AMPLIACIÓN DE MATEMÁTICAS

RAÍCES MÚLTIPLES.

Dado un polinomio con coeficientes en un cuerpo ¿existirá siempre un elemento del cuerpo que anula el polinomio? ¿Siempre existe un cuerpo donde podamos encontrar raíces de un polinomio con coeficientes en otro cuerpo dado? ¿Cuántas veces puede ser un elemento del cuerpo raíz de un polinomio? Veamos unos cuantos ejemplos para situar las preguntas anteriores.

Ejemplos 1. 1. *Sea* $p(x) = x^2 + 1 \in \mathbb{Q}[x]$. ***No*** *existe* $\alpha \in \mathbb{Q}$ *de modo que* $\overline{p}(\alpha) = \alpha^2 + 1 = 0$.

Sea $p(x) = x^2 + 1 \in \mathbb{R}[x]$. ***No*** *existe* $\alpha \in \mathbb{R}$ *de modo que* $\overline{p}(\alpha) = \alpha^2 + 1 = 0$.

Sea $p(x) = x^2 + 1 \in \mathbb{C}[x]$. $i, -i \in \mathbb{C}$ *son raíces del polinomio y así* $x^2 + 1 = (x - i)(x + i)$.

Además, sabemos que

$$\mathbb{Q} \subsetneq \mathbb{R} \subsetneq \mathbb{C}.$$

2. *Consideremos ahora* $x^2 + x + 1 \in \mathbb{Z}_2[x]$. $\mathbb{Z}_2 = \{0, 1\}$. *Ni* 0 *ni* 1 *son raíces del polinomio. De tener este polinomio una raíz ¿la tendrá en un cuerpo* $\mathbb{F}$ *mayor que* $\mathbb{Z}_2$*? (*$\mathbb{Z}_2 \subsetneq \mathbb{F}$*, incluido como subcuerpo).*
3. *Sea* $x^4 + 2x + 1 \in \mathbb{R}[x]$.

$$x^4 + 2x + 1 = (x^2 + 1)^2 = (x - i)^2(x + i)^2.$$

El polinomio no tiene raíces en el cuerpo de los coeficientes $\mathbb{R}$*, las tiene en un cuerpo más grande* $\mathbb{C}$*. Además las raíces son múltiples, en el sentido de que aparecen más de una vez en la descomposición del polinomio.*

En el tema siguiente veremos que ésto es una propiedad general. Así veremos que

Dado un polinomio p con coeficientes en un cuerpo $\mathbb{F}$, siempre existe otro cuerpo $\mathbb{K}$, más grande que el primero, donde el polinomio tiene al menos una raíz.

Aquí lo que vamos a estudiar es determinar cuando un polinomio tiene una raíz **múltiple** sin importarnos donde está la raíz. Para empezar vamos a recordar como descomponer un polinomio si conocemos sus raíces.

Sabemos que si α es una raíz de un polinomio $p \in \mathbb{F}[x]$, entonces

$$p(x) = (x - \alpha)q(x)$$

donde $q(x)$ es otro polinomio de grado $grad.p - 1$, cuyos coeficientes estarán en $\mathbb{F}$ si $\alpha \in \mathbb{F}$ o en otro cuerpo mayor que $\mathbb{F}$ si $\alpha \notin \mathbb{F}$.

Proposición 1. *Sea $p(x) \in \mathbb{F}[x]$, un polinomio con coeficientes en un cuerpo. Si $grad.p = n$, entonces p tiene a lo más n raíces en $\mathbb{F}$.*

Demostración: Por inducción sobre el grado del polinomio.

Si $grad.p = 1$, entonces $p(x) = ax + b$ con $a, b \in \mathbb{F}$ y $a \neq 0$. Así p tiene una única raíz

$$a\alpha + b = 0 \qquad \Rightarrow \qquad \alpha = \frac{-b}{a}.$$

Si $grad.p = n - 1$, supongamos que p tiene a lo más $n - 1$ raíces sobre $\mathbb{F}$.

Si $grad.p = n$, si el polinomio no tiene raíces en $\mathbb{F}$ hemos terminado. Si al menos tiene una, $\alpha \in \mathbb{F}$ con $\overline{p}(\alpha) = 0$, entonces $p(x) = (x-\alpha)q(x)$ donde, sin más que dividir, $q \in \mathbb{F}[x]$. Ahora es claro que cualquier otra raíz de p perteneciente a $\mathbb{F}$ tiene que ser también raíz de q. Como $grad.q = n-1$, y por hipótesis de inducción q tiene a lo más $n-1$ raíz en $\mathbb{F}$, deducimos que p tiene a lo más n raíces en $\mathbb{F}$ □

Definición 1. *Un polinomio $p \in \mathbb{F}[x]$, de grado n, que tiene n raíces sobre sobre el cuerpo $\mathbb{F}$ se dice que p se descompone sobre $\mathbb{F}$.*

Observación 1. *Veremos que todo polinomio con coeficientes sobre un cuerpo, se puede descomponer sobre otro cuerpo mayor o igual al cuerpo de los coeficientes.*

Proposición 2. *Si un polinomio $p \in \mathbb{F}[x]$, con $grad.p = n$, se descompone sobre $\mathbb{F}$, entonces*

$$p(x) = a_n(x - \alpha_1)(x - \alpha_2).....(x - \alpha_n),$$

*donde $\alpha_1, \alpha_2, ..., \alpha_n \in \mathbb{F}$ son las raíces de p sobre $\mathbb{F}$. (**No** tienen por que ser distintas).*

Demostración: Sean $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ y $\alpha_1, \alpha_2, ..., \alpha_n \in \mathbb{F}$ las n raíces de p en $\mathbb{F}$. Así existe $q \in \mathbb{F}[x]$ mónico de modo que

$$p(x) = a_n(x - \alpha_1)q(x).$$

Ahora, usando inducción, es fácil ver que

$$q(x) = (x - \alpha_2).....(x - \alpha_n) \ \square$$

Ejemplo 1. *$x^3 + 2x^2 + x = x(x+1)^2 \in \mathbb{Q}[x]$, es un polinomoio que se descompone en el cuerpo $\mathbb{Q}$, y de modo que al menos una de las raíces se repite.*

Definición 2. *Un raíz α de un polinomio $p \in \mathbb{F}[x]$, se dice que es una raíz de **multiplicidad** $k \in \mathbb{N}$, si se puede escribir*

$$p(x) = (x - \alpha)^k q(x),$$

con $q \in \mathbb{F}[x]$ y $\overline{q}(\alpha) \neq 0$.

Vamos a determinar un procedimiento, para conocer a priori, sin calcularlas, cuando un polinomio p sobre un cuerpo $\mathbb{F}$ tiene raíces múltiples o no. Para éllo necesitamos la noción formal de derivada de un polinomio.

Definición 3. *Dado $p \in \mathbb{F}[x]$, $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, un polinomoo de grado n, se llama **derivada formal** de p al polinomio*

$$p'(x) = na_n x^{n-1} + ... + 2a_2 x + a_1.$$

Proposición 3. *Dados $P, Q \in \mathbb{F}[x]$, dos polinomios y $a \in \mathbb{F}$, se verifica que*

a: $(P + Q)' = P' + Q'$
b: $(aP)' = aP'$
c: $(PQ)' = P'Q + PQ'$.

Demostración: Para $\mathbb{F} = \mathbb{R}$, no son más que las reglas habituales de derivación. Para cualquier otro cuerpo $\mathbb{F}$, unas cuantas cuentas triviales (¡comprobar las igualdades anteriores!) nos convencen de que las igualdades son ciertas $\square$

Ejemplo 2. *Sea* $x^6 + 2x^3 + 1 \in \mathbb{Z}_3[x]$.

$$(x^6 + 2x^3 + 1)' = 6x^5 + 6x^2 \equiv 0.$$

Proposición 4. *Si* $p \in \mathbb{F}[x]$ *y* $p' = 0$, *entonces todas las raíces de* p *son múltiples.*

Demostración: Sea α una raíz de p, entonces

$$p(x) = (x - \alpha)q(x)$$

derivando

$$0 = p'(x) = q(x) + (x - \alpha)q'(x) \qquad \Rightarrow \qquad q(x) = (x - \alpha)(-q'(x)),$$

luego α es raíz también de q. Por tanto, α es al menos raíz doble de p,

$$p(x) = (x - \alpha)^2 h(x) \ \square$$

Teorema 1. *Sea* p *un polinomio de grado* n *sobre un cuerpo* $\mathbb{F}$, *de modo que* $p' \neq 0$. *Son equivalentes:*

a: *existe* α *una raíz múltiple de* p.
b: $x - \alpha$ *divide a* p *y a* p'.
c: $m.c.d.(p, p')$ *mónico tiene grado mayor o igual a uno.*

Demostración:

a $\Rightarrow$ **b :** Si α es una raíz múltiple podemos escribir

$$p(x) = (x - \alpha)^k q(x), \qquad \text{con} \qquad k \geq 2.$$

Derivando,

$$p'(x) = ((x - \alpha)^k)' q(x) + (x - \alpha)^k q'(x)$$

(es fácil ver por inducción que $((x - \alpha)^k)' = k(x - \alpha)^{k-1}$)

$$= k(x-\alpha)^{k-1} q(x) + (x-\alpha)^k q'(x) = (x-\alpha)\left(k(x - \alpha)^{k-2} q(x) + (x - \alpha)^{k-1} q'(x)\right).$$

De lo que se deduce que $(x - \alpha)|p$ y que $(x - \alpha)|p'$.

b $\Rightarrow$ **c:** Es evidente que si $(x - \alpha)|p$ y que $(x - \alpha)|p'$, entonces

$$grad.(x - \alpha) = 1 \leq grad.(m.c.d.(p, p'),$$

por definición de máximo común divisor.
(Observemos que este resultado es independiente de que la raíz esté en el cuerpo de coeficientes o en otro mayor).

c $\Rightarrow$ a: Sea $d = m.c.d.(p, p')$ mónico con $grad.d \geq 1$. Si tomamos α una raíz de d (que estará en $\mathbb{F}$ o en otro cuerpo más grande), entonces $d(x) = (x - \alpha)r(x)$. Ahora como d divide a p y p' tenemos que

$$p(x) = d(x)q_1(x) = (x - \alpha)r(x)q_1(x)$$

y

$$p'(x) = d(x)q_2(x) = (x - \alpha)r(x)q_2(x).$$

Por tanto $\overline{p}(\alpha) = 0$ y $\overline{p'}(\alpha) = 0$. Consideremos ahora la descomposición de p

$$p(x) = a_n(x - \alpha)^{r_1}(x - \alpha_2)^{r_2}.....(x - \alpha_k)^{r_k},$$

donde $\alpha, \alpha_2, ..., \alpha_k$ son todas las raíces de p **distintas** (quizás en un cuerpo mayor que $\mathbb{F}$). **Si** suponemos que $r_1 = 1$, derivando

$$p'(x) = a_n \left[(x - \alpha_2)^{r_2}.....(x - \alpha_k)^{r_k} + (x - \alpha)\left((x - \alpha_2)^{r_2}.....(x - \alpha_k)^{r_k}\right)'\right].$$

De lo que se sigue que

$$\overline{p'}(\alpha) = a_n(\alpha - \alpha_2)^{r_2}.....(\alpha - \alpha_k)^{r_k} \neq 0.$$

Lo que nos lleva a contradicción. Por tanto $r_1 > 1$ y así α es una raíz múltiple $\square$

Observación 2. *De la prueba anterior se ve que si α es una raíz de $m.c.d.(p, p')$, entonces α es raíz tanto de p como de p'.*

Ejemplo 3. *Veamos si $p(x) = x^3 + x + 1 \in \mathbb{Z}_3[x]$ tiene raíces múltiples.*

Derivando $p'(x) = 3x^2 + 1 = 1$, por tanto $m.c.d.(x^3 + x + 1, 1) = 1$. Luego por el teorema anterior el polinomio no tiene raíces múltiples.

Observemos que $\alpha = 1$ es una raíz del polinomio y por tanto

$$p(x) = (x - 1)(x^2 + x + 2)$$

donde $x^2 + x + 2$ no tiene raíces en $\mathbb{Z}_3$ $\square$

Ejemplo 4. *Veamos si $p(x) = x^3 + x + 1 \in \mathbb{Z}_5[x]$ tiene raíces múltiples.*

Derivando $p'(x) = 3x^2 + 1$. Ahora usando el algoritmo de Euclides

$$\begin{array}{rl} x^3+x+1 & |\underline{3x^2+1} \\ \underline{-x^3-2x} & 2x \\ 4x+1 & \end{array} \qquad \text{y} \qquad \begin{array}{rl} 3x^2 \quad +1 & |\underline{4x+1} \\ \underline{-3x^2-2x} & 2x+2 \\ 3x+1 & \\ \underline{-3x-2} & \\ 4 & \end{array}$$

luego $m.c.d.(x^3+x+1, 3x^2+1) = 4$. Así el polinomio no tiene raíces múltiples $\square$

Proposición 5. *Sea $p \in \mathbb{F}[x]$ irreducible (es decir que no es divisible en $\mathbb{F}[x]$). El polinomio p tiene todas sus raíces distintas si y solo si $p' \neq 0$. (Entendiendo que estas raíces estarán en un cuerpo mayor que $\mathbb{F}$).*

Demostración: Hemos visto que si

$$p' = 0 \qquad \Rightarrow \qquad \text{todas las raíces de } \ p \text{ son múltiples.}$$

Si $p'(x) \neq 0$, entonces $m.c.d.(p, p') = 1$, ya que p es irreducible y así por el teorema anterior p no tiene raíces múltiples $\square$

Es chocante ver que la derivada de un polinomio de grado mayor o igual a 1 es nula. Veamos cuando puede ocurrir esta situación.

Observación 3. *Si la característica de un cuerpo es nula, $Char.\mathbb{F} = 0$, entonces para todo $p \in \mathbb{F}[x]$ con $grad.p \geq 1$ se tiene que $p'(x) \neq 0$.*

Demostración: Sea $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ y supongamos que su derivada es nula

$$p'(x) = na_n x^{n-1} + ... = 0.$$

Así $na_n = 0$ con $a_n \neq 0$. Por ser $\mathbb{F}$ un cuerpo y no tener divisores de cero implica que $n \equiv 0$. Si r es un primo que devide a $n \in \mathbb{N}$ se tiene que también $r \equiv 0$, luego $Char.\mathbb{F} = r$. Esto no puede ocurrir pués nuestro cuerpo es de característica 0 $\square$

Los cuerpos a los que estamos más acostumbrados $\mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$ tienen característica nula y por tanto no se anulan las derivadas de los polinomios, que era lo habitual hasta ahora.

En cambio en los cuerpos de característica no nula, $\mathbb{Z}_p$, p primo, por ejemplo, ya hemos visto que si puede haber derivadas de polinomios nulas. En general tenemos que

Observación 4. *Si $\mathbb{F}$ es un cuerpo finito y $q \in \mathbb{F}[x]$ con $q'(x) = 0$, entonces existe $r(x) \in \mathbb{F}[x]$ de modo que*

$$q(x) = (r(x))^{Char.\mathbb{F}}.$$

En este caso todas las raíces de q son múltiples.

Demostración: **La demostración usa Teoría de Cuerpos Finitos** que veremos en el próximo tema. De hecho, se sale un poco de nuestros objetivos. Veamos la prueba como un **apéndice.**

Si $\mathbb{F}$ es un cuerpo finito su cardinal es $Card.\mathbb{F} = p^k$, donde $p = Char.\mathbb{F}$, por tanto es un número primo, y $k \in \mathbb{N}$ (ver el tema siguiente).

Además, salvo isomorfismo, $\mathbb{F}$ es el conjunto de todas las raíces del polinomio $x^{p^k} - x \in \mathbb{F}[x]$ (ver el tema siguiente). Lo que quiere decir que para todo $\alpha \in \mathbb{F}$ se tiene que $\alpha^{p^k} - \alpha = 0$. Así

$$0 = (\alpha^{p^{k-1}})^p - \alpha \qquad \Rightarrow \qquad \sqrt[p]{\alpha} = \alpha^{p^{k-1}}.$$

Definición: *Un cuerpo $\mathbb{K}$ se llama **perfecto** si para todo $\alpha \in \mathbb{F}$ existe $\sqrt[Char.\mathbb{K}]{\alpha}$.*

Lo que acabamos de probar más arriba es que *todo cuerpo finito es perfecto.* Ahora podemos seguir con nuestra prueba.

Si $pq(x) = a_0 + \sum_{j=1}^{N} a_{n_j} x^{n_j} \in \mathbb{F}[x]$, con $a_{n_N} \neq 0$, entonces si su derivada es nula

$$0 = q'(x) = \sum_{j=1}^{N} n_j a_{n_j} x^{n_j - 1}.$$

Ésto quiere decir que $n_j a_{n_j} = 0$, y como no hay divisores de cero, necesariamente $n_j = 0$ para cada $j = 1, 2, ..., N$. Por la definición de característica de un cuerpo, se tiene que $p | n_j$ para cada $j = 1, 2, ..., N$. Como por otro lado existen las raíces $p-$ésimas de todo elemento del cuerpo perfecto $\mathbb{F}$ podemos escribir

$$q(x) = a_0 + \sum_{j=1}^{N} a_{n_j} x^{pk_j} = \left(\sqrt[p]{a_0} + \sum_{j=1}^{N} \sqrt[p]{a_{n_j}} x^{k_j} \right)^p = (r(x))^p$$

donde hemos usado la igualdad $(a+b)^p = a^p + b^p$ en un cuerpo $\mathbb{F}$ de característica p.

Es claro que $r(x) \in \mathbb{F}[x]$ y que las raíces de q y r son las mismas, por tanto las raíces de q son todas múltiples $\square$

Referencias

Departamento de Análisis Matemático, Facultad de Matemáticas, Universidad Complutense, 28040 Madrid, Spain
E-mail address: Cesar_Ruiz@mat.ucm.es