Polinomios separables y campos finitos

Facultad de Ciencias UNAM

Introducción

En esta sección introducimos y estudiamos (un poquito) las implicaciones de que un polinomio tenga (o no tenga) raíces múltiples. En el proceso demostraremos que el polinomio

$$x^{p^n} - x \in \mathbb{F}_p[x] \qquad \text{con } p \in \mathbb{Z}_{\geq 1} \text{ primo y } n \in \mathbb{Z}_{\geq 1}$$

tiene p^n raíces distintas. Luego, usaremos esto para demostrar la existencia y unicidad de campos finitos de cardinalidad p^n.

Un recordatorio amistoso

Supongamos que K/F es una extensión de campos y que $f(x) \in F[x]$. Si $f(x)$ se descompone en K/F, entonces el lector podrá fácilmente verificar que podemos escribir (de manera única, salvo por el orden de los factores)

$$f(x) = c \cdot (x - \alpha_1)^{n_1}(x - \alpha_2)^{n_2} \cdots (x - \alpha_k)^{n_k}$$

con $n_i \in \mathbb{Z}_{\geq 1}$, $c \in F$, $\alpha_1, \ldots, \alpha_k \in K$, y $\alpha_i \neq \alpha_j$ cuando $i \neq j$.

Recuerda que α_i es una **raíz múltiple de** $f(x)$ si $n_i > 1$ y en el caso que $n_i = 1$, decimos que α_i es una **raíz simple de** $f(x)$. Al entero n_i lo llamamos **la multiplicidad de** α_i.

Finalmente, recuerda que si $p \in \mathbb{Z}_{\geq 1}$ es primo, denotamos

$$\mathbb{F}_p := \mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}.$$

Polinomios separables

Definición

Supongamos que F es un campo, que $f(x) \in F[x]$, y que K/F es una extensión que contiene todas las raíces de $f(x)$. Decimos que $f(x)$ es **separable** si no tiene raíces múltiples en K.

Equivalentemente, si $\deg f(x) = n$, entonces $f(x)$ es separable si $f(x)$ tiene n raíces distintas en K.

Naturalmente, si $f(x)$ tiene raíces múltiples en K, decimos que $f(x)$ es **inseparable**.

Notemos que por vacuidad todo polinomio constante es inseparable. Por eso, por el resto de esta sección nos interesaremos en polinomios con grado ≥ 1.

Observación

Veamos que la definición anterior no depende del campo que contenga las raíces de $f(x)$.

Supongamos que K/F y K'/F son extensiones en donde $f(x)$ se descompone. En la proposición 2.9.2 vimos que los subcampos generados en K y K' respectivamente por las raíces de $f(x)$ (en K y K' respectivamente) son campos de descomposición de $f(x)$ sobre F.

Mas aun, en el teorema de unicidad de los campos de descomposición vimos que para cualesquiera dos campos de descomposición de $f(x)$ sobre F existe un isomorfismo que es biyectivo en las raíces de $f(x)$. En este caso, denotémoslo $\sigma : K \to K'$. Por lo tanto, si

$$f(x) = c \cdot (x - \alpha_1)^{n_1}(x - \alpha_2)^{n_2} \cdots (x - \alpha_k)^{n_k} \in K[x]$$

donde $n_i \in \mathbb{Z}_{\geq 1}$, $c, \alpha_1, \ldots, \alpha_k \in K$, y $\alpha_i \neq \alpha_j$ cuando $i \neq j$, entonces

$$f(x) = \sigma(c) \cdot (x - \sigma(\alpha_1))^{n_1}(x - \sigma(\alpha_2))^{n_2} \cdots (x - \sigma(\alpha_k))^{n_k} \in K'[x].$$

En particular, $f(x)$ no tiene raíces múltiples en K si y solo si $f(x)$ no tiene raíces múltiples en K'.

Ejemplos sencillos de polinomios separables/inseparables

- El polinomio $x^2 - 2 \in \mathbb{Q}[x]$ es separable porque sus raíces son $\pm\sqrt{2}$.
- En contraste, el polinomio $(x^2 - 2)^n \in \mathbb{Q}[x]$ es inseparable porque $\pm\sqrt{2}$ son raíces con multiplicidad n.

En lo que sigue, presentaremos una caracterización de separabilidad. Es curioso que para esto resulta muy útil el concepto de derivada de un polinomio. Por supuesto estarás familiarizado con este concepto para funciones de $\mathbb{R}$ en $\mathbb{R}$. También, recordaras que para calcular la derivada de un polinomio de $\mathbb{R}$ en $\mathbb{R}$ hay una formula muy sencilla que produce otro polinomio de $\mathbb{R}$ en $\mathbb{R}$. En la siguiente diapositiva usamos esta formula para generalizar el concepto de derivada de un polinomio a cualquier campo.

La derivada de un polinomio

Definición

Supongamos que F es un campo y que

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \in F[x].$$

Definimos **la derivada de** $f(x)$ como el siguiente polinomio

$$D_x f(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + 2 a_2 x + a_1 \in F[x].$$

$\mathrm{ch}(F) = 0 \iff \deg D_x f(x) = \deg(f(x)) - 1$ para todo $f(x) \neq 0$

Proposición 1

Si F es un campo, entonces $\mathrm{ch}(F) = 0$ si y solo si $\deg D_x f(x) = \deg(f(x)) - 1$ para todo $f(x) \in F[x]$ distinto de 0.

Demostración.

$\Longrightarrow$) El caso en que $\deg f(x) = 0$ o equivalentemente, $f(x)$ es un polinomio constante no cero, tenemos $D_x f(x) = 0$ y por lo tanto, como $\deg 0 = -1$ (por definición), obtenemos lo deseado.

Por lo tanto, supongamos que $n = \deg f(x) \geq 1$ y que

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0.$$

Por definición,

$$D_x f(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + 2a_2 x + a_1.$$

Como $a_n \neq 0$ (pues $\deg f(x) = n$), entonces $\mathrm{ch}(F) = 0$ implica $n a_n \neq 0$. Por lo tanto, $\deg D_x f(x) = \deg(f(x)) - 1$.

$\Longleftarrow$) Procedemos por contrapositiva. Supongamos que $p = \mathrm{ch}(F) \neq 0$. Considera $f(x) \coloneqq x^p$. Entonces

$$D_x f(x) = p x^{p-1} = 0 x^{p-1} = 0$$

y por lo tanto, $\deg D_x f(x) = \deg 0 = -1 \neq \deg(f(x)) - 1$.

La derivada de la suma y del producto

Proposición 2

Supongamos que F es un campo. Si $f(x), g(x) \in F[x]$ entonces

$$D_x\left(f(x)+g(x)\right) = D_x(f(x)) + D_x(g(x)) \quad \text{y}$$
$$D_x\left(f(x)\cdot g(x)\right) = D_x(f(x))\cdot g(x) + f(x)\cdot D_x(g(x)).$$

La demostración es muy sencilla y por eso se la dejamos al lector. Cabe recalcar que estas formulas se pueden demostrar directamente de la definición de derivada de un polinomio y no requieren ningún tipo de técnica involucrando limites o continuidad.

Un polinomio es inseparable si y solo si comparte una raíz con su derivada

Proposición 3

Supongamos que F es un campo. Si $f(x) \in F[x]$ tiene grado ≥ 1, entonces

$$\alpha \text{ es raíz múltiple de } f(x) \iff \alpha \text{ es raíz de } f(x) \text{ y de } D_x f(x).$$

En particular,

$$f(x) \text{ es inseparable} \iff f(x) \text{ y } D_x f(x) \text{ tienen una raíz común.}$$

Demostración.

$\Longrightarrow$) Supongamos que α es una raíz múltiple de $f(x)$. Entonces (por definición) existe un campo de descomposición K de $f(x)$ sobre F en donde

$$f(x) = (x-\alpha)^n g(x), \qquad \text{con } \ n \geq 2 \ \text{ y } \ g(x) \in K[x].$$

Calculando la derivada obtenemos

$$\begin{aligned} D_x f(x) &= D_x\left((x-\alpha)^n g(x)\right) \\ &= D_x\left((x-\alpha)^n\right) \cdot g(x) + (x-\alpha)^n \cdot D_x g(x) \\ &= n(x-\alpha)^{n-1} \cdot g(x) + (x-\alpha)^n \cdot D_x g(x) \end{aligned}$$

Ahora bien, como $n \geq 2$, entonces α es raíz de $(x-\alpha)^{n-1}$. Por lo tanto, evaluando α en la ecuación anterior obtenemos lo deseado.

$\Longleftarrow$) Supongamos que α es raíz de $f(x)$ y de $D_x f(x)$. Entonces existe un campo de descomposición L de $f(x)$ sobre F en donde

$$f(x) = (x - \alpha)h(x), \qquad \text{con } \ h(x) \in L[x]. \tag{1}$$

Calculando la derivada obtenemos

$$D_x(f(x)) = D_x\left(x - \alpha\right)h(x) + (x - \alpha)D_x h(x) = h(x) + (x - \alpha)h(x).$$

Luego, evaluando en α obtenemos

$$0 = D_x f(\alpha) = h(\alpha) + (\alpha - \alpha)D_x h(x) = h(\alpha)$$

donde la primera igualdad se da porque (por hipótesis) α es raíz de $D_x f(x)$. Por lo tanto, α es raíz de $h(x)$ en L. Entonces

$$h(x) = (x - \alpha)h_1(x), \text{ para algún } h_1(x) \in L[x].$$

Sustituyendo esta ecuación en (1) obtenemos

$$f(x) = (x - \alpha)\left((x - \alpha)h_1(x)\right) = (x - \alpha)^2 h_1(x)$$

y por lo tanto α es una raíz múltiple de $f(x)$. $\square$

Aplicaciones de la proposición anterior

- Supongamos que F es un campo tal que $\mathrm{ch}(F) \nmid n$. Entonces el polinomio $x^n - 1 \in F[x]$ es separable:

  Calculando su derivada obtenemos

  $$D_x\left(x^n - 1\right) = nx^{n-1}.$$

  Como $\mathrm{ch}(F) \nmid n$, entonces $D_x\left(x^n - 1\right) \neq 0$ y por lo tanto la única raíz de $D_x\left(x^n - 1\right)$ es 0. En particular, $x^n - 1$ y $D_x\left(x^n - 1\right)$ no comparten raíces y por lo tanto $x^n - 1$ es separable.

  Una consecuencia inmediata de este resultado es que para cualquier campo F con $\mathrm{ch}(F) \nmid n$, hay n distintas n-esimas raíces de la unidad en F.
- Conversamente, si F es un campo tal que $\mathrm{ch}(F)|n$, entonces hay menos de n distintas raíces de la unidad en F:

  En este caso, la derivada de $x^n - 1$ es idénticamente 0 y por lo tanto $x^n - 1$ es inseparable. Equivalentemente, $x^n - 1$ tiene menos de n distintas raíces.

- Supongamos que $p \in \mathbb{Z}_{\geq 1}$ es primo y que $n \in \mathbb{Z}_{\geq 1}$. Entonces el polinomio $x^{p^n} - x \in \mathbb{F}_p[x]$ es separable:

  Calculando su derivada obtenemos

  $$D_x(x^{p^n} - x) = p^n x^{p^n - 1} - 1 = 0 x^{p^n - 1} - 1 = -1$$

  donde la penúltima igualdad se cumple porque $p = 0$ en $\mathbb{F}_p$.

  En particular, $x^{p^n} - x$ y $D_x(x^{p^n} - x)$ no tienen raíces en común y por lo tanto $x^{p^n} - x$ es separable.

En lo que sigue, interrumpimos nuestro estudio de polinomios separables para dar una caracterización de los campos finitos. Afortunadamente, en el camino obtendremos resultados que luego serán útiles para el estudio de polinomios separables.

Comentario

Para empezar, notemos que cualquier campo finito tiene característica distinta de 0. Por lo tanto, tiene sentido estudiar a los campos con característica distinta de 0. Para esto, recordemos el teorema del binomio (el cual se satisface sobre cualquier anillo conmutativo y se puede demostrar por inducción sobre n):

Supongamos que R es un anillo conmutativo y que $n \in \mathbb{Z}_{\geq 1}$. Si $a, b \in R$, entonces

$$(a+b)^n = a^n + \binom{n}{1} a^{n-1}b + \cdots + \binom{n}{n-1} ab^{n-1} + b^n,$$

donde

$$\binom{n}{k} := \frac{n!}{k!(n-k)!} \in \mathbb{Z}_{\geq 0}, \quad 1 \leq k \leq n-1.$$

Consideremos el caso $n = p$ con p primo. Por definición, para toda $k \in \{1, \ldots, p-1\}$

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p(p-1)\cdots(k+1)k}{(p-k)!}.$$

Ahora bien, como p es primo, entonces (por el teorema fundamental de la aritmética) ninguna combinación de los factores que aparecen en $(p-k)!$ es igual a p y por lo tanto, el factor p en el numerador no se cancela. En particular,

$$p \text{ divide a } \binom{p}{k} \text{ para toda } k \in \{1, \ldots, p-1\}.$$

Con esto en mente, empecemos a estudiar a los campos con característica $p \neq 0$.

$$\mathrm{ch}(F) = p \neq 0 \implies (a+b)^p = a^p + b^p \text{ y } (ab)^p = a^p\, b^p$$

Proposición 4

Supongamos que F es un campo con $\mathrm{ch}(F) = p \neq 0$. Si $a, b \in F$, entonces

$$(a+b)^p = a^p + b^p \quad \text{y} \quad (ab)^p = a^p\, b^p.$$

Demostración. La igualdad $(ab)^p = a^p b^p$ es consecuencia inmediata de que F es un anillo conmutativo. Veamos la otra igualdad. Por el teorema del binomio,

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1} b + \cdots + \binom{p}{p-1} a b^{p-1} + b^p$$

Ahora bien, como p es primo[1], en el comentario anterior vimos que p divide a $\binom{p}{k}$ para toda $k \in \{1, \ldots, p-1\}$. Por lo tanto, $\binom{p}{k} = 0$ en F. Sustituyendo esto en la ecuación anterior, obtenemos lo deseado. □

[1] Recuerda que la característica de un anillo siempre es un numero primo.

El endomorfismo de Frobenius

Definición

Supongamos que F es un campo con $\mathrm{ch}(F) = p \neq 0$. Definimos el **endomorfismo de Frobenius** por

$$\begin{aligned} \varphi : F &\to F \\ a &\mapsto a^p. \end{aligned}$$

Claramente, la proposición anterior implica que φ es un homomorfismo. La verificación de que es un endomorfismo (es decir, que es un homomorfismo inyectivo) es trivial y se la dejamos al lector.

Una generalización de la proposición anterior

Proposición 5

Supongamos que F es un campo con $\mathrm{ch}(F) = p \neq 0$ y que $n \in \mathbb{Z}_{\geq 0}$. Si $a, b \in F$, entonces

$$(a+b)^{p^n} = a^{p^n} + b^{p^n} \quad \text{y} \quad (ab)^{p^n} = a^{p^n}\, b^{p^n} \text{ para toda } a, b \in \mathbb{F}.$$

Demostración. Para la igualdad $(ab)^{p^n} = a^{p^n}\, b^{p^n}$ no hay nada que probar[2]. Para la otra igualdad, procedamos por inducción sobre n. El paso base $n = 1$ es simplemente la proposición anterior.

[2] Es consecuencia inmediata de la conmutatividad multiplicativa.

Para el paso inductivo, supongamos que $n > 1$ y que

$$(\alpha + \beta)^{p^{n-1}} = \alpha^{p^n} + \beta^{p^{n-1}}.$$

para toda $\alpha, \beta \in F$. Entonces,

$$\begin{aligned}
(a+b)^{p^n} = (a+b)^{p \cdot p^{n-1}} &= \left((a+b)^p\right)^{p^{n-1}} \\
&= (a^p + b^p)^{p^{n-1}} && \text{(por el paso base)} \\
&= (a^p)^{p^{n-1}} + (b^p)^{p^{n-1}} && \text{(por hipótesis de inducción)} \\
&= a^{p^n} + b^{p^n}.
\end{aligned}$$

□

Lema 6

Supongamos que $p \in \mathbb{Z}_{\geq 0}$ es primo y que $F/\mathbb{F}_p$ es una extensión de campos. Entonces $[F : \mathbb{F}_p] = n$ si y solo si $|F| = p^n$.

Demostración.

$\Longrightarrow$) Supongamos que $[F : \mathbb{F}_p] = n$. Por definición, existen $\{v_1, \ldots, v_n\}$ una $\mathbb{F}_p$-base de F. Es decir, para todo elemento $a \in F$ existen únicos $a_1, \ldots, a_n \in \mathbb{F}_p$ tales que $a = a_1 v_1 + \cdots + a_n v_n$. La existencia y unicidad de esta combinación lineal implican que F es biyectable con el conjunto de las n-adas en $\mathbb{F}_p$, $\{(a_1, \ldots, a_n) \mid a_1, \ldots, a_n \in \mathbb{F}_p\}$. Por un argumento de combinatoria, este conjunto tiene cardinalidad $|\mathbb{F}_p|^n = p^n$ y por lo tanto obtenemos lo deseado.

$\Longleftarrow$) Procedamos por contradicción. Es decir, supongamos que $|F| = p^n$ y que $[F : \mathbb{F}_p] = m$ con $m \neq n$. Por "$\Longrightarrow$", esto implica que $|F| = p^m$, contradiciendo $|F| = p^n$.

□

Existencia de campos finitos con cardinalidad p^n

Proposición 7

Supongamos que $p \in \mathbb{Z}_{\geq 0}$ primo y que $n \in \mathbb{Z}_{\geq 0}$. Si $\mathbb{F}$ es el campo de descomposición de $x^{p^n} - x \in \mathbb{F}_p[x]$, entonces $|\mathbb{F}| = p^n$ y $[\mathbb{F} : \mathbb{F}_p] = n$.

En particular, para todo $p \in \mathbb{Z}_{\geq 0}$ primo y $n \in \mathbb{Z}_{\geq 0}$, existe un campo de cardinalidad p^n.

Demostración. Sea

$$E = \{\alpha \in \mathbb{F} \mid \alpha \text{ es raíz de } x^{p^n} - x \in \mathbb{F}_p[x]\}.$$

Notemos que $\mathbb{F}_p \subset E$ (pues $\alpha^{p-1} = 1$ para toda $\alpha \in \mathbb{F}_p$) y veamos que E es un campo. Para esto, primero recordemos que la característica de un anillo es invariante bajo extensiones (c.f. proposición 2.1.3) y por lo tanto, $\text{ch}(\mathbb{F}) = \text{ch}(\mathbb{F}_p) = p$. En particular (por la proposición anterior), tenemos que

$$(a+b)^{p^n} = a^{p^n} + b^{p^n} \quad \text{y} \quad (ab)^{p^n} = a^{p^n} b^{p^n} \text{ para toda } a, b \in \mathbb{F}.$$

Usando esto es fácil verificar que E es cerrado bajo suma y multiplicación.

Mas aun, si α es raíz de $x^{p^n} - x$, entonces $\alpha^{p^n} = \alpha$ y por lo tanto,

$$\alpha^{-1} = \left(\alpha^{p^n}\right)^{-1} = \left(\alpha^{-1}\right)^{p^n}.$$

Donde la ultima igualdad se puede verificar directamente por la definición de inverso multiplicativo. Claramente, esto implica que α^{-1} también es raíz de $x^{p^n} - x$ y entonces E es cerrado bajo división. Por lo tanto, E es un campo.

Juntando todo lo anterior tenemos que E es un campo tal que $\mathbb{F}_p \subset E \subset \mathbb{F}$ en donde $x^{p^n} - x$ se descompone[3] Como $\mathbb{F}$ es campo de descomposición de $x^{p^n} - x$, lo anterior implica que $E = \mathbb{F}$.

Por otro lado, recordemos que en ya vimos que $x^{p^n} - x \in \mathbb{F}_p[x]$ es separable y por lo tanto, hay p^n distintas raíces de $x^{p^n} - x$ en $\mathbb{F}$. En particular,

$$p^n = |E| = |\mathbb{F}|$$

y por el lema anterior también tenemos que

$$[\mathbb{F} : \mathbb{F}_p] = n.$$

□

[3]Esto es consecuencia inmediata de la definición de E.

Unicidad de los campos finitos con cardinalidad p^n

Proposición 8

Si $p \in \mathbb{Z}_{\geq 0}$ es primo, $n \in \mathbb{Z}_{\geq 0}$, y F es un campo con $|F| = p^n$, entonces F contiene a un subcampo isomorfo a $\mathbb{F}_p$ (esto nos permite tratar a F como a una extensión de $\mathbb{F}_p$) y F es el campo de descomposición de $x^{p^n} - x \in \mathbb{F}_p[x]$ sobre $\mathbb{F}_p$.

En particular, cualesquiera dos campos con cardinalidad p^n son isomorfos.

Demostración. Supongamos que F es un campo con $|F| = p^n$. Como (i) la característica de un anillo finito siempre divide a la cardinalidad del anillo (c.f. proposición 2.1.6) y (ii) la característica de un anillo finito siempre es un numero primo, entonces $\mathrm{ch}(F) = p$. En la proposición 2.1.4 vimos que esto implica que $\mathbb{F}_p$ es isomorfo al siguiente subconjunto de F

$$\{n \cdot 1_F \mid n \in \mathbb{Z}\} \subset F.$$

En lo que sigue tratamos a $\mathbb{F}_p$ como si fuese igual a este subconjunto de F.

Ahora bien, si $F^\times$ es el grupo multiplicativo de F, entonces $|F^\times| = p^n - 1$. Por lo tanto, (por teoría de grupos básica)

$$\alpha^{p^n-1} = 1 \text{ para toda } \alpha \in F^\times.$$

Multiplicando por α y observando que esta ecuación también se satisface para $\alpha = 0$, obtenemos que $\alpha^{p^n} = \alpha$ para toda $\alpha \in F$. En otras palabras, todo elemento de F es raíz de $x^{p^n} - x$ y por lo tanto,

$$\prod_{\alpha \in F} (x - \alpha) \text{ divide a } x^{p^n} - x. \tag{2}$$

Por otro lado, como $|F| = p^n$, entonces

$$\deg\left(\prod_{\alpha \in F} (x - \alpha)\right) = p^n = \deg\left(x^{p^n} - x\right) \tag{3}$$

Juntando (2) y (3) obtenemos $x^{p^n} - x = \prod_{\alpha \in F}(x - \alpha)$. Es fácil verificar que esto implica que F es el campo de descomposición de $x^{p^n} - x$ sobre $\mathbb{F}_p$. $\square$

Definición

Supongamos que $p \in \mathbb{Z}_{\geq 0}$ es primo. Denotamos por $\mathbb{F}_{p^n}$ al único campo (salvo isomorfismo) con cardinalidad p^n.

Usando el lema 6, es fácil verificar que una definición alternativa de $\mathbb{F}_{p^n}$ es como la única extensión de $\mathbb{F}$ (salvo isomorfismo) tal que $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$.

Finalmente, estamos listos para presentar nuestra caracterización de los campos finitos.

Todo campo finito es isomorfo a algún $\mathbb{F}_{p^n}$

Corolario 9

Supongamos que F es un campo finito. Entonces

1. $\mathrm{ch}(F) = p$ para algún $p \in \mathbb{Z}_{\geq 0}$ primo.
2. $\mathbb{F}_p$ es isomorfo a un subcampo de F (esto nos permite tratar a F como a una extensión de $\mathbb{F}_p$).
3. Si denotamos $n = [F : \mathbb{F}_p]$, entonces $|F| = p^n$.
4. $F \cong \mathbb{F}_{p^n}$ y F es el campo de descomposición de $x^{p^n} - x$ sobre $\mathbb{F}_p$.

Demostración.

1. Recuerda (i) que todo campo tiene característica 0 o característica prima y (ii) que si un campo tiene característica 0, entonces es infinito.
2. Por el inciso anterior y la proposición 2.1.4, $\mathbb{F}_p \cong \{n \cdot 1_F \mid n \in \mathbb{Z}\} \subset F$.
3. Es consecuencia inmediata del lema 6.
4. Es consecuencia inmediata del inciso anterior y la proposición 8.

□