

AMPLIACIÓN DE MATEMÁTICAS

LEMA DE BEZOUT. TEOREMA DE FACTORIZACIÓN ÚNICA.

Teorema 1. (*Lema de Bezout*). Sean dos polinomios $P, Q \in \mathbb{F}[x]$ y $d \in m.c.d.(P, Q)$, entonces existe otros dos polinomios $u, v \in \mathbb{F}[x]$ de modo que

$$d(x) = u(x)P(x) + v(x)Q(x).$$

Observación 1. Este Lema prueba, además, que el máximo común divisor de dos polinomios es **no** vacío.

Demostración: Se procede de forma análoga a como lo hicimos en $\mathbb{Z}$. Sea

$$A = \{ grad.h \in \mathbb{N} : h(x) = k_1(x)P(x) + k_2(x)Q(x) \neq 0 \text{ donde } k_1, k_2 \in \mathbb{F}[x] \}.$$

Como $grad.P$ y $grad.Q$ están en A , éste es no vacío, y por tanto existen $m \in A$ y $u, v \in \mathbb{F}[x]$ con $m = grad.(u(x)P(x) + v(x)Q(x))$.

Sea $d'(x) = u(x)P(x) + v(x)Q(x)$. Veamos ahora que d' divide a todo polinomio de la forma $k_1(x)P(x) + k_2(x)Q(x)$. Si no fuese así,

$$k_1(x)P(x) + k_2(x)Q(x) = q(x)d'(x) + r(x)$$

con $grad.r < grad.d'$ y $r \neq 0$. De lo que se deduce que

$$\begin{aligned} r(x) &= k_1(x)P(x) + k_2(x)Q(x) - q(x)d'(x) \\ &= (k_1(x) - q(x)u(x))P(x) + (k_2(x) - q(x)v(x))Q(x). \end{aligned}$$

Lo que contradice que m sea el mínimo del conjunto A .

Ahora podemos decir que $d'|P$ y que $d'|Q$. Si otro polinomio h divide a P y Q entonces

$$h|uP + vQ = d'$$

y por tanto $grad.h \leq grad.d'$. Lo que prueba que $d' \in m.c.d.(P, Q)$

La última parte de la demostración la da el siguiente corolario.

Corolario 1. Si $d, d' \in m.c.d.(P, Q)$, entonces existe $c \in \mathbb{F}^*$ de modo que $d = cd'$.

Demostración: Tanto d como d' dividen a P y Q y son de grado máximo, por lo tanto

$$\text{grad}.d = \text{grad}.d'$$

Por otro lado, $d' = uP + vQ$, por tanto $d|d'$, es decir $d' = qd$. Como d y d' tienen el mismo grado, necesariamente $q \in \mathbb{F}$ $\square$

Observación 2. Existe un único $d \in m.c.d.(P, Q)$ **mónico**.

Corolario 2. Sean $P, Q, H \in \mathbb{F}[x]$, de modo que P es un polinomio irreducible y tal que $P|QH$. Entonces o bien $P|Q$ o bien $P|H$.

Demostración: Si P divide a Q hemos terminado. Si no, como P es irreducible se tiene que $1 \in m.c.d.(P, Q)$ y por el Lema de Bezout

$$1 = u(x)P(x) + v(x)Q(x) \quad \Rightarrow \quad H(x) = u(x)P(x)H(x) + v(x)Q(x)H(x).$$

Como P divide a QH , se sigue que P divide a H $\square$

La propiedad que sigue, que ya probamos en $\mathbb{Z}$ (ver el capítulo sobre **Ideales Maximales**), es esencial para probar la existencia de **cuerpos de descomposición** de polinomios (que veremos en el próximo tema).

Corolario 3. Sea $\mathbb{F}$ un cuerpo y sea $P \in \mathbb{F}[x]$.

A: $\mathbb{F}[x]$ es un **dominio de ideales principales**.

B: (P) , el ideal generado por el polinomio P , es un **ideal maximal** si y solo si P es **irreducible**.

Demostración:

A: Sea $I \subseteq \mathbb{F}[x]$ un ideal. Tomemos $P, Q \in I$. Por el Lema de Bezout existe

$$m.c.d.(P, Q) = d(x) = u(x)P(x) + v(x)Q(x),$$

que podemos tomar mónico. Además por ser I ideal, $d \in I$.

- Si $d = 1$, entonces $I = \mathbb{F}[x]$.
- Si $\text{grad}.d > 0$, entonces $d\mathbb{F}[x] \subseteq I$.

Sea

$$n = \min\{\text{grad}.d \in \mathbb{N} \setminus \{0\} : d\mathbb{F}[x] \subseteq I\}$$

Veamos que si $d'\mathbb{F}[x] \subseteq I$ y $\text{grad}.d' = n$, entonces necesariamente $I = (d')$ y así es un ideal principal. Sea $P \in I$. Tenemos que $P(x) = q(x)d'(x) + r(x)$ con $\text{grad}.r < \text{grad}.d'$

- Si $r = 0$, entonces $P \in d'\mathbb{F}[x] = (d')$.
- Si $r \neq 0$, entonces $r = P - qd' \in I$ y así $r\mathbb{F}[x] \subseteq I$. Esto es contradictorio con la definición de n .

Todo lo cuál prueba que $I = d'\mathbb{F}[x]$, y por tanto es un ideal principal.

- B:**
- Si $d|P$, y $0 < \text{grad}.d < \text{grad}.P$, entonces $(P) \subsetneq (d)$. Así el ideal generado por P , (P) , no es maximal.
 - Si (P) es un ideal **no** maximal de $\mathbb{F}[x]$, entonces existe otro ideal (d) , por **A** este nuevo ideal es necesariamente principal, de modo que $P\mathbb{F}[x] = (P) \subsetneq (d) = d\mathbb{F}[x]$ y con $d\mathbb{F}[x] \subsetneq \mathbb{F}[x]$. Por lo tanto $d|P$, con $0 < \text{grad}.d < \text{grad}.P$ (en otro caso o bien $(d) = \mathbb{F}[x]$ o bien $(d) = (P)$ que sabemos que no ocurre). Por tanto P no es irreducible $\square$.

Ejemplo 1. $\mathbb{Z}[x]$ **no** es un dominio de ideales de principales. Esto es así ya que como $\mathbb{Z}$ no es un cuerpo, no tenemos ni el Teorema del Resto ni el Lema de Bezout que serían las herramientas para probarlo.

Veamos un ejemplo concreto. Sea

$$I = \{ f \in \mathbb{Z}[x] : \bar{f}(0) \in 3\mathbb{Z} \}.$$

Es muy fácil ver que I es un ideal en $\mathbb{Z}[x]$. Tampoco es difícil convencerse de que $I = (3, x)$. Luego **no** es un ideal principal $\square$

Teorema 2. (de Factorización Única). Sea $\mathbb{F}$ un cuerpo. Para cada $P \in \mathbb{F}[x]$ existe una única representación (salvo el orden) de la forma

$$P(x) = rP_1(x)P_2(x)\dots P_k(x),$$

donde $r \in \mathbb{F}$, y $P_j \in \mathbb{F}[x]$ es un polinomio mónico irreducible sobre $\mathbb{F}$ para $j = 1, 2, \dots, k$,

Demostración: Por inducción sobre el grado de P .

- Si $\text{grad}.P = 1$, entonces

$$P(x) = rx + b = r\left(x + \frac{b}{r}\right)$$

donde $\left(x + \frac{b}{r}\right)$ es mónico e irreducible (por ser de grado 1).

- Si $\text{grad}.P < n$, admitimos como hipótesis de inducción que P se descompone en producto de polinomios irreducibles.
- Si $\text{grad}.P = n$, o bien P es irreducible y no hay nada que probar (salvo sacar factor común el coeficiente de x^n), o bien existe $Q \in \mathbb{F}[x]$ con $1 \leq \text{grad}.Q < n$ de modo que

$$Q|P \quad \Leftrightarrow \quad P(x) = Q(x)q(x),$$

con $1 \leq \text{grad}.q < n$. Ahora se aplica la hipótesis de inducción a Q y q .

Por último veamos la unicidad. Si

$$P(x) = rP_1(x)P_2(x)\dots P_k(x) = sQ_1(x)Q_2(x)\dots Q_{k'}(x),$$

se tiene que $P_1|P$ y por tanto $P_1|Q_j$ para algún j . De la irreducibilidad de Q_j y de que es mónico, se tiene que $P_1 = Q_j$.

Ahora tenemos que

$$rP_2(x)\dots P_k(x) = sQ_1(x)Q_2(x)\dots Q_{j-1}Q_{j+1}\dots Q_{k'}(x).$$

Repitiendo el proceso anterior con P_2 luego con P_3 , etc llegamos a ver que todos los P_i son como los Q_j , que $k = k'$ y por último nos queda que $r = s$ $\square$

Observación 3. *El teorema nos dice que existe la factorización de todo polinomio, pero no como conseguirla.*

*Existen algoritmos para descomponer $P \in \mathbb{F}[x]$, para $\mathbb{F}$ un cuerpo **finito**, como el **algoritmo de Berlekamp** (pero esto ya es propio de un curso de Criptografía).*

Como en el caso de $\mathbb{Z}$, el costo computacional de factorizar $P \in \mathbb{F}[x]$ hace que los polinomios sobre cuerpos finitos sean útiles en Criptografía.

REFERENCIAS

DEPARTAMENTO DE ANÁLISIS MATEMÁTICO, FACULTAD DE MATEMÁTICAS,
UNIVERSIDAD COMPLUTENSE, 28040 MADRID, SPAIN
E-mail address: Cesar_Ruiz@mat.ucm.es