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

□

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.

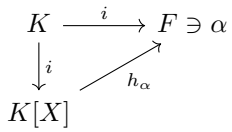
Claramente $EF = E(F) = F(E)$.

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.



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. □

La pregunta es, ¿toda extensión algebraica es finita? La respuesta es que no. Véase, [2]

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. Clausura algebraica

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

Haciendo $\alpha = x+ < f >$ si $f = \sum a_i X^i$ entonces

$$f(\alpha) = \sum (a_i+ < f >)(x+ < f >)^i = (\sum a_i x^i)+ < f >= f+ < f >= 0+ < f >$$

Esto es $f(\alpha) = 0$. □

Lema 3.2.
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.*
5. *No existen extensiones algebraicas $\frac{F}{K}$ con $F \neq K$.*

Definición 3.1 (Cuerpo algebraicamente cerrado)**.**
Un cuerpo K es algebraicamente cerrado si cumple cualquiera de las condiciones anteriores.

Teorema 3.3 (Teorema de Steinitz)**.**
Si K es un cuerpo existe un cuerpo algebraicamente cerrado F extensión de K.

Corolario 3.4.
Si K es un cuerpo, existe una extensión de K que es algebraica y algebraicamente cerrada.

Definición 3.2 (Clausura algebraica)**.**
Una extensión de cuerpos $\frac{F}{K}$ es una clausura algebraica de K si

1. Es una extensión algebraica.
2. F es un cuerpo algebraicamente cerrado.

4. Cuerpos de descomposición

Definición 4.1 (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 f factoriza en $F[X]$ como producto de polinomios lineales, esto es, $f = c\prod(X - \alpha_i)$ con $c \in K$ y $\alpha_i \in E$ y además verifica la propiedad de que f no descompone en ningún subcuerpo intermedio F, es decir, E es el menor cuerpo donde esto ocurre.

Proposición 4.1 (Existencia del cuerpo de descomposición)**.**
Sea $f \in K[X]$ un polinomio no constante de grado n y raíces α_i.

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

Demostración. 1. 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 $E = K$ entonces tomando $\alpha_1 = -a_1/a_0$ tenemos que $f = a_0(x - \alpha_1)$ y esto termina este caso.

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 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.

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.

2. Por inducción sobre n. (Ver Cox, 102) □

Teorema 4.2 (Unicidad del cuerpo de descomposición)**.**
Dados dos cuerpos F_1, F_2 isomorfos mediante un isomorfismo de cuerpos ϕ. Sea $f_1 \in F_1[X]$, sea $f_2 = \phi(f_1) \in F_2[X]$. Considérense los cuerpos de descomposición L_1, L_2 de f_1, f_2. Existe un isomorfismo $\overline{\phi}$ entre L_1 y L_2 que extiende a ϕ.

$$\begin{array}{ccc} L_1 & \xrightarrow{\overline{\phi}} & L_2 \\ \big| & & \big| \\ F_1 & \xrightarrow{\phi} & F_2 \end{array}$$

En particular, si L_1, L_2 son dos cuerpos de descomposición de $f \in F[X]$ entonces hay un isomorfismo entre las extensiones L_1, L_2 tal que es la identidad en F. Por tanto, el cuerpo de descomposición de un polinomio es único salvo isomorfismo.

Demostración. Hagamos inducción sobre $n = gr(f_1) = gr(f_2)$.

Si $n = 1$ entonces por la proposición anterior $[L_i : F_i] = 1$ y en particular, $L_1 = F_1$ y $L_2 = F_2$ y basta tomar $\overline{\phi} = \phi$.

Supongamos $n > 1$. Podemos asumir $L_1 = F_1(\alpha_1, \ldots, \alpha_n)$ con α_i raíces f_1 (fíjate que no asumimos lo mismo para L_2). Utilicemos la extensión $F_1(\alpha_1)$ observando que L_1 será el cuerpo de descomposición para el polinomio $g_1 = \frac{g_1}{x-\alpha_1}$. Procedemos en 5 pasos.

1. Sea $h_1 = Irr(\alpha_1, F_1[X])$ tenemos $F_1(\alpha_1) \cong \frac{F_1[X]}{\langle h_1 \rangle}$ con un homomorfismo que lleva α_1 a $x + \langle h_1 \rangle$.

2. Vamos a encontrar una raíz de f_2 que se corresponda con α_1. El punto importante es que ϕ induce un isomorfismo $\hat{\phi}$ entre los respectivos anillos de polinomios. Este isomorfismo lleva factores en factores e irreducibles en irreducibles luego en particular lleva a h_1 en un factor irreducible h_2 de f_2. Como f_2 descompone completamente sobre L_2 también le ocurre lo mismo a h_2 (ver los puntos 4.1.2 a 4.1.4 de los apuntes de Mario para confirmar esto). Por tanto, podemos etiquetar las raíces como $\beta_1, \ldots, \beta_n \in L_2$ con β_1 raíz de h_2.

3. La raíz β_1 de f_2 nos da una extensión $F_2(\beta_1)$ y L_2 será un cuerpo de descomposicón para $g_2 = \frac{f_2}{x-\beta_1}$ y como en el paso 1 también $F_2(\beta_1) \cong \frac{F_2[X]}{\langle h_2 \rangle}$ ya que h_2 es el polinomio mínimo de β_1 (porque es irreducible y β_1 es raíz de él). Este isomorfismo lleva β_1 en $x + \langle h_2 \rangle$.

4. Como $\hat{\phi}$ lleva h_1 en h_2, también lleva los $\langle h_1 \rangle$ en $\langle h_2 \rangle$ y por tanto, tenemos un isomorfismo entre los anillos cocientes de manera natural actuando como ϕ en los coeficientes y $x + \langle h_1 \rangle$ en $x + \langle h2 \rangle$. Por tanto, tenemos el siguiente isomorfismo

$$\phi_1 : F_1(\alpha_1) \cong \frac{F_1[X]}{\langle h_1 \rangle} \cong g_2 = \frac{f_2}{x - \beta_1} \cong F_2(\beta_1)$$

tal que lleva α_1 en β_1 y sobre F_1 actúa como ϕ.

5. En particular, lleva g_1 en g_2. Entonces tenemos la siguiente situación:

$$\begin{array}{ccc} L_1 & & L_2 \\ | & & | \\ F_1(\alpha_1) & \xrightarrow{\phi_1} & F_2(\beta_1) \\ | & & | \\ F_1 & \xrightarrow{\phi} & F_2 \end{array}$$

Como g_1 tiene grado $n-1$, el paso 5. implica que podemos aplicar la hipótesis de indución a g_1 y ϕ_1, lo que me da un isomorfphismo $\overline{\phi_1}$ cuya restricción a $F_1(\alpha_1)$ es ϕ_1 pero como $\phi_1|_{F_1} = \phi$ se sigue que la restricción de $\overline{\phi_1}$ a F_1 es ϕ.

Para el corolario basta tomar ϕ la identidad. □

El siguiente resultado se reaprovecha en teoría de Galois.

Proposición 4.3.
Sea L un cuerpo de descomposición de un polinomio de $F[X]$ y suponga que $h \in F[x]$ es irreducible y tiene dos raíces $\alpha, \beta \in L$. Entonces existe un isomorfismo de cuerpos que es la identidad en F y lleva α en β.

5. Extensiones normales

Proposición 5.1.
Sea L un cuerpo de descomposición de $f \in F[X]$ y sea $g \in F[X]$ irreducible. Si g tiene una raíz en L entonces g descompone completamente en L.

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 $\omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$.

6. Extensiones separables

7. Cuerpos finitos

7.1. Existencia y unicidad

Proposición 7.1.
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 7.1.
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 7.2 (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 7.3.
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 7.4.
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 [1] □

Proposición 7.5.
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 7.6 (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**]. □

7.2. 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 7.7 (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. [3] □

Proposición 7.8.
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, $gr(g) = [\mathbb{F}(\alpha) : \mathbb{F}_p]|[\mathbb{F}_{p^n} : \mathbb{F}_p]$l

$\Leftarrow$ 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 [3]

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

Proposición 7.9.
$\sum_{m|n} m|N_m| = p^n$

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 7.10.
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. □

Referencias

[1] 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).

[2] 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).

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