_i raíces d-ésimas de la unidad. Es claro, que todas estas raíces son raíces n-ésimas de la unidad cuyo orden es d y recíprocamente. Es claro, que juntando estos productos obtenemos $X^n - 1$ como producto de los ϕ_d para cada $d|n$.

2. Se hace por inducción sobre n.
3. Basta ver que hay $\phi(n)$ raíces primitivas de las unidad. Esto es así ya que un grupo cíclico de orden n tiene $\phi(n)$ generadores distintos como se vio en la teoría de grupos. Por tanto, ϕ_n tiene grado $\phi(n)$.
4.

□

Una forma de recordar la fórmula de Gauss y la fórmula que relaciona distintos ciclótomicos es ver que hay una dualidad entre ϕ y polinomios $X^m - 1$. Además, en nuestras fórmulas, μ siempre a alternado un argumento simétrico tipo $d, \frac{m}{d}$.

10.4. Polinomios ciclotómicos con coeficientes racionales

[4] ofrece una versión restringida a $\mathbb{Q}$ de los resultados generales en cualquier cuerpo a partir de la página 231. Puede ser de provecho. En particular, las raíces, tienen una expresión explícita en términos de la exponencial compleja.

Proposición 10.6 (Irreducibilidad de los polinomios ciclotómicos racionales)**.**
Para cada $n \in \mathbb{N}$, $\Phi_n(X)$ es irreducible sobre $\mathbb{Q}$.

Demostración. Sea ξ una raíz n-ésima primitiva de la unidad y $f(X) = Irr(\xi, \mathbb{Q})$. Veamos que $\phi_n(X) = f(X)$ con lo que $\phi_n(X)$ será irreducible. □

Corolario 10.7 (Grado de las extensiones ciclótomicas)**.**
Sea ξ una raíz n-ésima primitiva de la unidad entonces:

$[\mathbb{Q}(\xi) : \mathbb{Q}] = gr(\Phi_n(X)) = \phi(n)$

Proposición 10.8 (Grupo de Galois de las extensiones ciclotómicas racionales)**.**
Sea ξ una raíz n-ésima primitiva de la unidad, entonces:

$Gal(\mathbb{Q}(\xi)/\mathbb{Q}) \cong U(\mathbb{Z}_n)$ mediante el isomorfismo $\sigma \mapsto l$ con $\sigma(\xi) = \xi^l$.

Demostración. Obsérvese que como ϕ_n es irreducible en $\mathbb{Q}$, necesariamente, $\sigma(\xi)$ será raíz de ϕ_n. Como el grupo de las raíces n-ésimas de la unidad es cíclico, tendremos que, $\sigma(\xi) = \xi^l$ donde l será primo relativo con n (debe ser raíz primitiva y por tanto, el orden del subgrupo que genera debe ser n). Esto prueba que la aplicación f que dará el isomorfismo está bien definida.

En estas condiciones, f es un monomorfismo pues si $\sigma(\xi) = l \wedge \eta(\xi) = k$ entonces

$$(\sigma \circ \eta)(\xi) = \sigma(\eta(\xi)) = \xi^{kl}$$

y por tanto, $f(\sigma \circ \eta) = kl = f(\sigma)f(\eta)$. Por tanto, f es un homomorfismo. Que es inyectivo se sigue de que:

$$f(\sigma) = 1 \implies \sigma(\xi) = \xi \implies \sigma = Id$$

Como $|Gal(\mathbb{Q}(\xi)/\mathbb{Q})| = [\mathbb{Q}(\xi) : \mathbb{Q}] = \phi(n) = |U(\mathbb{Z}_n)|$, tenemos una aplicación inyectiva entre conjuntos de igual cardinal finito, luego debe ser biyectiva. □

11. Norma y traza

Definición 11.1 (Norma y traza)**.**
Sea F/K una extensión finita y separable con $[F : K] = n$. En estas condiciones se tiene que $[F : K]_s = [F : K]$, es decir hay n homomorfismos de F a la clausura de K. Sea $\alpha \in F$.

1. La norma de α en F/K es $N_{F/K}(\alpha) = \prod \sigma_i(\alpha)$.
2. La traza de α en F/K es $T_{F/K}(\alpha) = \sum \sigma_i(\alpha)$.

Proposición 11.1 (Propiedades generales)**.**
Sea F/K una extensión finita y separable de grado n.

1. *La norma es un homomorfismo multiplicativo en F con imagen K.*
   Análogamente, la traza es un homomorfismo aditivo en F con imagen K.
   Además, $N(1) = 1$, $T(0) = 0$.
2. *Comportamiento frente a escalares. Si $a \in K$ y $\alpha \in F$ entonces:*
$$N(a\alpha) = a^n N(\alpha) \wedge T(a\alpha) = naT(\alpha)$$
3. *Fórmulas de transitividad. Para $K \subseteq F \subseteq E$ con E/K finita y separable y $\alpha \in E$:*
$$N_{F/K}(N_{E/F}(\alpha)) = N_{E/K}(\alpha) \wedge T_{F/K}(T_{E/F}(\alpha)) = T_{E/K}(\alpha)$$
4. *Sea $\alpha \in F$ con $Irr(\alpha, K) = \sum_{i=0}^{r} a_i X^i$ entonces $N(\alpha) = (-1)^n (a_0)^{n/r} \wedge T(\alpha) = -(n/r)a_{r-1}$.*

12. Extensiones cíclicas

Definición 12.1 (Extensiones cíclicas y abelianas)**.**
Una extensión E/K es cíclica si es de Galois y su grupo de Galois es cíclico.

Una extensión E/K es abeliana si su grupo de Galois es un grupo abeliano.

12.1. Teorema 90 de Hilbert

Los siguientes dos teoremas se pueden entender como descriptores del núcleo de los homomorfismos norma y traza definidos en el apartado anterior, en el caso de extensiones cíclicas.

Teorema 12.1 (Teorema 90 de Hilbert)**.**
Sea E/K extensión cíclica de grado n con grupo $G = Gal(E/K) = \langle\sigma\rangle$ y sea $\beta \in E$. Son equivalentes:

1. $N_{E/K}(\beta) = 1$
2. *Existe* $0 \neq \alpha \in E$ *tal que* $\beta = \frac{\alpha}{\sigma(\alpha)}$.

Demostración. $\Leftarrow$) Usando que la norma es homomorfismo multiplicativo, se tiene que:

$$N_{E/K}(\beta) = \frac{N_{E/K}(\alpha)}{N_{E/K}(\sigma(\alpha))} = 1$$

$\Rightarrow$) Si tomamos β con $N(\beta) = 1$ esto implica que $\beta \neq 0$. Además, los automorfismos $1, \sigma, \ldots, \sigma^{n-1}$ son distintos dos a dos ya que si $\sigma^i = \sigma^j$ con $i > j$ entonces se deduciría que el orden del grupo de Galois es menor que n y entonces por el teorema de Artin, el grado de la extensión no sería n.

Como los automorfismos son todos distintos, por el lema de Dedekind son linealmente independientes como homomorfismos de espacios vectoriales sobre K. En particular, la aplicación:

$$\tau = 1 + \beta\sigma + (\beta\sigma(\beta))\sigma^2 + \cdots + (\beta\sigma(\beta)\ldots\sigma^{n-2}\beta)\sigma^{n-1}$$

no es idénticamente cero. En particular, $\exists\theta \in E.\tau(\theta) \neq \theta$. Sea $\alpha = \tau(\theta)$. Calculamos $\sigma(\alpha)$ en la expresión anterior y multiplicamos por β. Teniendo en cuenta que $\sigma^n = 1$ y $\beta\sigma(\beta)\ldots\sigma^{n-1}(\beta))\sigma^n(\beta) = 1$ quedaría $\beta\sigma(\alpha) = \alpha$. □

Teorema 12.2 (Teorema 90 de Hilbert aditivo)**.**
Sea K un cuerpo y E/K una extensión cíclica de grado n con grupo $G = Gal(E/K) = \langle\sigma\rangle$ y sea $\beta \in E$. Son equivalentes:

1. $T_{E/K}(\beta) = 0$.
2. $\exists\alpha \in E.\beta = \alpha - \sigma(\alpha)$.

12.2. Clasificación de los grupos cíclicos

Teorema 12.3 (Teorema de Lagrange)**.**
Sea K cuerpo y $n \in \mathbb{N} \setminus \{0\}$.

Si $p = Car(K) \neq 0$ supondremos además que $p \nmid n$.

Supongamos que existe una raíz n-ésima primitiva de la unidad en K.

1. *Si E/K es una extensión cíclica de grado n, entonces existe $\alpha \in E$ tal que:*

$$E = K(\alpha) \text{ y } Irr(\alpha, K) = X^n - a \text{ para algún } a \in K$$

2. *Sea $a \in K$. Si α es una raíz de $X^n - a$, entonces se tiene $K(\alpha)/K$ es una extensión cíclica de grado d con $d \mid n$ y $\alpha^d \in K$.*

La lectura adecuada del teorema anterior sería que considerando cuerpos de característica nula o prima p donde p no divide a cierto n que representa un grado de extensión o un índice de raíz, se tiene que toda extensión cíclica de grado n se obtiene como una extensión simple generada por una raíz n-ésima. Recíprocamente, partiendo de una raíz n-ésima genero una extensión cíclica de grado divisor de n tal que cierta potencia se puede ver en K (y no en $K(\alpha)$).

Un ejemplo sencillo de lo anterior nos lo da $X^2 + 1$ cuyo grupo de Galois consiste de la conjugación compleja y de la identidad.

Teorema 12.4 (Teorema de Artin-Schreier)**.**
Sea K un cuerpo de característica p. Se verifica:

1. *Si E/K es una extensión cíclica de grado p, entonces existe $\alpha \in E$ tal que:*

$$E = K(\alpha) \text{ y } Irr(\alpha, K) = X^p - X - a \text{ para algún } a \in K$$

2. *Sea $a \in K$. Tenemos dos casos según la estructura de $X^p - X - a$:*

   a*) Tiene una raíz en K. En este caso, todas las raíces están en K (no da extensión cíclica).*

   b*) Es irreducible. En este caso, si α es una raíz, la extensión $K(\alpha)/K$ es cíclica de grado p.*

Este teorema completaría una caracterización de las extensiones cíclicas. Por un lado, se tiene el caso en que $p \nmid n$. Por otro lado, el caso en que $p|n$. Este caso se ha disgregado implícitamente en dos subcasos. El caso $n = p$ que es el caso anterior y el caso $n = p^m t$ con $m \geq 1$. Este caso, se puede reducir al caso anterior.

En efecto, como el grupo de Galois de la extensión es cíclico tenemos para cada divisor un subgrupo de ese orden. Entonces, haciendo la correspondencia entre grupos y cuerpos obtendríamos un diagrama similar al siguiente:

$$\begin{array}{c} E_n \\ \Big| p \\ E_{n-1} \\ \Big| p \\ \cdots \\ \Big| p \\ E_1 \\ \Big| t \\ K \end{array}$$

donde todas las extensiones que nacen son cíclicas y se pueden estudiar mediante los criterios anteriores.

13. Extensiones solubles y radicales

Definición 13.1 (Extensión soluble)**.**
Una extensión finita y separable F/K es soluble si hay una extensión E/K de Galois con grupo de Galois soluble y $K \subseteq F \subseteq E$.

Proposición 13.1 (Definición equivalente de solubilidad de una extensión)**.**
Una extensión finita y separable F/K es soluble si la clausura normal de F/K tiene grupo de Galois soluble.

Demostración. Habría que demostrar dos implicaciones.

Si asumimos que la clausura normal de F/K tiene grupo de Galois soluble entonces ciertamente existe una extensión E/K de Galois con grupo de Galois soluble que contiene a F, esta es, la propia clausura.

Si asumimos que hay una extensión E/K de Galois con grupo de Galois soluble que contiene a F entonces observamos que la clausura normal M debe verificar que $K \subseteq M \subseteq E$. Como ciertamente, M/K es de Galois, el teorema fundamental nos dice que $Gal(E/M)$ es normal y que $Gal(M/K) \cong Gal(E/K)/Gal(E/M)$. Pero el cociente por un subgrupo normal de un grupo soluble es soluble. □

Definición 13.2 (Extensión soluble por radicales)**.**
Una extensión F/K finita separable es soluble por radicales cuando $mcd([F:K], car(K)) = 1$ y hay una torre:

$$K = E_0 \subseteq E_1 \subseteq \ldots \subseteq E_m = E$$

tal que $F \subseteq E$ y siendo cada E_{i+1}/E_i de una de estas dos formas:

- $E_{i+1} = E_i(\xi)$ con ξ raíz de la unidad (extensión ciclotómica)
- $E_{i+1} = E_i(\alpha)$ con α raíz de un polinomio $X^n - a \in E_i[X]$, si $p = Car(K) \neq 0$ entonces $p \nmid m$ y existe $\xi \in E_i$ raíz n-ésima primitiva de la unidad (primer tipo de extensión cíclica).
- $E_{i+1} = E_i(\alpha)$ con α raíz de un polinomio $X^p - X - a \in E_i[X]$ y $Car(K) = p$ primo (segundo tipo de extensión cíclica).

Teorema 13.2 (Teorema de Galois)**.**
Sea F/K una extensión finita y separable. Entonces:

F/K es soluble por radicales $\iff$ F/K es soluble.

14. Grupo de Galois como grupo de permutaciones

Proposición 14.1 (Inmersión del grupo de Galois en el grupo de permutaciones)**.**
Sea $f \in K[X]$ un polinomio separable de grado n y E su cuerpo de descomposición sobre K. Denotemos por α_i a las raíces de f en una clausura algebraica $\overline{K}$ de K.

La aplicación $Gal(E/K) \to S_n$ tal que $\sigma \mapsto \tau$ con $\sigma(\alpha_i) = \alpha_{\tau(i)}$ es un monomorfismo de grupos. Denotaremos por $Gal(f/K)$ al subgrupo imagen por este monomorfismo.

Este monomorfismo es la representación de la acción $\phi : Gal(E/K) \times \{1, \dots, n\} \to S_n$ tal que $(g, i) \mapsto \phi(g)(i)$. Una vez reconocido esto, podemos hablar de la transitividad de esta acción y de sus órbitas. En términos de las raíces las órbitas serán aquellas raíces que estén relacionadas mediante un homomorfismo y la acción será transitiva cuando sólo hay una órbita. Los siguientes resultados muestran que las órbitas se corresponden con los factores irreducibles de f.

Proposición 14.2 (Órbitas de la acción generada por la inmersión)**.**
En las condiciones anteriores,

1. *f es irreducible $\iff$ $Gal(f/K) \leq S_n$ es un subgrupo transitivo.*
2. *Supongamos que $f = \prod f_i$ con f_i irreducibles. Las órbitas para la acción ϕ coinciden con el conjunto formado por los conjuntos dados por las raíces de cada f_i.*

El teorema de los irracionales naturales es teorema clásico que permite relacionar los grupos de permutaciones asociados a las raíces de un polinomio en un cuerpo de descomposición cuando cambia el cuerpo base. Para entender el nombre de este teorema debería consultarse [4].

Teorema 14.3 (Teorema de los irracionales naturales)**.**
En las condiciones anteriores, tenemos un monomorfismo de grupos $Gal(f/F) \to Gal(f/K)$ dado por $\phi \to \phi|_E$.

Demostración. Observemos que $E = K(\alpha_1, \dots, \alpha_n)$ y que el cuerpo de descomposición para F sería $F' = F(\alpha_1, \dots, \alpha_n)$.

Dado $\phi \in Gal(F'/F)$ como ϕ determina una permutación de las raíces, entonces $\phi(E) \subseteq E$ y por tanto, $\phi|_E \in Gal(E/K)$.

La aplicación $\phi \to \phi|_E$ es inyectiva ya que si $\phi|_E = \psi_E$ como al extender el homomorfismo se debe preservar el valor sobre las raíces claramente, $\phi = \psi$. También se verifica que es un homomorfismo de grupos ya que para cualquier automorfismo de F', $\phi(E) \subseteq E$, tenemos que $(\phi \circ \psi)|_E = \phi_E \circ \psi|_E$.

Claramente, este monomorfismo se traslada a un monomorfismo de grupos permutaciones si recordamos la inmersión del grupo de Galois en el grupo de permutaciones. □

Corolario 14.4.
Si $Gal(f/K)$ es un grupo simple entonces $Gal(f/F) = Gal(f/K)$ o es trivial.

Demostración. Por el teorema anterior, $Gal(f/F)$ se ve como un subgrupo de $Gal(f/K)$. Pero además es un subgrupo normal. □

Teorema 14.5 (Criterio del discriminante)**.**
En la situación anterior, recordamos que $\Delta f = \prod_{i<j}(\alpha_i - \alpha_j)^2$. Se verifica que Δf es invariante por los elementos de $Gal(f/K)$ y en particular, $\Delta(f) \in K$.

Considerando $\sqrt{\Delta(f)} = \prod_{i<j}(\alpha_i - \alpha_j)$*, observamos que cuando* $car(K) \neq 2$ *entonces los elementos de* $Gal(f/K)$ *que fijan* $\sqrt{\Delta(f)}$ *son exactamente* $Gal(f/K) \cap A_n$*.*

Como consecuencia, $Gal(f/K) \subseteq A_n \iff \Delta(f)$ *es un cuadrado en* K*.*

Demostración. Sea $\sigma \in Gal(f/K) \cap A_n$ y F el cuerpo fijo $Gal(f/K) \cap A_n$ por entonces $\sigma(\sqrt{\Delta(f)}) = \sqrt{\Delta(f)}$ pues el número de trasposiciones de las raíces es par. Por tanto, $\sqrt{\Delta(f)}$ es fijo por el subgrupo y $K(\sqrt{\Delta(f)}) \subseteq F$.

Ahora bien, $Gal(f/K) \cap A_n$ tiene o índice uno o dos.

Si tuviera índice uno entonces $[F : K] = 1$ y por tanto, $F = K$ y por lo anterior tenemos la cadena $F = K = K(\sqrt{\Delta(f)}) \subseteq F$ y en particular, tenemos el enunciado.

Si tuviera índice dos entonces $[F : K] = 2$ entonces tenemos la situación $K \subset F$ y $K \subseteq K(\sqrt{\Delta(f)}) \subseteq F$ y el problema se reduce a determinar si la primera inclusión es propia. Se razona por reducción al absurdo. Se supone que $K(\sqrt{\Delta(f)}) \neq F$ y por tanto, debería haber una permutación impar σ tal que $\sigma(\sqrt{\Delta(f)}) = \sqrt{\Delta(f)}$ pero es claro que también se verifica que $\sigma(\sqrt{\Delta(f)}) = -\sqrt{\Delta(f)}$ de donde $2\sqrt{\Delta(f)} = 0$ y como la característica no es 2 se tendrá que $\sqrt{\Delta(f)} = 0$ en contradicción con que f es separable.

Veamos ahora la consecuencia:

$$Gal(f/K) \subseteq A_n \iff Gal(f/K) \cap A_n = Gal(f/K(\sqrt{\Delta(f)})) \iff Gal(f/K) = Gal(f/K(\sqrt{\Delta(f)})) \iff \sqrt{\Delta(f)} \in K$$

Esto es acaba la consecuencia. □

Referencias

[1] Various Authors. *Counter-example: any algebraic extension is finite*. 2017. URL: https://math.stackexchange.com/questions/2455932/counter-example-any-algebraic-extension-is-finite/2455980#2455980 (visitado 02-10-2017).

[2] Various authors. *Extending Homomorphism into Algebraically Closed Field, year = 2017, url = https://math.stackexchange.com/questions/897660/extending-homomorphism-into-algebraically-closed-field , urldate = 2017-10-13*.

[3] Various authors. *Is the sub-field of algebraic elements of a field extension of K containing roots of polynomials over K algebraically closed?, year = 2017, url = https://math.stackexchange.com/questions/27647/is-the-sub-field-of-algebraic-elements-of-a-field-extension-of-k-containing-ro , urldate = 2017-10-13*.

[4] David A. Cox. *Galois Theory*. Wiley, 2004.

[5] Keith Konrad. *Roots and Irreducibles, year = 2017, url = http://www.math.uconn.edu/ kconrad/blurbs/galoistheory/rootirred.pdf , urldate = 2017-10-13*.

[6] Serge Lang. *Algebra*. Springer, 2002.

[7] Jan Minac Sunil K. Chebolu. *Counting irreducible polynomials over finite fields using the inclusion-exclusion principle*. 2011.