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 $A[X_1, \cdots, X_n]$. $\square$

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 $aX_1^{k_1} \cdots X_i^{k_j} \cdots X_j^{k_i} \cdots X_n^{k_n} \geq a \prod_i X_i^{k_i}$. 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.

$\square$

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 $\alpha \in K(\{y_1, \cdots, y_{max(r,r')}\})$ $\square$

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.

$$\begin{tikzcd} K \arrow[r, "i"] \arrow[d, "i"] & F \ni \alpha \\ K[X] \arrow[ur, "h_\alpha"'] & \end{tikzcd}$$

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 $Ker(h_\alpha) =< f >$. 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, $f = g_1 g_2 = hfg_2 = hg_2 f$ 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, $g \in < f >$ 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. $\square$

La pregunta es, ¿toda extensión algebraica es finita? La respuesta es que no. Véase, [3]

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.
$$\begin{tikzcd} K_1[X] \arrow[r, dashed, "\overline{\sigma}"] \arrow[d, dash] & K_2[X] \arrow[d, dash] \\ K_1 \arrow[r, "\sigma"] & K_2 \end{tikzcd}$$

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 $\overline{\sigma}(f) \in F_2[X]$.*
$$\begin{tikzcd} u \in F_1 \arrow[r, "\tau"] \arrow[d, dash] & F_2 \ni \tau(u) \arrow[d, dash] \\ f \in K_1[X] \arrow[r, "\overline{\sigma}"] \arrow[d, dash] & K_2[X] \ni \overline{\sigma}(f) \arrow[d, dash] \\ K_1 \arrow[r, "\sigma"] & K_2 \end{tikzcd}$$

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 de f_2 en F_2.

$$\begin{tikzcd} u_1 \in F_1 \arrow[r, dash] \arrow[d, dash] & F_2 \ni u_2 \arrow[d, dash] \\ K_1(u_1) \arrow[r, dashed, "\tau"] \arrow[d, dash] & K_2(u_2) \arrow[d, dash] \\ f_1 \in K_1[X] \arrow[r, "\overline{\sigma}"] & K_2[X] \ni f_2 \end{tikzcd}$$

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.

$$\begin{tikzcd} K_1 \arrow[r, "p_1"] \arrow[dr, "p_2 \circ \sigma"'] & K_1[X] \arrow[d, dashed, "\overline{\sigma}"] \\ & K_2[X] \end{tikzcd}$$

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:

$$\begin{tikzcd} K_1[X] \arrow[r, "\overline{\sigma}"] \arrow[d, "p'"] & K_2[X] \arrow[r, "p"] & \frac{K_2[X]}{\langle f_2 \rangle} \\ \frac{K_1[X]}{\langle f_1 \rangle} \arrow[urr, dashed] & & \end{tikzcd}$$

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 .

$$\begin{tikzcd}
F \arrow[rr, "\tau"] \arrow[d, dash] & & F \arrow[d, dash] \\
K(u_1, \ldots, u_k) \arrow[r, "\tau_1"] \arrow[d, dash] & K(u_1, \ldots, u_k) & \\
K \arrow[ur, dash] & &
\end{tikzcd}$$

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_1 y entonces $x - \alpha_1$ es un factor de f en $F_1[X]$ de modo que $f = (x - \alpha_1)g$ con $g \in F_1[X]$ 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 $[L : F_1] \leq (n-1)!$.

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

$$[L : K] = [L : F_1][F(\alpha_1) : K] \leq n!$$

□

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.

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

$E = K(\{u \in F : \exists f \in \mathcal{F}. f(u) = 0\})$ *es un cuerpo de descomposición de $\mathcal{F}$.*

Proposición 3.8 (Unicidad del cuerpo de descomposición de una familia)**.**
El cuerpo de descomposición de una familia de polinomios es único salvo isomorfismo.

4. Clausura algebraica

Definición 4.1 (Cuerpo algebraicamente cerrado).
Un cuerpo que no tiene extensiones algebraicas propias es un cuerpo algebraicamente cerrado.

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 polinomioy 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 teoremade 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.

2. 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 [4]

□

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 algebraica $\frac{E}{K}$, 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 no constante tiene una raíz en E.*

Demostración. Veamos cada una de las equivalencias:

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 $S = \{u \in E : \exists f \in \{.f(u) = 0\}$

□

Proposición 4.4 (Transitividad de la clausura algebraica)**.**
Sea $K \subseteq F \subseteq E$ una torre de cuerpos con $\frac{F}{K}$ una extensión algebraica entonces

$E = \overline{F} \iff E = \overline{K}$.

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 $\tau : E \to \overline{K}$.

$$
\begin{tikzcd}
E \arrow[r, dashed, "\tau"] \arrow[d, dash] & \overline{K} \arrow[dd, dash] \\
F \arrow[ur, "\sigma"] \arrow[d, dash] & \\
K \arrow[r, "Id"] & K
\end{tikzcd}
$$

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 [1] 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 [1]. No está claro que podamos usar los teoremas anteriores porque trabajan con extensiones de isomorfismos no de homomorfismos. □

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 inifito entonces la clausura algebraica tiene el mismo cardinal que K.*

5. Extensiones normales

5.1. Extensiones conjugadas

Definición 5.1 (Elementos conjugados)**.**
$u, v \in \overline{K}$ son conjugados 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 transitividad de la clausura 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 $\sigma(F) = F$.*
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 una raíz en F. Si f no es lineal entonces tendrá alguna raíz v en un cuerpo extensión. Pero las raíces del mismo irreducibles son elementos conjugados sobre K y por tanto existe un automorfismo en $\overline{K}$ que lleva u en v. Este automorfismo restringido a 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.
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 $\sigma(K) = K$ y si tomo una raíz u un polinomio sobre K entonces $\sigma(u)$ es raíz de ese mismo polinomio. Por tanto, σ se puede ver como un endomorfismo en F. Como las extensionesson 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.

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 $\sigma : EF \to \overline{K}$ es un homomorfismo sobre K entonces $\sigma(EF) = \sigma(E)\sigma(F) = EF$ y por tanto la extensión $\frac{EF}{K}$ es normal.
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 transitividad de la clausura algebraica 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.

□

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 $\tau : F \to E$ se extiende a un automorfismo $\overline{\tau} : E \to E$.

$$\begin{tikzcd} E \arrow[r, dashed, "\overline{\tau}"] \arrow[d, dash] & E \\ F \arrow[ur, "\tau"] \arrow[d, dash] & \\ K & \end{tikzcd}$$

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 $\tau : E \to K$. 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

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

Proposición 5.7 (Existencia y unicidad de la clausura normal)**.**
Para toda extensión algebraica $\frac{F}{K}$existe una clausura normal $\frac{E}{K}$ además es única salvo isomorfismo.

Demostración. 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.

Si tengo dos clausuras normalescomo son intersección de normales y ambas lo son deben ser las misma!! (revisar) □

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

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

Demostración. El cuerpo de descomposición de f determina una extensión normal. Además, esta extensión es la mínima que puede ser normal. Continuará. □

Proposición 5.9.
La clausura normal de una extensión finita es finita.

5.4. Polinomio normal

Definición 5.5.
Un polinomio irreducible es normal si en todo extensión algebraica que tenga una raíz del polinomio, este descompone en factores lineales.

Proposición 5.10.
Las siguientes propiedades son equivalentes:

1. f *es normal sobre* K*.*
2. *El cuerop de descomposición de* f *sobre* K *es* $K(u)$ *con* u *una raíz de* f*.*
3. *Todas las raíces de* f *se expresan como polinomios en una cualquiera de ellas.*

6. Extensiones separables y cuerpos perfectos

6.1. Extensiones separables

Definición 6.1 (Separabilidad).
Sea K un cuerpo.

1. Un polinomio irreducible $p \in K[X]$ es separable si todas son raíces en un cuerpo de descomposición son simples (la multiplicidad de las raíces no depende del cuerpo de descomposición considerado).
2. Un polinomio $p \in K[X]$ es separable si sus factores irreducibles son separables.
3. Un elemento algebraico u sobre un cuerpo K es separable si $Irr(u, K)$ es separable.
4. Una extensión algebraica $\frac{F}{K}$ es separable si todos los elementos de F son separables sobre K.

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

Proposición 6.1 (Torres separables).
Sea $E \supseteq F \supseteq K$ una torre de cuerpos.

Si $\frac{E}{F}$ es una extensión separable entonces $\frac{E}{F}, \frac{F}{K}$ son extensiones separables.

Demostración. $\frac{F}{K}$ es separable ya que todo elemento de E es sobre K y todo elemento de F está en E.

Para ver que $\frac{E}{F}$ es separable sea $u \in E$ entonces claramente $Irr(u, F)|Irr(u, K)$ ya que $gr(Irr(u, F)) \leq gr(Irr(u, K))$ y como $Irr(u, K)(u) = 0$ claramente $Irr(u, K) \in \langle Irr(u, F)\rangle$ y como $Irr(u, K)$ no tiene raíces múltiples, tampoco puede tenerlas $Irr(u, F)$. □

6.2. Cuerpos perfectos

Definición 6.2 (Cuerpo perfecto).
Un cuerpo K es perfecto si se cumplen alguna de las condiciones de la siguiente proposición.

Proposición 6.2.
Sea K un cuerpo. Las siguientes condiciones son equivalentes:

1. *Todo polinomio $p \in K[X]$ es separable.*
2. *Todo α algebraico sobre K es separable.*
3. *Toda extensión algebraica es separable.*
4. *Toda extensión finita es separable.*

Proposición 6.3.
1. *Todo cuerpo de característica 0 o finito es perfecto.*
2. *Todo cuerpo de característica prima no nula es perfecto si y sólo si el endomorfismo de Frobenius es un automorfismo.*

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

7. Teoría de Galois Finita

Sea $Hom(\frac{F}{K}, \frac{E}{K})$ de homomorfismos de cuerpos entre $\frac{F}{K}$ y $\frac{E}{K}$.

Sea $Hom_K(F, E)$ el conjunto de homomorifismos de K-espacios vectoriales.

Proposición 7.1.
Damos estructura a los espacios anteriores.

1. $Hom(\frac{F}{K}, \frac{E}{K}) \subseteq Hom_K(F, E)$
2. $Hom_K(F, E)$ *tiene estrucutra de* E*-espacio vectorial.*

Demostración. □

8. Cuerpos finitos

8.1. Existencia y unicidad

Proposición 8.1.
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 8.1.
Sea A un anillo.

La característica de A, $car(A)$, es el número entero positivo o nulo n tal que $Ker(f) = n\mathbb{Z}$.

Obsérvese que es una buena definición ya que $\mathbb{Z}$ es un dominio de ideales principales.

Proposición 8.2 (Propiedades de la característica)**.**
1. 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 $\forall a \in A.na = 0$.

2. Si A es un dominio de integridad entonces $Car(A)$ es cero o un número primo.

3. Sea A un anillo de característica prima p entonces la aplicación $R(a) = a^p$ es un endomorfismo conocido como endomorfismo de Frobenius.

4. Si $f : A \to B$ es un homomorfismo entonces $car(B)|car(A)$.

Demostración. 1. Utilícese el primer teorema de isomorfía y la definición de característica.

2. 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.

3. 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.

4. $0 = f(0) = f(1Car(A)) = 1Car(A)$ y como $Car(B)$ debe ser el mínimo que anule a uno, tendrá que ser $Car(B)|Car(A)$. □

Teorema 8.3.
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, 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 $U = K - \{0\}$. 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:

- $(u+v)^{p^n} - (u+v) = u^{p^n} - u + v^{p^n} - v = 0$
- $(uv)^{p^n} - uv = u^{p^n} v^{p^n} - uv = 0$
- $(-u)^{p^n} - (-u) = 0$
- $(u^{-1})^{p^n} - u^{-1} = 0$
- $(1)^{p_n} - 1 = 0$

□

Proposición 8.4.
Sea $F^x = F - \{0\}$ el grupo de las unidades para el producto del cuerpo finito F. Se verifica que F^x es un grupo cíclico de orden $|F| - 1$.

Demostración. Ver [2] □

Proposición 8.5.
Si $f \in \mathbb{F}_p[X]$ entonces el número de raíces de f in $\mathbb{F}_{p^n}$ es el grado del polinomio $gcd(f, X^{p^n} - X)$.

Demostración. Ver Cox, 291. □

Proposición 8.6 (Retículo de subcuerpos de un cuerpo finito)**.**
Sean $\mathbb{F}_{q^m}, \mathbb{F}_{p^n}$ cuerpos finitos. Entonces $\mathbb{F}_{q^m}$ es isomorfo a un subcuerpo de $\mathbb{F}_{p^n}$ si y sólo si $p = q \wedge m|n$.

Demostración. $\Rightarrow$) 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 $m|n$.

$\Leftarrow$) Hay que utilizar extensiones de Galois o bien utilizar otras herramientas de la característica como en [**4**]. ☐

8.2. Polinomios irreducibles sobre cuerpos finitos

La representación de cuerpos finitos $\mathbb{F}_{p^n}$ como cocientes $\frac{F_p[X]}{f}$ con $f \in \mathbb{F}_p[X]$ un polinomio irreducible de grado n es esencial en los computadores. Necesitamos por tanto, un buen conocimiento de los polinomios irreducibles sobre $\mathbb{F}_p[X]$.

Proposición 8.7 (Raíces de un irreducible en $\mathbb{F}_p$)**.**
Sea $p \in \mathbb{F}_p[X]$ un irreducible de grado d. Consideremos un cuerpo extensión F donde p tiene una raíz α. Entonces p admite d raíces distintas α^{p^i} con $i = 0, \cdots, d-1$.

Demostración. [5] ☐

Proposición 8.8.
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.

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, $gr(g) = [\mathbb{F}(\alpha) : \mathbb{F}_p] | [\mathbb{F}_{p^n} : \mathbb{F}_p]1$

$\Leftarrow$ 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 $\mathbb{F}(\alpha) \cong \mathbb{F}_{p^m}$ 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 más detalles véase [5]

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

Proposición 8.9.
$\sum_{m|n} m|N_m| = p^n$

Demostración. Vimos en la prueba del teorema de Moore que $X^{p^n} - X$ es separable y en particular sus raíces en cuerpo de descomposición son todas simples. Esto implica que sus factores irreducibles en $\mathbb{F}_p[X]$ son todos distintos. Además como es mónico, podemos obtener su factorización como producto de polinomios mónicos.

La proposición anterior nos dice que debemos considerar como factores todos los irreducibles sobre $\mathbb{F}_p[X]$ que tengan grado divisor de n. 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 8.10.
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. □

Pero no sólo podemos calcular los polinomios mónicos irreducibles de grado primo. Veamos un ejemplo:

EJEMPLO 8.1: 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, $N_1 = p$.

El teorema implica que $p^2 = 2|N_2| + |N_1| = 2|N_2| + p$ luego $|N_2| = \frac{p^2 - p}{2}$, análogamente, $|N_4| = \frac{p^4 - p^2}{4}$.

Vamos a generalizar esta fórmulas para el cálculo del número de polinomios irreducibles.

Definición 8.2 (Función de Mobius)**.**

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

Teorema 8.11.
$N_n = \frac{1}{n} \sum_{m|n} \mu(m) p^{\frac{n}{m}}$

Demostración. Ver COUNTING IRREDUCIBLE POLYNOMIALS OVER FINITE FIELDS USING THE INCLUSION-EXCLUSION PRINCIPLE □

Referencias

[1] Various authors.

[2] Various Authors. *Confusion about the proof that the multiplicative group of a finite field is cyclic.* 2017. URL: https://math.stackexchange.com/questions/1434065/confusion-about-the-proof-that-the-multiplicative-group-of-a-finite-field-is-cyc?rq=1 (visitado 13-10-2017).

[3] 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).

[4] 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.*

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