

AMPLIACIÓN DE MATEMÁTICAS

DIVISIBILIDAD DE POLINOMIOS.

Ejemplo 1. *Dados dos polinomios $p, q \in \mathbb{Z}[x]$ con q **mónico** se puede "dividir" p entre q .*

$$\begin{array}{ccc} x^2 + 2x + 1 & \mid x + 1 & ; \\ 0 & x + 1 & ; \end{array} \quad \begin{array}{ccc} x^2 + 2x + 2 & \mid x + 1 & ; \\ 1 & x + 1 & ; \end{array} \quad ; \quad \begin{array}{ccc} 3x^2 + 2x + 1 & \mid 2x + 1 & ? \end{array}$$

Si tomamos un **cuerpo** como el conjunto de coeficientes de un anillo de polinomios, esto nos permite dividir dos polinomios cualesquiera.

Teorema 1. (*del Resto*). *Sea $\mathbb{F}[x]$ un anillo de polinomios sobre un cuerpo $\mathbb{F}$. Para todo $P, Q \in \mathbb{F}[x]$, con $Q \neq 0$, existen polinomios $q, r \in \mathbb{F}[x]$ **únicos** tales que*

$$P(x) = q(x)Q(x) + r(x)$$

con $\text{grad}.r < \text{grad}.Q$.

Demostración: Análoga a la vista para números enteros.

Tomamos $R = \{h = P - qQ : q \in \mathbb{F}[x]\}$. Si $0 \in R$, existe $q \in \mathbb{F}[x]$ para el cual $P = qQ$. Tomando $r = 0$ se resuelve el problema. Si no, sea

$$S = \{\text{grad}.h : h \in R\}.$$

Como $S \subset \mathbb{N}$ y S es no vacío ($\text{grad}.(P - Q) \in S$), existe

$$m = \min S.$$

Por tanto existe algún $q \in \mathbb{F}[x]$ de modo que $r = P - qQ$ tiene grado igual a m . Veamos ahora que necesariamente $m < \text{grad}.Q = n$. Si no fuese así, tomando

$$a_m \neq 0 \text{ el coeficiente de la potencia de mayor grado de } r$$

y

$$b_n \neq 0 \text{ el coeficiente de la potencia de mayor grado de } Q,$$

y considerando

$$\begin{aligned} S(x) &= r(x) - \frac{a_m}{b_n} x^{m-n} Q(x) \\ &= (P(x) - q(x)Q(x)) - \frac{a_m}{b_n} x^{m-n} Q(x) \\ &= P(x) - \left(q(x) - \frac{a_m}{b_n} x^{m-n} \right) Q(x). \end{aligned}$$

Ahora, $\text{grad}.S(x) \leq m-1 < \text{grad}.r$ lo que contradice la naturaleza del mínimo m .

Observemos que para hacer la prueba hemos usado de forma esencial que $\mathbb{F}$ sea un cuerpo, así hemos podido usar el inverso de b_n .

Solo nos falta ver la unicidad del resto. Si

$$P(x) = q_1(x)Q(x) + r_1(x) = q_2(x)Q(x) + r_2(x)$$

con $\text{grad}.r_1, \text{grad}.r_2 < \text{grad}.Q$, entonces se tiene que

$$(q_1 - q_2)Q = r_1 - r_2.$$

Dos casos,

- si $q_1 = q_2$ se tiene que $r_1 = r_2$ y tenemos la unicidad;
- si $q_1 \neq q_2$ se tiene que

$$\text{grad}.(q_1 - q_2) + \text{grad}.Q = \text{grad}.(r_1 - r_2) \leq \max\{\text{grad}.r_1, \text{grad}.r_2\}.$$

Así, o bien $\text{grad}.Q \leq \text{grad}.r_1$ o bien $\text{grad}.Q \leq \text{grad}.r_2$. En cualquier caso llegamos a contradicción con la hipótesis $\square$

Ejemplo 2. Sea $P(x) = 3x^3 + x + 1$ y $Q(x) = 2x^2 + 1$ ambos polinomios de $\mathbb{Q}[x]$.

$$\begin{array}{r} 3x^3 + x + 1 \\ -3x^3 - \frac{3}{2}x \\ \hline \end{array} \quad \begin{array}{r} \frac{2x^2 + 1}{\frac{3}{2}x} \\ -\frac{1}{2}x + 1 \end{array}$$

Así tenemos que

$$3x^3 + x + 1 = \frac{3}{2}x(2x^2 + 1) - \frac{1}{2}x + 1,$$

con $\text{grad}.(-\frac{1}{2}x + 1) = 1 < 2 = \text{grad}.(2x^2 + 1)$.

Ejemplo 3. Sea $P(x) = x^4 + 3x^3 + 2x^2 + x + 4$ y $Q(x) = 3x^2 + 2x$ ambos polinomios de $\mathbb{Z}_5[x]$.

Para dividir este par de polinomios tenemos que operar los coeficientes en congruencias módulo 5. Los exponentes se operan en $\mathbb{N}$.

$$\begin{array}{r}
 x^4 + 3x^3 + 2x^2 + x + 4 \\
 \underline{-x^4 - 4x^3} \\
 4x^3 + 2x^2 + x + 4 \\
 \underline{-4x^3 - x^2} \\
 x^2 + x + 4 \\
 \underline{-x^2 - 4x} \\
 2x + 4
 \end{array}
 \quad
 \begin{array}{r}
 |3x^2 + 2x \\
 2x^2 + 3x + 2
 \end{array}$$

Así tenemos que

$$x^4 + 3x^3 + 2x^2 + x + 4 = 2x^2 + 3x + 2(3x^2 + 2x)2x + 4,$$

con $\text{grad.}(2x + 4) = 1 < 2 = \text{grad.}(3x^2 + 2x)$.

Ejemplo 4. En un cuerpo $\mathbb{F}$ son equivalentes

- A:** 1. $m|n$ donde $m, n \in \mathbb{N}$.
 2. $x^m - 1 | x^n - 1$ (donde la barra indica división exacta).
 En particular son equivalentes
- B:** 1. $m|n$
 2. $p^m - 1 | p^n - 1$
 3. $x^{p^m - 1} - 1 | x^{p^n - 1} - 1$.

Observación 1. El ejemplo anterior sirve para estudiar las raíces de la unidad en un cuerpo $\mathbb{F}$.

Demostración: Si $m, n \in \mathbb{N}$ con $m \leq n$, se tiene que

$$n = qm + r \quad \text{con} \quad 0 \leq r < m.$$

- Si $r = 0$, es decir si $m|n$, entonces

$$\begin{array}{c}
 \frac{x^{qm} - 1}{-x^{qm} + x^{(q-1)m}} - 1 \quad \frac{|x^m - 1}{x^{(q-1)m} + x^{(q-2)m} + \dots + 1} \\
 \frac{-x^{qm} + x^{(q-1)m}}{x^{(q-1)m}} - 1 \\
 \vdots \\
 \frac{-x^m + 1}{0}
 \end{array}$$

- Si $r \neq 0$, es decir si $m \nmid n$, entonces

$$\begin{array}{c} \frac{x^{qm+r} - 1}{-x^{qm+r} + x^{(q-1)m+r}} - 1 \\ \vdots \\ \frac{-x^{m+r} + x^r}{x^r - 1} \end{array} \quad \frac{|x^m - 1|}{x^{(q-1)m+r} + x^{(q-2)m+r} + \dots + x^r}$$

En particular

- Si $r = 0$, entonces $p^n - 1 = p^{qm} - 1 = (p^m - 1) \sum_{j=0}^{q-1} p^{jm}$.
- Si $r \neq 0$, entonces $p^n - 1 = p^{qm+r} - 1 = (p^m - 1) \left(\sum_{j=0}^{q-1} p^{jm+r} \right) + (p^r - 1)$.
- Luego si $n_1 = p^n - 1$ y $m_1 = p^m - 1$, $m \leq n$, entonces

$$p^m - 1 | p^n - 1 \quad \Leftrightarrow \quad x^{p^m-1} - 1 | x^{p^n-1} - 1 \quad \square$$

Ejemplo 5. Sea p un número primo y sea el polinomio $x^{p-1} - 1 \in \mathbb{Z}_p[x]$. Por el Teorema de Euler, como $\phi(p) = p - 1$, para todo $a \in \mathbb{Z} \setminus \{0, p^k : k \in \mathbb{N} \setminus \{0\}\}$ se tiene que $a^{p-1} \equiv 1 \pmod{p}$. Por tanto

$$\mathbb{Z}_p^* = \{ [1], [2], \dots, [p-1] \}$$

son todas las raíces del polinomio $x^{p-1} - 1$.

DIVISIBILIDAD EN $\mathbb{F}[x]$.

Como en el caso de los enteros, en el contexto de los polinomios existen los conceptos de divisibilidad entre polinomios, máximo común divisor, polinomio no divisible o **irreducible**,...etc. Veámoslo.

Definición 1. Sea $\mathbb{F}$ un cuerpo y sean $P, Q \in \mathbb{F}[x]$.

A: Se dice que $Q \neq 0$ **divide** a P (**notación:** $Q|P$) si existe $q \in \mathbb{F}[x]$ de modo que

$$P(x) = q(x)Q(x).$$

B: Se dice que el polinomio P es **irreducible** si para todo polinomio $Q \neq 0$ con $Q|P$ se tiene que o bien $\text{grad}.Q = 0$ (es decir $Q \in \mathbb{F}$) o bien $\text{grad}.Q = \text{grad}.P$

C: Se dice que $d \in \mathbb{F}[x]$ es un **máximo común divisor** de P y Q (**notación:** $d \in \text{m.c.d.}(P, Q)$) si d es un divisor común a P y Q (es decir $d|P$ y $d|Q$) y además el grado de d es máximo (es decir si $h|P$ y $h|Q$, entonces $\text{grad}.h \leq \text{grad}.d$).

Observación 2. **a:** Si $P \in \mathbb{F}[x]$ y $\alpha \in \mathbb{F}$, entonces existe un único $q \in \mathbb{F}[x]$ de forma que

$$P(x) = q(x)(x - \alpha) + \overline{P}(\alpha).$$

b: Si α es una raíz del polinomio P , entonces $x - \alpha | P(x)$.

Demostración: Por el Teorema del Resto, existen $q, r \in \mathbb{F}[x]$ únicos de modo que

$$P(x) = q(x)(x - \alpha) + r(x) \quad \text{de modo que} \quad 0 \leq \text{grad}.r(x) < \text{grad.}(x - \alpha) = 1.$$

Luego $r \in \mathbb{F}$ y además como α es raíz de $x - \alpha$, se tiene que $r = \overline{P}(\alpha)$.

Ejemplos 1. ■ $x - 1 | x^p - 1$ para todo $p > 1$.

■ $x^2 + 1 \in \mathbb{R}[x]$ es irreducible. Si no lo fuese

$$x^2 + 1 = (ax + b)\left(\frac{x}{a} + c\right) \quad \Rightarrow \quad -\frac{b}{a} \in \mathbb{R}$$

es una raíz del polinomio. Lo cuál sabemos que no es posible.

■ En $\mathbb{R}[x]$, $\text{m.c.d.}(x^2 + 1, (x^2 + 1)(x - 1)) = \{cx^2 + c : c \in \mathbb{R}\}$.

Observación 3. Si $P, Q \in \mathbb{F}[x]$, el $\text{m.c.d.}(P, Q)$ no es único. Si $d(x) \in \text{m.c.d.}(P, Q)$, entonces para $c \in \mathbb{F}$ se tiene que $cd(x) \in \text{m.c.d.}(P, Q)$. Veremos más adelante que existe un único $\text{m.c.d.}(P, Q)$ **mónico**.

Observación 4. Si $P \in \mathbb{F}[x]$ irreducible sobre $\mathbb{F}$, entonces existe $\alpha \in \mathbb{F}$ raíz del polinomio P si y solo si $\text{grad}.P = 1$.

Demostración: Si $\text{grad}.P = 1$, se tiene que $P(x) = ax + b$ con $a \neq 0$, y así $\alpha = -\frac{b}{a}$ es un raíz de P .

Por otro lado, si $\alpha \in \mathbb{F}$ es raíz de P , entonces $P(x) = (x - \alpha)q(x)$. Ahora como P es irreducible y $x - \alpha | P(x)$ se sigue de la definición de irreducibilidad que $1 = \text{grad.}(x - \alpha) = \text{grad}.P(x) \square$

Ejemplo 6. Consideramos $P(x) = x^5 + 3x^3 + x^2 + 2x \in \mathbb{Z}_5[x]$. ¿Cuáles son las raíces de P en $\mathbb{Z}_5$?

$P(x) = x^5 + 3x^3 + x^2 + 2x = x(x^4 + 3x^2 + x + 2)$. Así vemos que $\alpha = 0$ es un raíz.

Sea $Q(x) = (x^4 + 3x^2 + x + 2)$. Claramente las raíces de Q lo son de P . Vamos a buscar las raíces de Q . Usamos dos caminos.

- Si α es una raíz de Q entonces

$$Q(x) = (x - \alpha)(x^3 + ax^2 + bx^2 + cx + d)$$

luego al hacer este producto resulta que $\alpha \times d = 2$. Las raíces de Q se encuentran entre los divisores de 2 en $\mathbb{Z}_5$.

$\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Mirando la tabla de $(\mathbb{Z}_5^*, \times)$, vemos que los divisores de 2 en $\mathbb{Z}_5^*$ son todos los números posibles: 1, 2, 3 y 4. En este caso concreto, el estudio de los divisores del término independiente d no nos ahorra trabajo.

- Las posibles raíces de Q son 1, 2, 3 y 4. Probémoslas. Para ello tendremos en cuenta que para todo $a \in \mathbb{Z}_5^*$ se tiene que $a^4 \equiv 1 \pmod{5}$.

$$\begin{aligned} Q(1) &= 1 + 3 + 1 + 2 = 2 \neq 0 \\ Q(2) &= 1 + 2 + 2 + 2 = 2 \neq 0 \\ Q(3) &= 1 + 2 + 3 + 2 = 3 \neq 0 \\ Q(4) &= 1 + 3 + 4 + 2 = 0 \end{aligned}$$

Así $\alpha = 4$ es raíz de Q y por tanto de P . Además $x - 4 = x + 1$ divide a Q ,

$$\begin{array}{r} x^4 + 3x^2 + x + 2 \\ -x^4 - x^3 \\ \hline -x^3 + 3x^2 + x + 2 \\ x^3 + x^2 \\ \hline 4x^2 + x + 2 \\ x^2 + x \\ \hline 2x + 2 \\ 2x + 2 \\ \hline 0 \end{array} \quad \begin{array}{l} |x+1 \\ \hline x^3 - x^2 - x + 2 \end{array}$$

Así, $P(x) = x(x + 1)(x^3 - x^2 - x + 2)$. El polinomio $R(x) = x^3 - x^2 - x + 2$ **no** tiene por raíces a 1, 2 ni a 3, pues no lo son de Q . Por otro lado $R(4) = 4 - 1 - 4 + 2 = 1 \neq 0$, luego el 4 **no** es raíz **doble** de Q ni de P . Así las únicas raíces de P son el 0 y el 4 $\square$

REFERENCIAS

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