Álgebra Computacional

Pablo Pallàs

4 de abril de 2023

Índice

1. Bases de Groebner

1.1. Orden en los monomios de $K[x_1, \ldots, x_n]$ y división

Para cada $(\alpha_1, \ldots, \alpha_n) = \alpha \in \mathbb{N}^n$ tenemos un monomio $x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in K[x_1, \ldots, x_n]$ y viceversa.

Definición 1.1. *Diremos que tenemos un* ***orden monomial*** *en $\mathbb{N}^n$ si se verifican las siguientes condiciones para unos $\alpha, \beta \in \mathbb{N}^n$:*

1. *$>$ es orden total en $\mathbb{N}^n$, es decir, ó bien $\alpha > \beta$ ó $\beta > \alpha$ para todo $\alpha, \beta \in \mathbb{N}^n$.*
2. *Si tenemos que $\alpha > \beta$, entonces $\alpha + \gamma > \beta + \gamma$, es decir, al multiplicar por un monomio se mantiene el orden.*
3. *Todo subconjunto no vacío A de $\mathbb{N}^n$ tiene un elemento que es menor que todos los demás, un elemento mínimo. Esto es equivalente a decir que el conjunto está bien ordenado para $>$, es decir, que $\exists \alpha \in A$ tal que $\alpha < \beta \; \forall \beta \in A$. Esto* ***es equivalente a que toda sucesión decreciente de*** *$\alpha_i \in A$* ***se estaciona****.*

Observación 1.1.1. *Notar que en cualquier orden monomial se tiene que* $\alpha > 0 = (0, \ldots, 0)$ *para todo* α*. Esto es así ya que si* $\alpha < 0$ *se tendría que, sumando* α *en cada paso, la serie*

$$0 > \alpha > 2\alpha > 3\alpha > \ldots$$

se estacionaría por la tercera condición antes expuesta, es decir, tendríamos que $n\alpha = (n-1)\alpha$*, luego* $\alpha = 0$*. Más adelante veremos que el recíproco también es cierto.*

Notar también que si $n = 1$ el único orden monomial es el orden natural en $\mathbb{N}$.

Aunque aquí hayamos escogido $\mathbb{N}^n$ los órdenes monomiales son ordenaciones de monomios de un anillo, normalmente para establecer un algoritmo de división en polinomios de varias variables. El anillo en cuestión es $K[x_1, \ldots, x_n]$, con K un cuerpo.

Veamos dos órdenes monomiales concretos:

Definición 1.2. ***Orden lexicográfico****, denotado por* $>_{lex}$*. Si* $\alpha, \beta \in \mathbb{N}^n$ *diremos que* $\alpha >_{lex}$ *si en* $\alpha - \beta$ *la primera componente no nula empezando por la izquierda es positiva. Notar que es importante el orden de las variables.* ***Orden graduado lexicográfico****, denotado* $>_{grlex}$*. Si* $\alpha, \beta \in \mathbb{N}^n$ *diremos que* $\alpha >_{grlex} \beta$ *si*

$$|\alpha| = \sum_{i=1}^{n} a_i > |\beta| = \sum_{i=1}^{n} \quad \text{ó} \quad |\alpha| = |\beta|, a >_{lex} \beta.$$

Definición 1.3. *Sea* $0 \neq f = \sum_\alpha a_\alpha x^\alpha \in K[x_1, \ldots, x_n]$ *con un orden monomial* $>$*. Entonces:*

- *El* ***multigrado*** *de* f *es* $multideg(f) = max\{\alpha \in \mathbb{N}^n : a_\alpha \neq 0\}$.
- *El* ***coeficiente director*** *de* f *es* $LC(f) = a_{multideg(f)} \in K$.
- *El* ***monomio director*** *de* f *es* $LM(f) = x^{multideg(f)} \in K$.
- *El* ***término director*** *de* f *es* $LT(f) = LC(f)LM(f)$.

Teorema 1.4 (***Algoritmo de la división en*** $K[x_1, \ldots, x_n]$)**.** *Sea* $>$ *un orden monomial y sea* $F = (f_1, \ldots, f_s)$ *una s-tupla de polinomios en* $K[x_1, \ldots, x_n]$*. Para todo* $f \in K[x_1, \ldots, x_n]$ *existen* $a_1, \ldots, a_s, r \in K[x_1, \ldots, x_n]$ *tales que*

$$f = a_1 f_1 + \ldots a_s f_s + r,$$

con $r = 0$ *ó una combinación lineal en* K *de monomios que no son divisibles por ninguno de los* $LT(f_1), \ldots, LT(f_s)$*. Diremos que* r *es un resto de la división de* f *por* F*.*

Demostración: Partimos de un $p = f$, $r = 0$ y $a_i = 0$, de manera trivial tenemos que

$$f = a_1 f_1 + \ldots a_s f_s + p + r.$$

Si $LT(p)$ es divisible por algún $LT(f_i)$ cambiamos a_i por $a_i + LT(p)/LT(f_i)$ y p oir $p - f_i(LT(p)/LT(f_i))$ siguiendo el orden $i = 1, \ldots, s$. Notar que en cada paso se mantiene la igualdad

$$f = a_1 f_1 + \ldots a_s f_s + p + r$$

y además se tiene que el término director de $f_i(LT(p)/LT(f_i))$ es $LT(p)$, luego el monomio director del nuevo p es menor estricto que el que tenía el p anterior. Además, los monomios que añadimos a cada a_i al multiplicarlos por f_i tienen como monomio director $LM(p)$, luego menor que el monomio director de f y en cada paso de $multideg(f) \geq multideg(a_i f_i)$. Hacemos esto hasta llegar a un p tal que su monomio director no es divisible por ninguno de los monomios directores de f_i. Si $p = 0$ ya está, en otro caso camviamos p por $p - LT(p)$ y r por $r + LT(p)$. Se sigue teniendo la igualdad y los términos de r no son divisibles por ninguno de los $LT(f_i)$. En este paso también conseguimos un p con monomio director más pequeño. Continuamos así hasta llegar a $p = 0$.

□

Ejemplo 1.4.1. *Vamos a calcular el resto y los coeficientes de la división de* $f = x^2y + xy^2 + y^2$ *por el conjunto de los polinomios* $F = (y^2 - 1, xy - 1)$ *siguiendo el orden lexicográfico.*

Notar que en f *tenemos un monomio elevado a* $\alpha = (2, 1)$*, un monomio* $\beta = (1, 2)$ *y un monomio* $\gamma = (0, 2)$*. Así que tenemos que* $\alpha >_{lex} \beta >_{lex} \gamma$*, luego* $LT(f) = x^2y$*. Del conjunto* F *llamaremos* $f_1 = y^2 - 1$ *y* $f_2 = xy - 1$*, y tenemos claramente que* $LT(f_1) = y^2$ *y* $LT(f_2) = xy$*.*

Comenzamos poniendo $f = a_1f_1 + a_2f_2 + p + r$*, con* $r = a_1 = a_2 = 0$ *y* $p = f = x^2y + xy^2 + y^2$*. Ahora,* $LT(p) = x^2y$ *es divisible por* $LT(f_2) = xy$ *y* $LT(p)/LT(f_2) = x^2y/xy = x$ *luego podemos sustituir* a_2 *por* $a_2 + x$*,* p *por* $p - xf_2 = x^2y + xy^2 + y^2 - x^2y + x = xy^2 + y^2 + x$*.*

Ahora tenemos $f = a_1f_1 + xf_2 + p + r$*, con* $a_1 = r = 0$ *y* $p = xy^2 + y^2 + x$*.* $LT(p) = xy^2$ *es divisible por* $LT(f_1) = y^2$ *y* $LT(p)/LT(f_1) = xy^2/y^2 = x$ *luego podemos sustituir* a_1 *por* $a_1 + x$ *y* p *por* $p - xf_1 = xy^2 + y^2 + x - xy^2 + x = y^2 + 2x$*.*

Tenemos $f = xf_1 + xf_2 + p + r$*, con* $r = 0$ *y* $p = y^2 + 2x$*.* $LT(p) = 2x$ *no es divisible ni por* $LT(f_1)$ *ni por* $LT(f_2)$*, pero si hacemos* $p = y^2$ *y* $r = 2x$ *entonces* $LT(p) = y^2$ *sí es divisible por* $LT(f_1) = y^2$ *y* $LT(p)/LT(f_1) = 1$ *luego podemos sustituir* $a_1 = x$ *por* $a_1 + 1 = x + 1$ *y* p *por* $p - f_1 = y^2 - y^2 + 1 = 1$*. Así que queda* $f = xf_1 + f_1 + xf_2 + p + r$*, con* $p = 1$ *y* $r = 2x$*. Si hacemos que* $p = 0$ *y* $r = 2x + 1$ *ya está:*

$$f = xf_1 + f_1 + xf_2 + 2x + 1.$$

■

1.2. Ideales monomiales. Lema de Dickson

Definición 1.5. *Un ideal* I *de* $K[x_1, \ldots, x_n]$ *diremos que es* ***ideal monomial*** *si se puede generar por monomios, es decir, si existe un subconjunto* $A \subseteq \mathbb{N}^n$ *tal que* $I = \langle x^\alpha : \alpha \in A \rangle$*.*

Notar que I estará formado por lo polinomios que son una suma finita de la forma

$$\sum_\alpha h_\alpha x^\alpha, \quad h_\alpha \in K[x_1, \ldots, x_n].$$

Proposición 1.6. *Dado un ideal monomial $I = \langle x^\alpha : \alpha \in A \rangle$, con $A \subseteq \mathbb{N}^n$, se tiene que:*

- *Dado un $\beta \in \mathbb{N}^n$, $x^\beta \in I$ si y sólo si x^β es múltiplo de x^α para algún $\alpha \in A$.*
- *Para un $f \in K[x_1, \ldots, x_n]$ se tiene que $f \in I$ si y sólo si todos los términos de f están en I.*
- *Para un $f \in K[x_1, \ldots, x_n]$ se tiene que $f \in I$ si y sólo si f es combinación lineal con coeficientes en K de monomios de I.*

Demostración: Es un sencillo ejercicio.

□

Corolario 1.6.1. *Dos ideales monomiales son el mismo si y sólo si contienen los mismos monomios.*

Si $n = 2$ podemos representar los monomios en el plano $\mathbb{Z} \times \mathbb{Z}$ y los ideales generados por un conjunto de monomios serán una región de ese plano.

Ejemplo 1.6.1. *Podemos representar el ideal $I = \langle x^4y^2, x^3y^4, x^2y^5 \rangle$ usando lo que se conoce como **diagrama de Young** ya que $n = 2$ y podemos usar un plano $\mathbb{Z} \times \mathbb{Z}$. Del primer monomio sacamos $\alpha = (4, 2)$, del segundo $\beta = (3, 4)$ y del tercero $\gamma = (2, 5)$. El conjunto de puntos $S = \{(4, 2), (3, 4), (2, 5)\}$ también lo conoceremos como el grafo del ideal monomial I.*

Teorema 1.7 (*Lema de Dickson*). *Sea $A \subseteq \mathbb{N}^n$, $I = \langle x^\alpha : \alpha \in A \rangle$ un ideal monomial. Entonces existen $\alpha_1, \ldots, \alpha_s \in A$ tales que $I = \langle x^{\alpha_1}, \ldots, x^{\alpha_n} \rangle$. En particular, I tiene una base finita.*

Demostración: Lo haremos por inducción sobre n. Para $n = 1$, $A \subseteq \mathbb{N}$ y existe un $\beta \in A$ tal que $\beta \leq \alpha$ para todo $\alpha \in A$. Se tiene que $I = \langle x^\alpha : \alpha \in A \rangle = \langle x^\beta \rangle$.

Supongamos ahora que $n > 1$ y que el teorema es cierto para $n - 1$. Llamaremos $y = xn$ y todos los monomios de $K[x_1, \ldots, x_{n-1}, y]$ son de la forma $x^\alpha y^r$, siendo $\alpha \in \mathbb{N}^{n-1}$ y $r \in \mathbb{N}$.

Sea I un ideal monomial de $K[x_1, \ldots, x_{n-1}, y]$. Sea J el ideal de $K[x_1, \ldots, x_{n-1}]$ generado por los monomios x^α, con $\alpha \in \mathbb{N}^{n-1}$, para los que existe $r \in \mathbb{N}$ de modo que $x^\alpha y^r \in I$.

(Considerando el homomorfismo de anillos $K[x_1, \ldots, x_{n-1}, y] \longrightarrow K[x_1, \ldots, x_{n-1}]$ sustitución de y por 1, entonces J está generado por las imágenes de los monomios de I y se le llama proyección de I en $K[x_1, \ldots, x_{n-1}]$.)

Por hipótesis de inducción existen $\alpha_1, \ldots, \alpha_s \in \mathbb{N}^{n-1}$ y $m_1, \ldots, m_s \in \mathbb{N}$ tales que

$$J = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle, \quad x^{\alpha_i} y^{m_i} \in I, i = 1, \ldots, s.$$

Sea m el mayor de los m_i. Un monomio cualquiera de I será de la forma $x^\beta y^r$, con $\beta \in \mathbb{N}^{n-1}$, $r \in \mathbb{N}$. Y como $x^\beta \in J$ se tiene que x^β es múltiplo de algún x^{α_i}. Si $r > m$, nuestro monomio es múltiplo de alguno de los siguientes monomios: $x^{\alpha_1} y^m, \ldots, x^{\alpha_s} y^m$.

Ahora pensemos en los monomios $x^\beta y^r$ con $r < m$. Para cada k entre 0 y $m-1$ consideramos los monomios de I de la forma $x^\beta y^k$, con $\beta \in \mathbb{N}^{n-1}$, y hacemos su proyección sobre $K[x_1, \ldots, x_{n-1}]$ y llamamos J_k al ideal de $K[x_1, \ldots, x_{n-1}]$ que generan las imágenes, es decir,

$$J_k = \langle x^\beta \rangle \subseteq K[x_1, \ldots, x_{n-1}], x^\beta y^k \in I.$$

Otra vez por hipótesis de inducción existen $\alpha_{k1}, \ldots, \alpha_{ks} \in \mathbb{N}^{n-1}$ tales que

$$J_k = \langle x^{\alpha_{k1}}, \ldots, x^{\alpha_{ks}} \rangle, \quad x^{\alpha_{ki}} y^k \in I, i = 1, \ldots, s.$$

Vamos a buscar en I los monomios cuyas proyecciones me dan estos conjuntos finitos de generadores. De J_0, $x^{\alpha_{01}}, \ldots, x^{\alpha 0 s}$. De J_1, $x^{\alpha_{11}} y, \ldots, x^{\alpha_{1s}} y$. De J_k, $x^{\alpha_{k1}} y^k, \ldots, x^{\alpha_{ks}} y^k$. De J_{n-1}, $x^{\alpha_{n-11}} y^{n-1}, \ldots, x^{\alpha_{n-1s}} y^{n-1}$ y añadimos los múltiplos de los generadores de J, $x^{\alpha_1} y^m, \ldots, x^{\alpha_s} y^m$.

Tenemos así un conjunto finito de monomios de I. Sea $x^\alpha y^p$ un monomio en I, con $\alpha \in \mathbb{N}^{n-1}, p \in \mathbb{N}$. Se tiene que $x^\alpha \in J$ y por tanto es múltiplo de algún x^{α_i} y si $p > m$ se tiene que $x^\alpha y^p$ es múltiplo de alguno de los monomios $x^{\alpha_1} y^m, \ldots, x^{\alpha_s} y^m$.

Si $p < m$, $x^\alpha \in J_p$ luego es múltiplo de algún $x^{\alpha_{pi}}$ y $x^\alpha y^p$ es múltiplo de alguno de los $x^{\alpha_{p1}} y^p, \ldots, x^{\alpha_{ps}} y^p$.

Así, hemos visto que el ideal generado por este conjunto finito e I tienen los mismos monomios y por la proposición anterior son el mismo ideal.

Para terminar, supongamos que $A \subseteq \mathbb{N}^n$ y $I = \langle x^\alpha : \alpha \in A \rangle$. Ya hemos probado que existen $\beta_1, \ldots, \beta_s \in \mathbb{N}^n$ tales que $I = \langle x^{\beta_1}, \ldots, x^{\beta_s} \rangle$. Por 1.6 existen $\alpha_1, \ldots, \alpha_s \in A$ tales que x^{β_i} es múltiplo de x^{α_i} y se tiene que $I = \langle x^{\beta_1}, \ldots, x^{\beta_s} \rangle \subseteq \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle \subseteq I$. Luego $I = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle$.

□

Corolario 1.7.1. *Sea $>$ una relación de orden total en $\mathbb{N}^n$ que verifica que si $\alpha > \beta$ se tiene que $\alpha + \gamma > \beta + \gamma$ para todo $\alpha, \beta, \gamma \in \mathbb{N}^n$.*

Tenemos además que es un orden monomial si y sólo si $\alpha > 0$ para todo $\alpha \in \mathbb{N}^n$.

Demostración: Ya sabemos que en los órdenes monomiales $\alpha > 0$ para todo $\alpha \in \mathbb{N}^n$

Para el recíproco, sea $A \subseteq \mathbb{N}^n$. Consideremos $I = \langle x^\alpha : \alpha \in A \rangle$ y por el *Lema de Dickson* existen $\alpha_1, \ldots, \alpha_s \in A$ tales que $I = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle$. Por ser un orden total podemos suponer que $\alpha_1 < \alpha_i$ para $i = 2, \ldots, s$.

Sea $\alpha \in A$, por ser $x^\alpha \in I$, x^α es múltiplo de algún x^{α_i}, con $i = 1, \ldots, s$, luego existe $\gamma \in \mathbb{N}^n$ tales que $\alpha = \alpha_i + \gamma$.

Por hipótesis $\gamma > 0$, luego $\alpha = \alpha_i + \gamma > \alpha_i > \alpha_1$ y tenemos que α_1 es mínimo en A.

□

Notar que de las primeras líneas de la demostración del *Lema de Dickson* sacamos que, dado un $\alpha in \mathbb{N}^n$,

$$\langle \alpha \rangle = \{\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n : \beta_i \geq \alpha_i, i = 1, \ldots, n\}$$

y así $\langle x^\alpha \rangle = \{x^\beta : \beta \in \mathbb{N}^n\}$ tal que $\alpha \leq \beta$.

1.3. El Teorema de la base de Hilbert

Definición 1.8. *Sea I un ideal no nulo de $K[x_1, \ldots, x_n]$. Consideremos el siguiente conjunto:*

$$LT(I) = \{cx^\alpha : \exists f \in I : LT(f) = cx^\alpha\}.$$

Entonces el conjunto $LT(I)$ genera un ideal monomial. Hay que tener en cuenta que si $I = \langle f_1, \ldots, f_s \rangle$ se tiene obviamente que

$$\langle LT(f_1), \ldots, LT(f_s) \rangle \subseteq \langle LT(I) \rangle.$$

Veamos que este contenido puede ser estricto:

Ejemplo 1.8.1. *En $K[x, y]$ con el orden grlex consideramos $I = \langle x^3 - 2xy, x^2y - 2y^2 + x \rangle$. Se tiene que $\langle LT(x^3 - 2xy), LT(x^2y - 2y^2 + x) \rangle = \langle x^3, x^2y \rangle$. Ahora:*

$$-y(x^3 - 2xy) + x(x^2y - 2y^2 + x) = x^2 \in I \Longrightarrow x^2 \in \langle LT(I) \rangle$$

pero $x^2 \notin \langle LT(x^3 - 2xy), LT(x^2y - 2y^2 + x) \rangle = \langle x^3, x^2y \rangle$.

■

Proposición 1.9. *Sea I un ideal no nulo de $K[x_1, \ldots, x_n]$, se tiene que $\langle LT(I) \rangle$ es un ideal monomial, y por el Lema de Dickson $\exists g_1, \ldots, g_s \in I$ tales que $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_s) \rangle$.*

Teorema 1.10 (***Teorema de la base de Hilbert***)**.** *Todo ideal I de $K[x_1, \ldots, x_n]$ es finitamente generado, es decir, que existen $g_1, \ldots, g_t \in I$ tales que $I = \langle g_1, \ldots, g_t \rangle$.*

Demostración: Si $I = 0$ la afirmación es trivial. En otro caso, por la proposición anterior sabemos que existen $g_1, \ldots, g_t \in I$ tales que $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$. Veamos que $I = \langle g_1, \ldots, g_t \rangle$. Un contenido es evidente: $\langle g_1, \ldots, g_t \rangle \subseteq I$.

Sea $f \in I$. Por el algoritmo de la división existen $a_1, \ldots, a_s, r \in K[x_1, \ldots, x_n]$ tales que $f = a_1g_1 + \ldots a_tg_t + r$, con $r = 0$ ó una combinación lineal con coeficientes en K de monomios que no son divisibles por ninguno de los $LM(g_1), \ldots, LM(g_t)$. Tenemos ahora que $r = f - (a_1g1 + \ldots + a_tg_t)$, luego $LT(r) \in \langle LT(I) \rangle = \langle LT(g_1, \ldots, LT(g_t) \rangle$ y si fuera no nulo sería múltiplo de algún $LT(g_i)$, absurdo por la definición de r. Así, $r = 0$ y $f \in \langle g_1, \ldots, g_t \rangle$ luego $I \subseteq \langle g_1, \ldots, g_t \rangle$ y tenemos que $I = \langle g_1, \ldots, g_t \rangle$.

□

Definamos ya lo que son las bases de Groebner:

Definición 1.11. *Fijado un orden monomial en $K[x_1, \ldots, x_n]$, un conjunto finito $G = \{g_1, , \ldots, g_t\}$ de polinomios de un ideal I se dice* ***base de Groebner*** *ó base estándar si*

$$\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle.$$

Notar que por la demostración del *Teorema de la base de Hilbert* si $G = \{g_1, \ldots, g_t\}$ es una base de Groebner de I se tiene que

$$I = \langle g_1, \ldots, g_t \rangle.$$

Además, tales bases siempre existen.

Ejemplo 1.11.1. *Sea $\mathbb{R}[x, y, z]$ con el orden lex y un ideal $I = \langle x+z, y-z \rangle$. Veamos que $\{x + z, y - z\}$ sí es una base de Groebner de I.*

Tenemos que probar que $\langle LT(I) \rangle = \langle LT(x+z), LT(y-z) \rangle = \langle x, y \rangle$, es decir, que el término director de cualquier polinomio de I es múltiplo de x ó de y. Supongamos que existe $f = A(x+z)+B(y-z)$ no nulo cuyo término director no es divisible por x ni por y. Por definición del orden lex, f será un polinomio en z. Pero ahora,

$$Cz = A(x + z) + B(y - z) = Ax + Az + By - Bz = Ax + By + (A - B)z,$$

lo cual es absurdo porque el único polinomio que lo cumple es el nulo.

■

Notar que en el ejemplo de $I = \langle x^3 - 2xy, x^2y - 2y^2 + x \rangle$ el conjunto $\{x^3 - 2xy, x^2y - 2y^2 + x\}$ no es base de Groebner ya que $x^2 \in \langle LT(I) \rangle$ pero $x^2 \notin \langle LT(x^3 - 2xy), LT(x^2y - 2y^2 + x) \rangle$.

Corolario 1.11.1 (***La condición de cadena ascendente***)**.** *Toda cadena ascendente de ideales de $K[x_1, \ldots, x_n]$ se estaciona. Si tenemos $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ ideales de $K[x_1, \ldots, x_n]$, entonces existe un $n \in \mathbb{N}$ tal que $I_n = I_k$ para todo $k \geq n$.*

Demostración: Es fácil ver que $\cup_n I_n = I$ es un ideal. Por el *Teorema de la base de Hilbert* existen $f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$ tales que $I = \langle f_1, \ldots, f_s \rangle$ y por definición de I se tiene que existe algún $n \in \mathbb{N}$ tal que $\{f_1, \ldots, f_s\} \subseteq I_n$. Para cada $k > n$ se tiene que $I = \langle f_1, \ldots, f_s \rangle \subseteq I_k \subseteq I$, luego $I = I_k$.

□

Notar que, en un anillo, decir que una cadena de ideales ascendente estacione es equivalente a decir que todo ideal es finitamente generado.

Corolario 1.11.2. *Para un ideal I de $K[x_1, \ldots, x_n]$, denotamos la variedad que lo define así:*

$$V(I) = \{(a_1, \ldots, a_n) \in \mathbb{K}^n : f(a_1, \ldots, a_n) = 0 \, \forall f \in I\}.$$

Notar que si K no es finito, I tiene una cantidad infinita de elementos.

Existe un conjunto finito $\{g_1, \ldots, g_t\} \subseteq I$ tal que $V(I) = V(g_1, \ldots, g_s)$.

Demostración: Por el *Teorema de la base de Hilbert* se tiene que existe un conjunto finito $\{g_1, \ldots, g_t\} \subseteq I$ tal que $I = \langle g_1, \ldots, g_t \rangle$ y claramente tenemos que $V(I) = V(g_1, \ldots, g_t)$.

□

1.4. Propiedades de las bases de Groebner

Proposición 1.12. *Sea $G = \{g_1, \ldots, g_t\}$ una base de Groebner para el ideal I de $K[x_1, \ldots, x_n]$. Para $f \in K[x_1, \ldots, x_n]$ existe unos únicos $g, r \in K[x_1, \ldots, x_n]$ verificando:*

1. *$g \in I$ y $f = g + r$.*
2. *Ningún término de r es múltiplo de ninguno de los $LT(g_1), \ldots, LT(g_t)$. En particular si aplicamos el algoritmo de la división de f por los polinomios de G, el resto que se obtiene no depende del orden en el que pongamos a los elementos de G. Además, $f \in I$ si y sólo si el resto de la división por $g_1, \ldots, g_t$ es cero.*

Demostración: La existencia se deduce del algoritmo de la división. Supongamos que r y r' satisfacen las condiciones 1 y 2, $g = f - r \in I$ y también $g' = f - r' \in I$, luego $r - r' \in I$. Por la segunda condición que cumplen r y r' se tiene que si $r - r'$ no es nulo, $LT(r - r')$ no es múltiplo de ningún $LT(g_1), \ldots, LT(g_t)$.

Por ser $G = \{g_1, \ldots, g_t\}$ una base de Groebner para el ideal I se tiene que $LT(I) = \langle LT(g_1), \ldots, LT(g_t)\rangle$. Como $r - r' \in I$, $LT(r - r')$ debería ser múltiplo de alguno de los $LT(g_1), \ldots, LT(g_t)$, de donde se deduce que $r - r' = 0$ y $r = r'$.

□

A este resto de f se llama a veces forma normal de f. La propiedad de que $f \in I$ si y sólo si el resto de la división por $g_1, \ldots, g_t$ es cero caracteriza el hecho de que una base $g_1, \ldots, g_t$ de I sea base de Groebner. También caracteriza la condición de ser base de Groebner el hecho de que el resto sea siempre único.

Veamos ahora cómo saber si una familia generadora es una base de Groebner. Buscaremos polinomios de I que puedan tener un término director que no esté en el ideal generado por los directores de la base.

Definición 1.13. *Sean f y g polinomios no nulos en $K[x_1, \ldots, x_n]$, $LM(f) = x^\alpha$, $LM(g) = x^\beta$. El mínimo común múltiplo de x^α y x^β es x^γ, con $\gamma_i = max(\alpha_i, \beta_i)$ (mínimo común múltiplo de x^α y x^β). El* ***S-polinomio*** *de f y g será*

$$S(f, g) = \frac{x^\gamma}{LT(f)} f - \frac{x^\gamma}{LT(g)} g.$$

Proposición 1.14. *Sea un polinomio f que es suma de polinomios con el mismo multigrado δ, $f = \sum_i f_i$ y verificando que $ultideg(f) < \delta$. Entonces f es una combinación lineal con coeficientes en K de los polinomios $S(f_i, f_j)$. Además, estos polinomios verifican que $multideg(S(f_i, f_j)) < \delta$.*

Demostración: Por ser los monomios directores de f_i y f_j iguales a x^δ, se tiene que

$$S(f_i, f_j) = \frac{1}{LC(f_i)} f_i - \frac{1}{LC(f_i)} f_j$$

es un polinomio con multigrado menor que δ. Llamaremos $p_i = \dfrac{1}{LC(f_i)} f_i$, que son polinomios con término director x^δ. Se tiene que

$$S(f_i, f_j) = S(p_i, p_j) = p_i - p_j.$$

Por ser $multideg(f) < \delta$, se tiene que $\sum_i LC(f_i) = 0$.

Sean $c_i = LC(f_i) \in K$. Se tiene $f = \sum_i f_i = \sum_i c_i p_i = c_1(p_1 - p_2) + (c_1 + c_2)(p_2 - p_3) + (c_1 + c_2 + c_3)(p_3 - p_4) + \ldots + (c_1 + \ldots + c_{s-1})(p_{s-1} - p_s) + (c_1 + \ldots + c_{s-1} + c_s)p_s$ y así f es combinación lineal con coeficientes en K de los polinomios $S(f_i, f_j)$.

□

Teorema 1.15 (***El criterio de Buchberger***)**.** *Sea I un ideal de polinomios y $G = \{g_1, \ldots, g_t\}$ una familia generadora (base) de I. Se tiene que $G = \{g_1, \ldots, g_t\}$ es una base de Groebner de I si y sólo si para todo par $i \neq j$ se tiene que el resto de la división de $S(g_i, g_j)$ por G es cero (Considerando los elementos de G en algún orden).*

Demostración: Si G es una base de Groebner, como $S(g_i, g_j) \in I$, se tiene, por la caracterización dada en la proposición anterior que el resto de la división por G es cero.

Recíprocamente para probar que G es base de Groebner, tenemos que ver que para todo $f \in I$ se tiene que

$$LT(f) \in \langle LT(g_1), \ldots, LT(g_t) \rangle.$$

Sean $h_i \in K[x_1, \ldots, x_n]$ tales que $f = \sum h_i g_i$. Los h_i no son únicos pero en todos los casos considerando los monomios de cada lado de la igualdad según el orden establecido, se tiene

$$LM(f) \leq max\{LM(h_i g_i)\} = x^\gamma.$$

Notemos que si se tiene la igualdad $LT(f)$ es múltiplo de $LT(g_i)$ para algún i. El monomio x^γ depende de los h_i elegidos y si consideramos todos los posibles, tenemos un conjunto de monomios que por las propiedades del orden monomial tiene un mínimo. Elegimos ese mínimo x^γ.

Ahora consideramos $f = \sum h_i g_i$ de modo que $x^\gamma = max\{LM(h_i g_i)\}$ y vamos a ver que $LM(f) = max\{LM(h_i g_i)\} = x^\gamma$.

Supongamos que $LM(f) < max\{LM(h_i g_i)\} = x^\gamma$ y llegaremos a contradicción construyendo otra suma $f = \sum h_i g_i$ con $x^\gamma > max\{LM(h_i g_i)\}$.

Cnsideramos

$$f = \sum_{LM(h_i g_i) = x^\gamma} h_i g_i + \sum_{LM(h_i g_i) < x^\gamma} h_i g_i.$$

Ahora separamos en los h_i el término director de los siguientes

$$f = \sum_{LM(h_i g_i) = x^\gamma} LT(h_i) g_i + \sum_{LM(h_i g_i) = x^\gamma} (h_i - LT(h_i)) g_i + \sum_{LM(h_i g_i) < x^\gamma} h_i g_i.$$

Los dos sumandos últimos tienen monomio director menor que x^γ y como el monomio director de f es menor que x^γ, forzosamente también el primer sumando tiene monomio director menor que x^γ.

Ahora llamamos f_i a los polinomios $LT(h_i)g_i$ tales que $LM(h_ig_i) = x^\gamma$, que tenemos que tiene todos monomio director x^γ y además ese primer sumando es $\sum_i f_i$. Por el resultado anterior, este polinomio es una combinación lineal con coeficientes en K de los polinomios

$$S(f_i, f_j) = S(LT(h_i)g_i, LT(h_j)g_j)$$

Y por el resultado anterior nuevamente se tiene que el monomio director de $S(f_i, f_j)$ es menor que x^γ. Pero como $LT(h_i)g_i, LT(h_j)g_j$ tienen el mismo monomio director x^γ, se tiene que

$$S(f_i, f_j) = \frac{1}{LC(f_i)}f_i - \frac{1}{LC(f_j)}f_j = \frac{1}{LC(h_i)LC(g_i)}LT(h_i)g_i - \frac{1}{LC(h_j)LC(g_j)}LT(h_j)g_j.$$

Introducimos $LM(g_i)$ y por ser $LT(h) = LC(h)LM(h)$, se tiene

$$S(f_i, f_j) = \frac{LM(g_i)}{LT(g_i)}LM(h_i)g_i - \frac{LM(g_j)}{LT(g_j)}LM(h_j)g_j = \frac{x^\gamma}{LT(g_i)}g_i - \frac{x^\gamma}{LT(g_j)}g_j.$$

Llamamos x^α al mínimo común múltiplo de $LM(g_i)$ y $LM(g_j)$. Como se tiene que $LM(h_i)LM(g_i) = x^\gamma$ y $LM(h_j)LM(g_j) = x^\gamma$, x^γ es múltiplo de los dos, luego es múltiplo de x^α. Llamamos $x^{\alpha_{ij}} = x^\gamma/x^\alpha$ y se tiene que

$$S(f_i, f_j) = x^{\alpha_{ij}}S(g_i, g_j).$$

Ahora aplicamos la hipótesis de que para cada j, k existen $a_{ijk} \in K[x_1, \ldots, x_n]$ tales que

$$S(g_j, g_k) = \sum_i a_{ijk}g_i,$$

además con el multrigrado de $S(g_j, g_k)$ mayor o igual que el multigrado de $a_{ijk}g_i$ para todo i.

Multiplicando por $x^{\alpha_{jk}}$ se tiene

$$S(f_i, f_k) = x^{\alpha_{jk}}\sum_i a_{ijk}g_i = \sum_i x^{\alpha_{jk}}a_{ijk}g_i,$$

verificándose que el multigrado de $x^{\alpha_{jk}}a_{ijk}g_i$ es menor o igual que el multigrado de $x^{\alpha_{jk}}S(g_j, g_k) = S(f_i, f_j)$ que es menor que γ.

Volvemos a considerar la igualdad

$$f = \sum_{LM(h_ig_i)=x^\gamma} LT(h_i)g_i + \sum_{LM(h_ig_i)=x^\gamma} (h_i - LT(h_i))g_i + \sum_{LM(h_ig_i)<x^\gamma} h_ig_i$$

y hemos visto que para el primer sumando existe $c_{jk} \in K$ tales que

$$\sum_i f_i = \sum_{j,k} c_{jk} S(f_j, f_k)$$

y luego

$$\sum_i f_i = \sum_{j,k} c_{jk} S(f_j, f_k) = \sum_{j,k} c_{jk} (\sum_i x^{\alpha_{jk}} a_{ijk} g_i) = \sum_i \bar{h}_i g_i.$$

Recordemos que el multigrado de $a_{ijk} g_i$ es menor o igual que el multigrado de $S(g_j, g_k)$ y por tanto

$$LM(x^{\alpha_{jk}} a_{ijk} g_i) \leq LM(x^{\alpha_{jk}} S(g_j, g_k)) < x^\gamma.$$

Como $\bar{h}_i g_i$ es una suma de polinomios con monomios directores menores que x^γ, tenemos que $LM(\bar{h}_i g_i) < x^\gamma$ y tenemos la contradicción que buscábamos.

□

1.5. El algoritmo de Buchberger

Teorema 1.16. *Consideramos el ideal de polinomios $I = \langle f_1, \ldots, f_s \rangle$. El siguiente procedimiento nos proporciona una base de Groebner de I en un número finito de pasos: para cada pareja i, j se considera el resto que se obtiene al dividir $S(f_i, f_j)$ por la familia $f_1, \ldots, f_s$ (en el orden dado). Añadimos a la familia todos los restos no nulos y procedemos del mismo modo con la nueva familia. Llega un momento que los restos son todos cero y la familia obtenida es una base de Groebner de I que contiene a la base inicial.*

Demostración: Todos los polinomios que se añaden están en I puesto que si partimos de dos polinomios $f, g \in I$, se tiene que $S(f, g)$ está en I y por tanto el resto de dividir por polinomios de I sigue estando en I. Como todas las familias obtenidas contienen a la base inicial, todas son base.

En cada paso, si llamamos G a la base que tenemos, analicemos el ideal $< LT(f) : f \in G \rangle$. El resto de dividir un polinomio por G cumple la condición de que sus términos no son múltiplos de ninguno de los $LT(f)$, con $f \in G$, luego al añadir esos restos obtenemos una nueva familia G' tal que

$$\langle LT(f) : f \in G \rangle < \langle LT(f) : f \in G' \rangle$$

y por la condición de cadena ascendente esta cadena se estaciona, lo que implica que los restos son todos cero y lo que se obtiene es así una base de Groebner.

□

Tener en cuenta que este algoritmo que acabamos de describir se puede refinar muchísimo y la base de Groebner que se obtiene es demasiado grande.

Definición 1.17. *Una **base minimal de Groebner** para un ideal I es una base de Groebner G del ideal I que verifica:*

1. *$LC(p) = 1$ para todo $p \in G$.*

2. *Para todo $p \in G$ $LT(p) \notin \langle LT(G - p)\rangle$.*

Es evidente que a partir de una base de Groebner podemos construir una minimal, ya que G es base de Groebner cuando $\langle LT(G)\rangle = \langle LT(I)\rangle$, y si $LT(p) \in \langle LT(G-p)\rangle$ se tiene que $\langle LT(G - p)\rangle = \langle LT(G)\rangle$, luego $G - p$ también es base de Groebner.

También está claro que dos bases de Groebner minimales tienen los mismos términos directores.

Definición 1.18. *Una **base de Groebner reducida** para un ideal I es una base de Groebner G del ideal I que verifica:*

1. *$LC(p) = 1$ para todo $p \in G$.*

2. *Para todo $p \in G$ ningún monomio de p está en $\langle LT(G - p)\rangle$.*

De la definición es claro que toda base de Groebner reducida es minimal.

Proposición 1.19. *Todo ideal de polinomios no nulo tiene una única base de Groebner reducida.*

Demostración: Partimos de una base de Groebner G minimal. Para $g \in G$ consideramos g' el resto de dividir g por $G \setminus \{g\}$. Por ser G minimal el monomio director de g es el mismo que el de g'. Además, la famiilia que resulta de sustituir en G el polinomio g por g' genera el mismo ideal y como los monomios directores de sus elementos son los mismos, se tiene que es la base de Groebner minimal. Si cambiamos cada g por su correspondiente resto de dividir por los demás obtenemos una base de Groebner reducida.

Veamos ahora que es única. Sean G y G' dos bases de Groebner reducidas, por ser bases de Groebner minimalles tienen los mismos monomios directores. Para cada $g \in G$ elegimos unn $g' \in G'$ tal que $LT(g) = LT(g')$. Tenemos que los términos de $g - g'$ son de g ó de g' distintos de $LT(g) = LT(g')$, que se ha anulado. Así, $g - g'$ no tiene monomios divisibles por ninguno de los $LT(G) = LT(G')$. Así, el resto de dividir $g - g'$ por los elementos de G es el propio $g - g'$, y por ser G una base de Groebner del ideal y estar $g - g'$ en el ideal, este resto es 0, luego $g = g'$.

□

Ejemplo 1.19.1. *En $K[x, y]$ con el orden grlex, consideramos $I = \langle x^3 - 2xy, x^2y - 2y^2 + x\rangle$. Encontremos una base de Groebner reducida.*

Llamamos $f_1 = x^3 - 2xy$ y $f_2 = x^2y - 2y^2 + x$. Está claro que $LM(f_1) = x^3$ y $LM(f_2) = x^2y$, con $m.c.m(x^3, x^2y) = x^3y$. Entonces

$$S(f_1, f_2) = y(x^3 - 2xy) - x(x^2y - 2y^2 + x) = -x^2,$$

y como no es divisible por ninguno de los términos líderes de f_i se tiene que es el resto de dividir por los f_i.

Cogemos $f_3 = -x^2$, y:

$$S(f_1, f_3) = -x^3 + 2xy + x(x^2) = 2xy,$$

y como no es divisible por ninguno de los términos líderes de f_i, se tiene que es el resto de dividir por los f_i. Llamamos ahora a $f_4 = 2xy$. Ahora:

$$S(f_2, f_3) = -(x^2y - 2y^2 + x) - y(-x^2) = 2y^2 - x,$$

y como no es divisible por ninguno de los términos líderes de f_i, se tiene que es el resto de dividir por los f_i. Llamamos así $f_5 = 2y^2 - x$. Así, $f_1 = x^3 - 2xy, f_2 = x^2y - 2y^2 + x, f_3 = -x^2, f_4 = 2xy, f_5 = 2y^2 - x$. Y es fácil ver que los restos de dividir por estos f_i todos los $S(f_i, f_j)$ dan cero y así es base de Groebner.

El ideal de los monomios líderes es $LT(I) = \langle x^3, x^2y, x^2, xy, y^2\rangle = \langle x^2, xy, y^2\rangle$. Luego $\{x^2, xy, y^2\}$ es una base minimal y reducida.

■

Ejemplo 1.19.2. *Sea $K[x, y, z]$ con el orden grlex y consideramos el ideal $I = \langle x + 2y + z - 3, x + 3y - 2z + 1\rangle$. Encontremos una base de Groebner: Sea $f_1 = x + 2y + z - 3$, $f_2 = x + 3y - 2z + 1$. $LM(f_1) = x$, $LM(f_2) = x$. $\langle LT(I)\rangle = \langle LT(x + 2y + z - 3), LT(x + 3y - 2z + 1)\rangle = \langle x\rangle$. Supongamos ahora que existe un $f = A(x + 2y + z - 3) + B(x + 3y - 2z + 1) \in I$ no nulo cuyo término director no es múltiplo de x, es decir, un polinomio en z, y:*

$Cy + Dz + E = A(x + 2y + z - 3) + B(x + 3y - 2z + 1) = Ax + 2Ay + Az - 3A + Bx + 3By - 2Bz + B = (A + B)x + (2A + 3B)y + (A - 2B)z - 3A + B$. *Luego:*

$$\left.\begin{array}{rcl} A + B &=& 0 \\ 2A + 3B &=& C \\ A - 2B &=& D \\ -3A + B &=& E \end{array}\right\}$$

De donde sacamos que $A = -B$, $C = B$, $D = -3B$, $E = 4B$.

Como esta condición se puede cumplir tenemos que $\{f_1, f_2\}$ no es una base de Groebner. Calculemos el S-polinomio:

$$S(f_1, f_2) = f_1 - f_2 = -y + 3z - 4,$$

y llamamos a $f_3 = -y+3z-4$. Añadimos f_3 y consideramos $\langle LT(f_1), LT(f_2), LT(f_3)\rangle = \langle x, y\rangle$. Veamos si $\langle x, y\rangle = \langle LT(I)\rangle$. Supongamos un $f = A(x + 2y + z - 3) + B(x + 3y - 2z + 1) \in I$ no nulo cuyo término director no sea múltiplo de x ni de y, es decir, que es un polinomio en z:

$$Cz + E = A(x + 2y + z - 3) + B(x + 3y - 2z + 1),$$

y ahora

$$\left.\begin{array}{rcl} A + B &=& 0 \\ 2A + 3B &=& 0 \\ A - 2B &=& C \\ -3A + B &=& E \end{array}\right\}$$ *de donde sacamos que $A = B = 0$ y así f sería nulo, lo que es absurdo.*

Luego $\langle x, y\rangle = \langle LT(I)\rangle$ y así $\{f_1, f_2, f_3\}$ sería una base de Groebner.

■

1.6. Intersección de ideales

Definición 1.20. *Sean I, J dos ideales de $K[x_1, \ldots, x_n]$. Tenemos entonces los siguientes ideales de $K[x_1, \ldots, x_n]$:*

$$I + J = \{f + g : f \in I, g \in J\},$$
$$IJ = \{f_1 g_1 + \ldots + f_r g_r : f_i \in I, g_i \in J, r \in \mathbb{N}\},$$
$$I \cap J = \{f : f \in I, f \in J\}.$$

Es bastante sencillo probar que son ideales y que, si $I = \langle f_1, \ldots, f_r \rangle$ y $J = \langle g_1, \ldots, g_t \rangle$ se tiene que

$$I + J = \langle f_1, \ldots, f_r, g_1, \ldots, g_t \rangle$$
$$IJ = \langle f_i g_i : i = 1, \ldots, r, j = 1, \ldots, t \rangle.$$

Ahora, para buscar una base de $I \cap J$ tendremos que:

Proposición 1.21. *Para un ideal I de $K[x_1, \ldots, x_n]$ y un polinomio en una variable distinta t, $f(t) \in K[t]$ denotamos fI el ideal que, siendo $K[x_1, \ldots, x_n, t]$ generado por $\{f(t)h(x) : h \in I\}$ (no es un producto de ideales), si $I = \langle f_1(x), \ldots, f_r(x) \rangle$ se tiene:*

1. *$f(t)I = \langle f(t)f_1(x), \ldots, f(t)f_r(x) \rangle$.*
2. *Si $g(x,t) \in f(t)I$, $a \in K$ entonces $g(x,a) \in I$.*

Demostración: Sencillo ejercicio. □

Proposición 1.22. *Sea I un ideal de $K[x_1, \ldots, x_{l-1}, x_l, \ldots, x_n]$. Tenemos que $I \cap K[x_1, \ldots, x_n]$ es un ideal de $K[x_1, \ldots, x_n]$. Si consideramos el orden lex con $x_1 > \ldots > x_{l-1} > x_l > \ldots > x_n$ y G es una base de Groebner de I, entonces $G \cap K[x_l, \ldots, x_n]$ es una base de Groebner de $I \cap K[x_l, \ldots, x_n]$.*

Teorema 1.23. *Sean I, J dos ideales de $K[x_1, \ldots, x_n]$. Consideramos $K[t, x_1, \ldots, x_n]$. Entonces*

$$I \cap J = (tI + (1-t)J) \cap K[x_1, \ldots, x_n].$$

Demostración: Fácil usando $t = 0$ y $t = 1$. □

Así, tenemos un procedimiento para buscar una base de Groebner de la intersección de dos ideales a partir de las bases de los dos.

Sean $I = \langle f_1, \ldots, f_r \rangle, J = \langle g_1, \ldots, g_s \rangle$ ideales de $K[x_1, \ldots, x_n]$. Consideramos el ideal

$$\langle tf_1, \ldots, tf_r, (1-t)g_1, \ldots, (1-t)g_s \rangle.$$

Buscamos una base de Groebner de este ideal y los polinomios de esa base que no contengan la variable t forman una base de Groebner de $I \cap J$.

2. Cuerpos finitos

Teorema 2.1 (***Teorema de Wedderburn***)**.** *Todo cuerpo finito es conmutativo.*

Definición 2.2 (***Característica de un cuerpo***)**.** *La* ***característica*** *de un cuerpo K se define como el mínimo p de los enteros positivos n tales que $n{\cdot}1 = 1{+}\ldots{+}1 = 0$, donde 0 es el elemento neutro de la suma y 1 es el elemento neutro del producto en el cuerpo K. Si tal p no existe, como ocurre con el cuerpo de los números reales, decimos que K tiene característica 0.*

Notar que la característica p de un cuerpo ha de ser un número primo (siempre que no sea característica 0). Esto es así porque si $p = rs$, con $1 < r, s < p$ entonces $0 = p \cdot 1 = (r \cdot 1)(s \cdot 1)$ y uno de los dos factores debería ser 0 (ya que un cuerpo es siempre un dominio de integridad y no tiene divisores de cero), pero esto contradice la minimalidad de p. En este caso diremos que el cuerpo tiene característica prima p.

Para criptografía y teoría de códigos nos serán de especial interés los cuerpos de característica 2.

2.1. Polinomios irreducibles y cuerpos

Recordemos que si K es un cuerpo entonces el anillo de polinommios $K[x]$ es un dominio euclídeo con el grado de un polinomio $p \in K[x]$, denotado por $\delta(p)$. Por ser dominio euclídeo es también dominio de ideales principales , luego para todo ideal I existe $p \in K[x]$ tal que

$$I = (p) = \{pq : q \in K[x]\}.$$

También es un dominio de factorización única. El teorema del resto y la factorización única impiden que un polinomio en un cuerpo tenga más raíces que su grado.

Proposición 2.3. *Un polinomio $p \in K[x]$ es irreducible si y sólo si $K[x]/(p)$ es un cuerpo.*

Demostración: Supongamos que $K[x]/(p)$ es un cuerpo. Si $p = fg$ con $f, g \in K[x]$ y $\delta(f), \delta(g) < \delta(p)$ tendríamos $(f + (p))(g + (p)) = (p)$, es decir, que $f + (p), g + (p)$ serían divisores de cero en $K[x]/(p)$, luego no tendrían inverso y por tanto $K[x]/(p)$ no sería cuerpo. Luego si $p = fg$, con $f, g \in K[x]$, uno de los dos polinomios es constante y por lo tanto p es irreducible.

Supongamos ahora que p es irreducible y sea $f + (p) \neq (p)$. Se tiene que el máximo común divisor de f y p es 1, luego por la identidad de Bézout existirán $a, b \in K[x]$ tales que $af + bp = 1$. Así, $(a + (p))(f + (p)) = 1 + (p)$ y por lo tanto todo $f + (p)$ no nulo es unidad y así $K[x]/(p)$ es cuerpo.

□

En un dominio euclídeo el máximo común divisor de dos elementos es el mayor de los divisores comunes (mayor absoluto en los enteros o mayor grado en los anillos

de polinomios en un cuerpo) y es único salvo asociados (es decir, productos por unidades). Si $d = mcd(a, b)$ tenemos que $(d) = (a) + (b)$.

La forma más práctica de caclular el máximo común divisor es mediante el *algoritmo de Euclides*, que se basa en lo siguiente:

Dados D y d, por el algoritmo de la división existen c, r tales que $D = cd + r$, es claro que

$$\{\text{divisores de } D \text{ y } d\} = \{\text{divisores de } d \text{ y } r\}.$$

Veamos el algoritmo con un ejemplo en $\mathbb{Z}$, calculando el máximo común divisor de 192 y 162.

En la fila Q ponemos los cocientes enteros de dos de los números de la fila R. Esta fila se forma con los correspondientes restos. El máximo común divisor es el último resto no nulo, en este caso 6:

Q		1	5	2	2	2
R	192	162	30	12	6	0

Ahora, recordemos que la identidad de Bézout nos dice que, si el $mcd(a, b) = d$ (a y b dados), entonces existen u y v tales que $au + bv = d$.

Entonces, demostraremos por inducción sobre i que para todos los restos r_i que van saliendo al aplicar el algoritmo de Euclides existen u_i, v_i tales que $au_i + bv_i = r_i$.

Construyamos el cuadro del algoritmo de la división ampliado con dos filas nuevas. En el cuadro pondremos $R_1 = a$, $R_2 = b$, $u_1 = 1$, $v_1 = 0$, $u_2 = 0$, $v_2 = 1$ y se tiene

$$R_1 = au_1 + bv_1, \quad R_2 = au_2 + bv_2.$$

Recordar cómo se construyen las dos filas del algoritmo de Euclides y describimos ahora la construcción de las otras dos filas: q_i es el cociente entero de dividir r_{i-1} por r_i. El resto de esta división es r_{i+1}. Así: $r_i = r_{i-2} - r_{i-1}q_{i-1}$, $u_i = u_{i-2} - u_{i-1}q_{i-1}$, $v_i = v_{i-2} - v_{i-1}q_{i-1}$.

Así pues:

Q		q_2	$q_3 \ldots$
R	$r_1 = a$	$r_2 = b$	$r_3 \ldots$
U	$u_1 = 1$	$u_2 = 0$	$u_3 \ldots$
V	$v_1 = 0$	$v_2 = 1$	$v_3 \ldots$

Demostraremos por inducción sobre i que $au_i + bv_i = r_i$. Claramente es cierto para $i = 1, 2$. Aplicando la hipótesis de inducción se tiene que

$$r_i = r_{i-2} - r_{i-1}q_{i-1} = au_{i-2} + bv_{i-2} - (au_{i-1} + bv_{i-1})q_{i-1} = a(u_{i-2} - u_{i-1}q_{i-1}) + b(v_{i-2} - v_{i-1}q_{i-1}) = au_i + bv_i.$$

Proposición 2.4 (***Existencia raíz***)**.** *Supongamos que $p \in K[x]$ es irreducible, entonces existe un cuerpo E que contiene a K como subcuerpo tal que p tiene una raíz en E.*

Demostración: Supongamos que $p(x) = a_n x^n + \ldots + a_1 x + + a_0$. Por la proposición anterior sabemos que $E = K[x]/(p)$ es un cuerpo. Consideramos el homomorfismo de anillos

$$\begin{array}{ccc} K[x] & \longrightarrow & E \\ f & \longmapsto & f + (p) = \bar{f} \end{array}$$

Notemos que si $a \in K$ no nulo, entonces $\bar{a} \neq \bar{0}$, por lo que K es isomorfo a $\bar{K} = \{\bar{a} : a \in K\} \subseteq E$. Identificamos K con $\bar{K}$. Con esta identificación tenemos que el polinomio p se transforma en $p_0(x) = \bar{a}_n x^n + \ldots \bar{a}_1 x + \bar{a}_0 \in \bar{K}[x]$. Consideramos el elemento $e = x + (p) = \bar{x} \in E$. Se tiene $p_0(e) = (\bar{a}_n x^n + \ldots + \bar{a}_1 x + \bar{a}_0) + (p) = \bar{p} = \bar{0}$ y así la proposición queda demostrada.

□

Notar que este cuerpo E es $K[x]/(p)$, es decir, si $p \in K[x]$ es irreducible entonces p tiene una raíz en $K[x]/(p)$.

Definición 2.5. *El **cuerpo primo** de un cuerpo K es la intersección de todos los subcuerpos de K.*

Proposición 2.6. *Sea F el cuerpo primo de K. Si la característica de K es cero, entonces F es isomorfo a $\mathbb{Q}$ y si la característica de K es p, entonces F es isomorfo a $\mathbb{Z}_p$.*

Demostración: Si $n \in \mathbb{N}$, definimos $n = 1 + \ldots + 1$. Sea F el cuerpo primo de K. Si *char* $K = 0$

$$F = \{nm^{-1} : n, m \in \mathbb{N} \setminus \{0\}\} \cup \{0\}.$$

F tiene que contener todos estos elementos por ser subcuerpo. El conjunto es cerrado para el producto y el inverso de nm^{-1} es $n^{-1}m$. Es cerrado para la suma: $nm^{-1} + n'm'^{-1} = (nm' + n'm)(mm')^{-1}$. Luego F es el cuerpo primo de K. Definimos

$$\begin{array}{rccc} f: & F & \longrightarrow & \mathbb{Q} \\ & nm^{-1} & \longmapsto & n/m, \end{array}$$

está bien definida y es un isomorfismo de cuerpos. Si *char* $K = p$, veamos que $F = \{i : 1 \leq i \leq p-1\} \cup \{0\}$ $(*)$.

Es claramente cerrado para la suma y para el producto (porque $i = i + kp$, $k \in \mathbb{N}$). Si $1 \leq i \leq p-1$, entonces $(i, p) = 1$. Por Bézout $1 = ai + bp$. Entonces a es el inverso de i. Así, se prueba $(*)$. Definimos

$$\begin{array}{rccc} f: & F & \longrightarrow & \mathbb{Z}_p \\ & i & \longmapsto & i + p\mathbb{Z} = \bar{i}, \end{array}$$

y f es isomorfismo de cuerpos.

□

Ejercicio 1. *Sean a, b elementos de un anillo R tales que $ab = ba$. Si n es un entero positivo, entonces*

$$(a+b)^n = \sum_{j=0}^{n} \binom{n}{j} a^j b^{n-j}.$$

Recordemos que $\binom{n}{j} = \dfrac{n!}{(n-j)!j!}$. *Lo haremos por inducción sobre* n, *veamos que para* $n = 1$ *se cumple que*

$$(a+b) = \sum_{j=0}^{1} \binom{1}{j} a^j b^{n-j} = \binom{1}{0} b + \binom{1}{1} a = a + b.$$

Ahora supongamos que es cierto para todo n *y veamos que tambiñen lo es para* $n+1$*: por un lado tenemos que*

$$(a+b)^{n+1} = \sum_{j=0}^{n+1} \binom{n+1}{j} a^j b^{n+1-j} = \sum_{j=0}^{n+1} \left[\binom{n}{j-1} + \binom{n}{j} \right] a^j b^{n+1-j}.$$

Y por otro lado:

$$(a+b)^{n+1} = (a+b)^n(a+b) = \left(\sum_{j=0}^{n} \binom{n}{j} a^j b^{n-j}\right)(a+b) = \sum_{j=0}^{n} \binom{n}{j} a^{j+1} b^{n-j} + \sum_{j=0}^{n} \binom{n}{j} a^j b^{n+1-j} = \sum_{j=1}^{n+1} \binom{n}{j-1} a^j b^{n+1-j} + \binom{n}{0} b^{n+1} + \sum_{j=1}^{n} \binom{n}{j} a^j b^{n+1-j} = \sum_{j=1}^{n} = \sum_{j=1}^{n} \binom{n}{j-1} a^j b^{n+1-j} + \binom{n}{n} a^{n+1} + \binom{n}{0} b^{n+1} + \sum_{j=1}^{n} \binom{n}{j} a^j b^{n+1-j} = \sum_{j=1}^{n} \left[\binom{n}{j-1} + \binom{n}{j} \right] a^j b^{n+1-j} + \binom{n+1}{n+1} a^{n+1} + \binom{n+1}{0} b^{n+1} = \sum_{j=1}^{n} \binom{n+1}{j} a^j b^{n+1-j} + \binom{n+1}{n+1} a^{n+1} + \binom{n+1}{0} b^{n+1} = \sum_{j=0}^{n+1} \binom{n+1}{j} a^j b^{n+1-j} = (a+b)^{n+1}.$$

■

Ejercicio 2. *En un cuerpo de característica* p *tenemos que*

$$(a+b)^p = a^p + b^p.$$

Por el ejercicio anterior sabemos que

$$(a+b)^p = \sum_{j=0}^{p} \binom{p}{j} a^j b^{p-j} = \binom{p}{0} b^p + \binom{p}{1} a b^{p-1} + \ldots + \binom{p}{p} a^p.$$

Ahora, tenemos que como $\binom{p}{i} = \dfrac{p!}{(p-i)!i!} = \dfrac{p \cdot (p-1) \cdots (p-(i+1))}{i!}$ *para todo* $i = 1, \ldots, p-1$ *(en* $i = 1, p-1$ *tendremos que* $\binom{p}{i} = p$*) y ésto es divisible por* p *entonces, al estar en un cuerpo de característica* p *y ser múltiplo de* p*, serán todos nulos. Quedan así sólo* $\binom{p}{0} b^p = b^p$, $\binom{p}{p} a^p = a^p$, *luego* $(a+b)^p = a^p + b^p$.

■

Proposición 2.7. *Sea* $K = \mathbb{Z}_p$, *con* p *primo y* $p(x) \in K[x]$ *un polinomio irreducible en* $K[x]$ *de grado* $n \geq 1$. *Entonces el cuerpo* $K[x]/(p)$ *tiene exactamente* p^n *elementos.*

Demostración: Como $p(x)$ es irreducible tenemos que $K[x]/(p)$ es un cuerpo y todo elemento de $K[x]/(p)$ será de la forma $g(x) + (p)$. Ahora, por el algoritmo de la división existen $q(x), r(x) \in K[x]$ tales que $g(x) = p(x)q(x) + r(x)$, con $r = 0$ ó $\delta(r) <$

$\delta(p) = n$ y asi $g(x)+(p) = p(x)q(x)+r(x)+(p) = r(x)+(p) = a_{n-1}x^{n-1}+\ldots+a_1x+a_0$. Como $a_{n-1}, \ldots, a_1, a_0 \in \mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ habrá p^n combinaciones y por lo tanto p^n elementos distintos.

□

2.2. Raíces y polinomios irreducibles

Proposición 2.8. *Sea K un subcuerpo de E y $f \in K[x]$ con $f' \neq 0$, donde f' es la derivada del polinomio f. Se tiene que*

1. *Si $a \in E$, a es raíz múltiple de f si y sólo si $f(a) = f'(a) = 0$.*
2. *Si $(f, f') = 1$, entonces f no tiene raíces múltiples en E.*
3. *Si f es irreducible en $K[x]$, entonces todas las raíces de f son distintas.*
4. *Si la característica de K es cero, los irreducibles de $K[x]$ no tienen raíces múltiples en ningún cuerpo extensión de K.*
5. *Si la característica de K es p, los irreducibles de $K[x]$ de grado no múltiplo de p no tienen raíces múltiples en ningún cuerpo extensión de K.*

Demostración: Iremos punto por punto:

1. Se dice que $a \in E$ es raíz múltiple de f si en $E[x]$ tenemos que $f = (x-a)^n q$ para algúnn $n \geq 1$ y $q \in E[x]$. En ese caso $f' = n(x-a)^{n-1}q + (x-a)^n q'$ y $f'(a) = 0$.

   Recíprocamente, si a no es raíz múltiple $f = (x-a)q$ de modo que $q(a) \neq 0$. En este caso, $f' = q + (x-a)q'$ y $f'(a) = q(a) \neq 0$.

2. Si $(f, f') = 1$ existen $A, B \in K[x]$ tales que $Af + Bf' = 1$ y si existiera una raíz múltiple a tendríamos que $f(a) = f'(a) = 0$ y así $1 = 1(a) = 0$, absurdo.

3. Por ser $f' \neq 0$ lo deducimos de 2.

4. La derivada de un polinomio no constante no es nula y se puede aplicar lo anterior.

5. La derivada de un polinomio de grado no múltiplo de p no es nula y se puede aplicar también lo anterior.

□

Proposición 2.9. *Sea E un cuerpo de característica cero o p tal que p no divide a n en el que $f = x^n - 1$ factoriza como producto de polinomios de grado 1. Las raíces de f se llaman raíces n-ésimas de la unidad. El polinomio f tiene exactamente n raíces distintas y forman un grupo cíclico con la multiplicación de E.*

Demostración: Como la característica de K es cero ó p, $f' = nx^{n-1} \neq 0$, además f y f' son primos entre sí, luego por el resultado anterior se tiene que las raíces de f en E son todas distintas.

Sea H el conjunto de las n raíces de f. Es claro que H es un grupo abeliano con la multiplicación de E. Los elementos de H que están en un subgrupo de orden p, con p divisor de n son raíces de $x^p - 1$, luego sólo pueden existir p elementos de este tipo, es decir, sólo existe un subgrupo de H de orden p, que sólo lo cumplen los grupos cíclicos.

Así, para $H = \{\text{raíces de } x^n - 1\}$ $\exists \xi \in H$ tal que $H = \langle \xi \rangle = \{1, \xi, \xi^2, \ldots, \xi^{n-1}\}$. A esta ξ se le llama raíz n-ésima primitiva de la unidad.

□

2.3. Extensiones algebraicas de cuerpos

Definición 2.10. *Decimos que E/K es una extensión de cuerpos si K es un subcuerpo de E.*

Es claro que E es un K-espacio vectorial. La extensión se dice finita si la dimensión de E como K-espacio vectorial es fintia. Escribiremos $|E : K| = dim_K E$ y a este número lo llamaremos grado de la extensión.

Proposición 2.11. *Sea E una extensión de L, y a su vez L una extensión de K. Diremos entonces que L es un cuerpo intermedio, ya que se tiene que $K \subseteq L \subseteq E$. Entonces E/K es finita si y sólo si E/L y L/K lo son. En este caso, se tiene*

$$|E : K| = |E : L||L : K|.$$

Demostración: Partimos primero de que E/K es finita, entonces $|E : K|$ es finita y que L como K-espacio vectorial esté contenido en E K-espacio vectorial implica que $dim_K L \leq dim_K E < \infty$, es decir, $|L : K|$ es finito. Por otro lado, si $B = \{u_1, \ldots, u_n\}$ es una base de E como K-espacio vectorial y $v \in E$, entonces $v = \sum_i k_i u_i$, con los $k_i \in K \subseteq L$. Así, B genera E como L-espacio vectorial, es decir, $dim_L E$ es finita y así $|E : L|$ también.

Recíprocamente, si $|L : K| = s$ y $|E : L| = r$, sean $\{l_1, \ldots, l_s\}$ y $\{e_1, \ldots, e_r\}$ bases de L como K-espacio vectorial y E como L-espacio vectorial respectivamente. Veamos ahora que $U = \{v_{ij} : v_{ij} = l_i e_j, \forall i, j\}$ es una base de E como K-espacio vectorial. En efecto, si $m \in E$, $m = \sum_j^r d_j e_j$, con $d_j \in L$, y a su vez $d_j = \sum_i^s c_{ji} l_i$, con los $c_{ji} \in K$. Por lo tanto,

$$m = \sum_{j=1}^{r} \left(\sum_{i=1}^{s} c_{ji} l_i \right) e_j = \sum_{j=1}^{r} \sum_{i=1}^{s} c_{ji} v_{ij}, \;\; c_{ji} \in K.$$

Con esto, U genera el E K-espacio vectorial. Ahora veamos que U es también linealmente independiente, para ello supongamos que

$$0 = \sum_{j=1}^{r} \sum_{i=1}^{s} c_{ji} v_{ji} = \sum_{j=1}^{r} \left(\sum_{i=1}^{s} c_{ji} l_i \right) e_j, \;\; c_{ji} \in K.$$

Como $\{e_1, \ldots, e_r\}$ es una base de E como L-espacio vectorial tenemos que $\sum_i^s c_{ji} l_i = 0$ para todo $j = 1, \ldots, r$. Y como $\{l_1, \ldots, l_s\}$ es una base de L como K-espacio

vectorial entonces $c_{ji} = 0$ también para todo $i = 1, \ldots, s$. Así, es linealmente independiente, y además

$$|E : K| = rs = |E : L||L : K|.$$

□

Definición 2.12. *Sea E una extensión de K y sean $f(x) = \sum_i k_i x^i \in K[x]$ y $a \in E$. Diremos que a es una **raíz** de f si $f(a) = \sum_i k_i a^i = 0$.*

Definición 2.13. *Sea E/K una extensión y $X \subseteq E$. Entonces $K(X)$ es la intersecciń de los subcuerpos de E que contienen a K y a X, es decir, el menor subcuerpo de E que contiene a K y a X.*

Proposición 2.14. *Sea E/K una extensión y $\alpha \in E$. Entonces*

$$K(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} : f, g \in K[x], g(\alpha) \neq 0 \right\}.$$

Además, por inducción podemos definir $K(\alpha_1, \ldots, \alpha_n) = K(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n)$.

Definición 2.15. *Sea E/K una extensión y $\alpha \in E$. Diremos que α es **algebraico** sobre K si existe un $p \in K[x]$ no nulo tal que $p(\alpha) = 0$, es decir, que α sea una raíz de p. Si α no es algebraico sobre K se dice entonces que es **trascendente**. La extensión E/K se dirá **algebraica** si todo elemento de E es algebraico sobre K.*

Ejemplo 2.15.1. *Algunos ejemplos:*

1. *Si $\alpha \in E$, entonces α es algebraico sobre E.*
2. *$\sqrt{2}$ es algebraico sobre $\mathbb{Q}$, ya que es raíz de $x^2 - 2$.*
3. *Los números e y π son trascendentes sobre $\mathbb{Q}$.*
4. *El número $\alpha = \sqrt{2 + \sqrt{5}}$ es algebraico sobre Q, pues $\alpha^2 = 2 + \sqrt{5}$ ó sea $\alpha^2 - 2 = \sqrt{5}$, y entonces $\alpha^4 - 4\alpha^2 - 1 = 0$. Por tanto, α es raíz del polinomio $p(x) = x^4 - 4x^2 - 1 \in \mathbb{Q}[x]$.*

■

Proposición 2.16. *Toda extensión finita es algebraica.*

Demostración: Sea E/K finita y $n = |E : K|$. Si $\alpha \in E$, la familia $\{1, \alpha, \ldots, \alpha^n\}$ tienen $n + 1$ elementos (iguales o repetidos). Como $dim_K E = n$, dicha familia tiene que ser linealmente dependiente. Así, existen $t_0, t_1, \ldots, t_n \in K$ no todos nulos tales que $t_0 1 + t_1\alpha + \ldots + t_n\alpha^n = 0$. Sea $p(x) = t_0 + t_1 x + \ldots + t_n x^n$. Entonces $p(x) \in K[x]$, $p(x) \neq 0$ y $p(\alpha) = 0$.

□

Proposición 2.17 (*Elemento algebraico*). *Sean E/K una extensión y $a \in E$ algebraico sobre K, se tiene:*

1. *Existe un único polinomio mónico $p \in K[x]$ irreducible en $K[x]$ tal que $p(a) = 0$.*

2. *Si $q \in K[x]$, entonces $q(a) = 0$ si y sólo si p divide a q.*

3. *$K(a) = \{f(a) : f \in K[x]\}$.*

4. *Si $\delta(p) = n$, entonces $\{1, a, \ldots, a^{n-1}\}$ es una K-base del espacio vectorial $K(a)$. Por tanto, $|K(a) : K| = \delta(p)$.*

Demostración: Veamos cada parte:

1. Para probar este apartado reutilizaremos conceptos del apartado siguiente. Supongamos que $p = gh$, se tiene que $0 = g(a)h(a)$ luego g ó h están en I, en contra de la minimalidad del grado de p, luego absurdo y así p es irreducible. Cualquier otro polinommio de I es divisible por p, luego es el único polinomio de I irreducible y mónico, además de tener el menor grado posible.

2. Definimos
$$\begin{array}{rccc} \varphi\colon & K[x] & \longrightarrow & E \\ & f & \longmapsto & f(\alpha), \end{array}$$
que es la restricción a $K[x]$ del homomorfismo evaluación, luego es homomorfismo de anillos. Como a es algebraico, el ideal $I = Ker\varphi$ es distinto de $\{0\}$. Por ser $K[x]$ un dominio de ideales principales, existe un único $p \in K[x]$ mónico tal que $I = (p)$ (de grado mínimo en I). Tenemos que si $q \in K[x]$ entonces $q(a) = 0$ si y sólo si p divide a q.

3. $\varphi(K[x]) = \{f(a) : f \in K[x]\} \subseteq K(a)$. Como p es irreducible $K[x]/(p) = K[x]/Ker\varphi$ es cuerpo, luego $\varphi(K[x]) \cong K[x]/Ker\varphi$ es cuerpo, claramente contiene a K y al elemento $a \in E$, luego $\varphi(K[x]) = K(a)$ y así $K(a) = \{f(a) : f \in K[x]\}$.

4. Sea $\delta(p) = n$, si $\{1, a, \ldots, a^{n-1}\}$ fuese K-ligada existiría un polinomio no nulo $g \in K[x]$ de grado $n-1$ tal que $g(a) = 0$, en contra de 1. Todo elemento $K(a)$ es de la forma $f(a)$ para algún $f \in K[x]$ por el apartado anterior. Por ser $K[x]$ un dominio euclídeo, existen $q, r \in K[x]$ tales que $f = qp+r$ y $\delta(r) < \delta(p) = n$. Se tiene así que $f(a) = q(a)p(a) + r(a) = r(a)$ y como $\delta(r) < n$, $r(a)$ es una K-combinación lineal de $\{1, a, \ldots, a^{n-1}\}$. Así $\{1, a \ldots, a^{n-1}\}$ genera $K(a)$ y ya está.

□

Definición 2.18. *Al polinomio que acabamos de ver se le conoce como* ***polinomio mínimo*** *ó también* ***polinomio irreducible*** *de a sobre K y se denota por $Irr(a, K)$. Es el polinomio mónico, irreducible y de menor grado posible de $K[x]$ que tiene a a por raíz. Cualquier otro polinomio de $K[x]$ que tenga por raíz a a será múltiplo de $Irr(a, K)$.*

Ejercicio 3. *Sea $p(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$, recordemos que existe un cuerpo en el que este polinomio tiene una raíz que llamamos a. Sea $\mathbb{Z}_2(a)$. Veamos cuántos elementos tiene $\mathbb{Z}_2(a)$ y cuántos tiene el grupo de unidades de $\mathbb{Z}_2(a)$.*

Lo primero que vamos a ver es que $x^3 + x + 1 \in \mathbb{Z}_2(a)$ es irreducible en $\mathbb{Z}_2[x]$. Para ello hay que ver que no se puede poner como producto de 2 polinomios de grado

inferior a 3 (uno de grado 1 y otro de grado 2), y como consecuencia, se reduce a comprobar que dicho polinomio no tiene raíces en $\mathbb{Z}/2\mathbb{Z} = \mathbb{Z}_2 = \{0, 1\}$.

Para lo primero: $x^3 + x + 1 = (x^2 + ax + b)(x + c) = x^3 + cx^2 + ax^2 + acx + bx + bc$, *luego* $c + a = 0$, $ac + b = 1$ *y* $bc = 1$ *y vemos que no se puede porque llegaríamos a la conclusión de que* $1 = 0$. *También podríamos evaluar el polinomio y obtendríamos que* $p(0) = 1 \neq 0$ *y* $p(1) = 1 \neq 0$, *luego* p *no tiene raíces en* $\mathbb{Z}_2$ *y así es irreducible en* $\mathbb{Z}_2[x]$.

Al ser mónico tenemos que $Irr(a, \mathbb{Z}_2) = p$, *con* a *una raíz de* p. *El cuerpo en el que* p *tiene una raíz sabemos que es* $\mathbb{Z}_2[x]/(p)$, *que por un resultado anterior sabemos que tiene* $2^{\delta(p)} = 2^3 = 8$ *elementos. Así que* $\mathbb{Z}_2(a)$ *tiene 8 elementos. Y como es cuerpo sabemos que 7 de ellos son unidades. También sabemos que una base de* $\mathbb{Z}_2(a)$ *es* $\{1, a, a^2\}$, *con* a *raíz de* p. *Luego* $\mathbb{Z}_2(a) = \{t_0 + t_1 a + t_2 a^2 : t_0, t_1, t_2 \in \mathbb{Z}_2\}$. *Y además esto tiene sentido ya que los únicos valores posibles para* t_0, t_1, t_2 *son 0 ó 1.*

■

Ejemplo 2.18.1. *Algunos casos de polinomios irreducibles:*

1. *Si consideramos la extensión* $\mathbb{Q}(i)/\mathbb{Q}$, *entonces* $x^2 + 1 \in \mathbb{Q}[x]$ *es irreducible, mónico y tiene a* i *por raíz, luego es el polinomio irreducible de* i *sobre* $\mathbb{Q}$. *Así,* $\{1, i\}$ *es una base de* $\mathbb{Q}(i)$ *sobre* $\mathbb{Q}$:

$$\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}.$$

2. *De igual forma tenemos que* $x^2 - 2 = Irr(\sqrt{2}, \mathbb{Q})$, $x^2 - 3 = Irr(\sqrt{3}, \mathbb{Q})$ *y así* $|\mathbb{Q}(\sqrt{2}) : \mathbb{Q}| = 2$, $|\mathbb{Q}(\sqrt{3}) : \mathbb{Q}| = 2$ *y* $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, $\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} : a, b \in \mathbb{Q}\}$.

■

Definición 2.19. *Sea una extensión* E/K, *llamaremos* ***clausura algebraica*** *de* K *en* E *al conjunto de los elementos algebraicos de una extensión, y la denotaremos por* $Cl_K^E = \{\alpha \in E : \alpha \text{ es algebraico sobre } K\}$.

Proposición 2.20. *Sea* E/K *una extensión. Si* $\alpha_1, \ldots, \alpha_n \in E$ *son algebraicos sobre* K, $K(\alpha_1, \ldots, \alpha_n)/K$ *es finita, luego algebraica.*

Demostración: La haremos por inducción sobre n. Si $n = 1$, ya sabemos que $|K(\alpha_1) : K|$ es finito. Supongamos el resultado cierto para $n - 1$ y probémoslo para n. Como α_n es algebraico sobre K, también es algebraico sobre $K(\alpha_1, \ldots, \alpha_{n-1})$. Así, $|K(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n) : K(\alpha_1, \ldots, \alpha_{n-1})|$ es finito. Por inducción, $|K(\alpha_1, \ldots, \alpha_{n-1}) : K|$ es finito. Pero $K(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n) = K(\alpha_1, \ldots, \alpha_n)$. Por 2.11

$$|K(\alpha_1, \ldots, \alpha_n) : K| = |K(\alpha_1, \ldots, \alpha_n) : K(\alpha_1, \ldots, \alpha_{n-1})||K(\alpha_1, \ldots, \alpha_{n-1}) : K|$$

es finito.

□

Lema 2.20.1. *Sea $\sigma\colon K_1 \longrightarrow K_2$ un isomorfismo de cuerpos. Entonces σ se extiende a un isomorfismo de $K_1[x]$ en $K_2[x]$ haciendo que, si $f \in K_1[x]$ con $f = a_0 + a_1x + \ldots + a_kx^k$, entonces $\sigma(f) = \sigma(a_0) + \sigma(a_1)x + \ldots + \sigma(a_k)x^k$. En particular,*

$$f \text{ es irreducible} \Longleftrightarrow \sigma(f) \text{ es irreducible.}$$

Proposición 2.21. *Sean E_1/K_1 y E_2/K_2 dos extensiones. Sean $\sigma\colon K_1 \longrightarrow K_2$ un isomorfismo. Sea $p_1 \in K_1[x]$ irreducible. Sea $p_2 = \sigma(p_1)$. Sea α_i raíz de p_i, $i = 1, 2$. Entonces σ se extiende a un isomorfismo de cuerpos $\theta\colon K_1(\alpha_1) \longrightarrow K_2(\alpha_2)$ tal que $\theta(\alpha_1) = \alpha_2$.*

$$\begin{array}{ccc} K_1(\alpha_1) & \xrightarrow{\quad\theta\quad} & K_2(\alpha_2) \\ \uparrow & & \uparrow \\ K_1 & \xrightarrow{\quad\sigma\quad} & K_2 \end{array}$$

Demostración: Supongamos que p_1 es mónico, con lo que p_2 también lo es. Entonces, como p_1 y p_2 son irreducibles,

$$p_1 = Irr(\alpha_1, K_1),$$

$$p_2 = Irr(\alpha_2, K_2).$$

Ahora, $K_1(\alpha_1) = \{f(\alpha_1) : f \in K_1[x]\}$, $K_2(\alpha_2) = \{f(\alpha_2) : f \in K_2[x]\}$. Definimos

$$\begin{array}{rccc} \theta\colon & K_1(\alpha_1) & \longrightarrow & K_2(\alpha_2) \\ & f(\alpha_1) & \longmapsto & \sigma(f)(\alpha_2). \end{array}$$

Y ahora veamos que está bien definida: si $f, g \in K_1[x]$, $f(\alpha_1) = g(\alpha_1) \Leftrightarrow (f - g)(\alpha_1) = 0 \Leftrightarrow p_1 \mid f - g \Leftrightarrow \sigma(p_1) \mid \sigma(f - g) \Leftrightarrow p_2 \mid \sigma(f) - \sigma(g) \Leftrightarrow (\sigma(f) - \sigma(g))(\alpha_2) = 0 \Leftrightarrow \sigma(f)(\alpha_2) = \sigma(g)(\alpha_2)$.

Es inyectiva: $\theta(f(\alpha_1)) = \sigma(f)(\alpha_2) = 0 \Rightarrow f(\alpha_1) = 0$. Es fácil ver que también es suprayectiva.

Y es claro que θ es homomorfismo de cuerpos:

$$\theta(f(\alpha_1) + g(\alpha_1)) = \theta((f + g)(\alpha_1)) = \sigma(f + g)(\alpha_2) = (\sigma(f) + \sigma(g))(\alpha_2) = \sigma(f)(\alpha_2) + \sigma(g)(\alpha_2) = \theta(f(\alpha_1)) + \theta(g(\alpha_1)).$$

Igual con el producto.

□

Corolario 2.21.1. *Sea $p \in K[x]$ irreducible, α y β raíces de p en una extensión E de K. Existe un isomorfismo $\theta\colon K(\alpha) \longrightarrow K(\beta)$ tal que $\theta|_K = id, \theta(\alpha) = \beta$. Recíprocamente, si $\alpha, \beta \in E$, siendo E/K una extensión, y existe un isomorfismo $\theta\colon K(\alpha) \longrightarrow K(\beta)$ tal que $\theta|_K = id, \theta(\alpha) = \beta$, entonces $Irr(\alpha, K) = Irr(\beta, K)$.*

Demostración: La primera parte se deduce del anterior resultado, tomando $K_1 = K_2$ y $\sigma = id$. Sea ahora $Irr(\alpha, K) = x^k + a_{k-1}x^{k-1} + \ldots + a_1 x + a_0$. Entonces,

$$\alpha^k + a_{k-1}\alpha^{k-1} + \ldots + a_1\alpha + a_0 = 0.$$

Aplicando θ tenemos: $\theta(\alpha)^k + a_{k-1}\theta(\alpha)^{k-1} + \ldots + a_1\theta(\alpha) + a_0 = \beta^k + a_{k-1}\beta^{k-1} + \ldots + a_1\beta + a_0 = 0$ (ya que $\theta|_K = id$). Luego, $Irr(\alpha, K) = Irr(\beta, K)$.

□

Recordemos la necesidad de que $p \in K[x]$ sea irreducible. Entonces, dadas α y β raíces en una extensión E de K,

$$\begin{array}{rccc} \theta\colon & K(\alpha) & \longrightarrow & K(\beta) \\ & \alpha & \longmapsto & \beta \\ & k & \longmapsto & k \end{array}$$

Definición 2.22. *Si E es una extensión algebraica de K, $\alpha, \beta \in E$, diremos que α y β son **conjugados sobre** K si $Irr(\alpha, K) = Irr(\beta, K)$, o equivalentemente si α es raíz de $Irr(\beta, K)$. Lo denotaremos por $\alpha\ conj_K\ \beta$.*

Así, el anterior corolario nos viene a decir que todo eso ocurre si y sólo si α y β son conjugados.

Definición 2.23. *Sea E/K una extensión. Diremos que $\varphi\colon E \longrightarrow E$ es un **K-homomorfismo de cuerpos** si*

1. *φ es un homomorfismo de cuerpos.*
2. *$\varphi|_K = id_K$, es decir, $\varphi(k) = k\ \forall k \in K$.*

Definición 2.24. *Diremos que un cuerpo K es **algebraicamente cerrado** si contiene a todas las raíces de los polinomios no constantes de $K[x]$.*

Proposición 2.25. *Si K es un cuerpo algebraicamente cerrado y E es un extensión algebraica de K, entonces $E = K$.*

Demostración: Si $\alpha \in E$, $f(x) = Irr(\alpha, K)$ es un polinomio no constante de $K[x]$. En consecuencia α es raíz de f, con $f \in K[X]$. Como K es algebraicamente cerrado, $\alpha \in K$.

□

Recordemos el siguiente resultado:

Proposición 2.26. *Sea $p \in K[x]$ y $a \in K$. Entonces $p(a) = 0$ si, y sólo si $x - a \mid p$.*

Demostración: Aplicamos el algoritmo de la división a p y $x - a$: $p = (x - a)q + r$, donde $r = 0$ ó $\delta(r) < \delta(x - a)$. Si $r = 0$ ya está, si no entonces es una constante y como $p(a) = 0 \Leftrightarrow r(a) = 0$ entonces $r = 0$ y así $x - a \mid p$.

□

Definición 2.27. *Sea $f \in K[x]$ un polinomio y E/K una extensión. Diremos que f* ***se escinde*** *en E si existen $a_1, \ldots, a_n \in E$ tales que $f = a(x - a_1) \ldots (x - a_n)$, con $a \in K$. Si además $E = K(a_1, \ldots, a_n)$ decimos que E es un* ***cuerpo de escisión de f sobre*** *K.*

Los cuerpos de escisión siempre existen y son únicos:

Teorema 2.28 (***Existencia de cuerpos de escisión***)**.** *Si $f \in K[x]$, existe un cuerpo de escisión de f sobre K.*

Demostración: Lo haremos por inducción sobre el grado de f: Si f se escinde en K (en particular, si $\delta(f) = 1$), entonces K es un cuerpo de escisión de f sobre K. Supongamos que no es así y sea f_1 un factor irreducible de f de grado mayor que 1. Por **??**, existe una extensión E de K en la que f_1 tiene una raíz a. Entonces $f(a) = 0$ ya que $f_1(a) = 0$. Por 2.26 $x - a \mid f$ y así $f = (x - a)g$, con $g \in K(a)[x]$. Como $\delta(g) < \delta(f)$, por la hipótesis de inducción tenemos que existe un cuerpo de escisión de g sobre $K(a)$. Será $g = b(x - b_1) \ldots (x - b_m)$ y el cuerpo de escisión de g (sobe $K(a)$) será $K(a)(b_1, \ldots, b_m) = K(a, b_1, \ldots, b_m)$. Ahora, $f = b(x - a)(x - b_1) \ldots (x - b_m)$ y su cuerpo de escisión sobre K es $K(a, b_1, \ldots, b_m)$.

□

Proposición 2.29. *Sea $\sigma\colon K_1 \longrightarrow K_2$ un isomorfismo, $f_1 \in K_1[x]$ y $f_2 = \sigma(f_1) \in K_2[x]$. Sean E_i, con $i = 1, 2$ cuerpos de escisión de f_i sobre K_i, $i = 1, 2$. Entonces existe un isomorfismo $\tau\colon E_1 \longrightarrow E_2$ que extiende σ, es decir, $\tau|_{K_1} = \sigma$.*

Demostración: Inducción sobre $|E_1 : K_1|$:

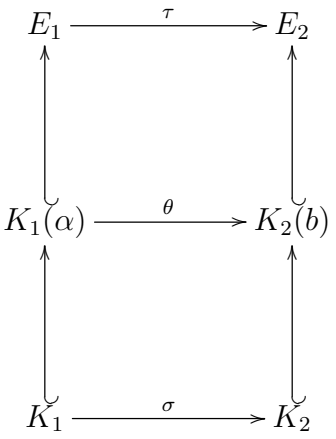
Si $|E_1 : K_1| = 1$, entonces $E_1 = K_1$ es cuerpo de escisión de f_1 sobre K_1. Como $\sigma\colon K_1[x] \longrightarrow K_2[x]$ es isomorfismo de anillos, también $\sigma(f_1)$ $(= f_2)$ se escindirá sobre K_2. Así $E_2 = K_2$ y basta tomar $\tau = \sigma$.

Supongamos que $|E_1 : K_1| > 1$ y que el resultado es cierto para extensiones de menor grado. Como $|E_1 : K_1| > 1$, f_1 no se escinde en K_1 y existe un factor irreducible (importante esto!) p de f_1 tal que $\delta(p) > 1$. Como f_1 se escinde en E_1, también p se escinde en E_1 y $\sigma(p)$ se escinde en E_2. Sea $a \in E_1$, raíz de p y sea $b \in E_2$ raíz de $\sigma(p)$. Por existe un isomorfismo $\theta\colon K_1(a) \longrightarrow K_2(b)$ que extiende σ, es decir $\theta|_{K_1} = \sigma$.

Ahora, E_1 es cuerpo de escisión de f_1 sobre $K_1(a)$. Y E_2 es cuerpo de escisión de f_2 $(= \sigma(f_1))$ sobre $K_2(b)$. Además,

$$|E_1 : K_1| = |E_1 : K_1(a)||K_1(a) : K_1| > |E_1 : K_1(a)|, \text{ ya que } a \notin K_1 .$$

Por inducción, existe $\tau\colon E_1 \longrightarrow E_2$ isomorfismo que extiende θ, luego también extiende σ.



□

Corolario 2.29.1 (***Unicidad de los cuerpos de escisión***)**.** *Si E_1, E_2 son cuerpos de escisión de un mismo polinomio f de $K[x]$ sobre K, existe entonces $\tau\colon E_1 \longrightarrow E_2$ isomorfismo tal que $\tau|_K = id$.*

Demostración: Basta hacer $K_1 = K_2 = K$ y $\sigma = id$ en la proposición anterior.

□

2.4. Cuerpos finitos

Teorema 2.30. *Sea K un cuerpo finito, entonces $|K| = p^n$ para algún primo p y algún entero n. Recíprocamente, para todo primo p y entero positivo n existe un único cuerpo, salvo isomorfismo, de p^n elementos.*

Demostración: Sabemos que por ser finito la caracteristica debe ser un primo p y por 2.6 el cuerpo primo de K es F isomorfo a $\mathbb{Z}_p$. Por ser K finito K es F-espacio vectorial de dimensión finita y existen $a_1, \ldots, a_n \in K$ que son una F-base. Como cada elemento de K se escribe de manera única como F-combinación lineal de los elementos a_i, concluimos que $|K| = p^n$.

Recíprocamente, supongamos que p es un primo y n un entero positivo. Sea $F = \mathbb{Z}_p$ y E el cuerpo de escisión de $f = x^{p^n} - x \in F[x]$. Notemos que $f' = -1$, luego no tiene factores comunes con f y en tal caso sabemos que todas las raíces son distintas y $|U| = p^n$, con U el conjunto de todas las raíces de f. Si $a, b \in U$, por el ejercicio 2 tenemos que $a - b \in U$, y si $b \neq 0, a/b \in U$. Tenemos así que U es un subcuerpo de E y como $E = F(U)$ se tiene que $U = E$ y $|E| = p^n$.

Sea L otro cuerpo de p^n elementos. Por ser finito su característica es finita, su cuerpo primo es $\mathbb{Z}_q$, con q primo, y su orden una potencia de q, luego $p = q$ y el cuerpo primo D es isomorfo a F. Los elementos no nulos de L son un grupo multiplicativo de orden $p^n - 1$, luego el orden de cualquiera de ellos es divisor de $p^n - 1$ y se tiene que para todo $0 \neq l \in L$, $l^{p^n - 1} = 1$, luego $l^{p^n} = l$.

Así, L es cuerpo de escisión de $x^{p^n} - x$ sobre D. Por la unicidad de los cuerpos de escisión de un mismo polinomio tenemos que L es isomorfo a E.

□

Al cuerpo de p^n elementos se le suele denotar $GF(p^n)$, por *Galois Field*.

Proposición 2.31. *Para todo primo p y entero positivo n, existen polinomios en $\mathbb{Z}_p[x]$ irreducibles de grado n.*

Demostración: Sea $f = x^{p^n} - x \in \mathbb{Z}_p[x]$ y E cuerpo de escisión de f sobre $\mathbb{Z}_p$. Ya hemos dicho que las raíces de f son p^n y además son un cuerpo, luego $E = \{\text{raíces de } f\}$ y $|E : \mathbb{Z}_p| = n$. Pero por otra parte

$$\{\text{raíces de } f\} = \{0\} \cup \{\text{raíces de } x^{p^n-1} - 1\}$$

y $\{\text{raíces de } x^{p^n-1} - 1\}$ es un grupo cíclico, por lo que va a existir un $a \in E$ tal que $\{\text{raíces de } x^{p^n-1} - 1\} = \langle a \rangle$ y se tiene que $E = \mathbb{Z}_p(a)$ y por el grado de la extensión, el grado del polinomio mínimo de a sobre $\mathbb{Z}_p$, que es irreducible, es n.

□