Un poquito mas acerca de polinomios separables

Facultad de Ciencias UNAM

Introducción

En la sección anterior interrumpimos nuestro estudio de polinomios separables para demostrar la existencia y unicidad de campos finitos con cardinalidad p^n. En esta sección regresemos a nuestro estudio de polinomios separables.

Recordemos que en la proposición 2.13.3 demostramos que para cualquier campo F y cualquier polinomio $f(x) \in F[x]$ con grado ≥ 1 tenemos

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

En lo que sigue, usaremos esto para caracterizar el concepto de separabilidad en términos del concepto de polinomios primos relativos.

Para esto, recordemos que en el corolario 1.24.4 vimos que una de las consecuencias del algoritmo de la división para polinomios con coeficientes en un campo es el siguiente resultado.

> *Supongamos que K/F es una extensión de campos. Si $f(x), g(x) \in F[x]$, entonces el máximo común divisor de $f(x)$ y $g(x)$ en $F[x]$ coincide con el máximo común divisor de $f(x)$ y $g(x)$ en $E[x]$.*

En particular,

$$f(x) \text{ y } g(x) \text{ son primos relativos en } F[x] \iff$$
$$f(x) \text{ y } g(x) \text{ son primos relativos en } K[x].$$

Con esto en mente, procedamos a la caracterización de separabilidad en términos del concepto de polinomios primos relativos.

$f(x)$ es separable $\iff \big(f(x), D_x f(x)\big) = 1$

Proposición 1

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

$$f(x) \text{ es separable} \iff f(x) \text{ y } D_x f(x) \text{ son primos relativos en } F[x].$$

Demostración. Es fácil verificar que para todo campo E, dos polinomios son primos relativos en $E[x]$ si y solo si no tienen ninguna raíz común en E. Usando esto y la proposición 2.13.3 obtenemos que si K es un campo que contiene todas las raíces de $f(x)$, entonces

$$f(x) \text{ es separable} \iff f(x) \text{ y } D_x f(x) \text{ son primos relativos en } K[x].$$

Usando esto y el recordatorio de la diapositiva anterior, obtenemos lo deseado. □

$D_x f(x) = 0 \implies f(x)$ inseparable

Corolario 2

Supongamos que F es un campo y que $f(x) \in F[x]$ tiene grado ≥ 1. Si $D_x f(x) = 0$, entonces $f(x)$ es inseparable.

Demostración. Si $D_x f(x) = 0$, entonces claramente $f(x)$ y $D_x f(x)$ *no* son primos relativos (en este caso $f(x)$ es un mcd de $f(x)$ y $D_x f(x) = 0$). En particular, por la proposición anterior, obtenemos lo deseado. □

En la siguiente proposición vemos que en el caso que $f(x)$ es irreducible, también se vale el regreso.

Si $f(x)$ es irreducible en $F[x]$, entonces $D_x f(x) \neq 0 \iff f(x)$ es separable

Proposición 3

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

$$D_x f(x) \neq 0 \iff f(x) \text{ es separable.}$$

Demostración.

$\Longrightarrow$) Supongamos que F es un campo y que $f(x) \in F[x]$ es irreducible en $F[x]$. Veamos que $f(x)$ y $D_x f(x)$ son primos relativos en $F[x]$.

Queremos ver que el 1 es máximo común divisor de $f(x)$ y $D_f(x)$ o equivalentemente, queremos ver que

- 1 es divisor común de $f(x)$ y $D_x f(x)$.
- Si $p(x)$ es divisor común (en $F[x]$) de $f(x)$ y $D_x f(x)$, entonces $p(x)$ divide al 1, o equivalentemente (como F es un campo) $p(x)$ es constante.

Por supuesto, la primera condición es trivial. Para la segunda, supongamos que $p(x)$ es divisor común (en $F[x]$) de $f(x)$ y $D_x f(x)$ y veamos que $p(x)$ es constante.

Como $f(x)$ es irreducible en $F[x]$, entonces los únicos divisores en $F[x]$ de $f(x)$ son constantes o de la forma $a \cdot f(x)$ para alguna $a \in F$.

Veamos que $p(x)$ es constante demostrando que $p(x)$ no puede ser de la forma $a \cdot f(x)$ para alguna $a \in F$.

Si $p(x) = a \cdot f(x)$ para alguna $a \in F$, entonces (como $p(x)$ es divisor de $D_x f(x)$), tendríamos que $a \cdot f(x) = p(x)$ divide a $D_x f(x)$. Sin embargo, esto es imposible porque $\deg f(x) > \deg D_x f(x)$ y $D_x f(x) \neq 0$.

Notemos que la hipótesis $D_x f(x) \neq 0$ es necesaria para el argumento porque de lo contrario no habría ningún problema con que $a \cdot f(x)$ divida a $D_x f(x)$.

Por lo tanto, $f(x)$ y $D_x f(x)$ son primos relativos en $F[x]$, o equivalentemente (por la proposición 1), $f(x)$ es separable.

$\Longleftarrow$) Esto es simplemente el corolario anterior (ni siquiera hace falta pedir irreducibilidad).

$\square$

Comentario

Todos estos resultados naturalmente producen interés en el caso en que un polinomio tiene derivada 0. Por ejemplo, es natural preguntarse ¿cuales son condiciones suficientes y necesarias para que un polinomio tenga derivada 0?

En lo que sigue respondemos esta pregunta para el caso en que el campo tiene característica distinta de 0.

Si $\mathrm{ch}(F) = p \neq 0$ y $D_x f(x) = 0$, entonces los únicos coeficientes de $f(x)$ que no son cero son los que corresponden a un múltiplo de p

Proposición 4

Supongamos que F es un campo con $\mathrm{ch}(F) = p \neq 0$ y que $f(x) \in F[x]$ tiene grado ≥ 1. Si $D_x f(x) = 0$, entonces existen únicas $b_0, b_1, \ldots, b_m \in F$ tales que

$$f(x) = b_m x^{pm} + b_{m-1} x^{p(m-1)} + \cdots + b_1 x^p + b_0.$$

En palabras, si la derivada de un polinomio con coeficientes en un campo de característica $p \neq 0$ es 0, entonces los únicos coeficientes que no son cero son los que corresponden a un múltiplo de p.

Demostración. Supongamos que $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in F[x]$ con $a_n \neq 0$ es tal que $D_x f(x) = 0$. Entonces, por definición de derivada

$$na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2 x + a_1 = 0$$

Obviamente esto sucede si y solo si

$$na_n = (n-1)a_{n-1} = \cdots = 2a_2 = a_1 = 0.$$

Ahora bien, si $a_k \neq 0$ con $k \in \{1, \ldots, m\}$, entonces la ecuación anterior implica que $k = 0$ en F o equivalentemente, (como estamos en un campo de característica p) que k es un múltiplo de p en $\mathbb{Z}$.

En otras palabras, si $a_k \neq 0$ con $k \in \{1, \ldots, n\}$, entonces $k = pj$ para alguna $j \in \mathbb{Z}_{\geq 0}$ y por lo tanto

$$p(x) = \sum_{a_k \neq 0} a_k x^k = \sum_{j=0}^{n} a_{pj} x^{pj}.$$

donde la suma en el ultimo termino llega hasta n porque supusimos $a_n \neq 0$. Definiendo $b_j = a_{pj}$ obtenemos lo deseado. □

Observación

Supongamos que F es un campo con $\mathrm{ch}(F) = p \neq 0$. Sean

$$g(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in F[x] \quad \text{y} \quad h(x) = x^p.$$

Denotemos $g(x^p) \coloneqq g \circ h(x)$. Entonces

$$g(x^p) = a_n^{x^{pm}} + a_{n-1} x^{p(m-1)} + \cdots + a_1 x^p + a_0 \quad \text{y} \quad D_x \left(g \circ h\right)(x) = 0.$$

Abusando (un poquito) de la notación, podemos reescribir la segunda ecuación como

$$D_x \left(g(x^p)\right) = 0.$$

Si $\mathrm{ch}(F) = p \neq 0$, entonces
$D_x f(x) = 0 \iff f(x) = g(x^p)$ para alguna $g(x) \in F[x]$

Proposición 5

Supongamos que F es un campo con $\mathrm{ch}(F) = p \neq 0$. Si $f(x) \in F[x]$ tiene grado ≥ 1, entonces

$$D_x f(x) = 0 \iff \exists! g(x) \in F[x] \text{ tal que } f(x) = g(x^p).$$

Debería de ser claro que esto es consecuencia inmediata de la proposición anterior y de la observacion anterior.

Una pregunta natural que hasta este momento no hemos contestado es: ¿cual es la relación entre polinomios irreducibles y polinomios separables?

En lo que sigue contestamos esta pregunta para el caso en que el campo es finito o tiene característica 0.

En campos de característica 0, irreducible $\Longrightarrow$ separable

Corolario 6

Supongamos que F es un campo con $\mathrm{ch}(F) = 0$. Si $f(x) \in F[x]$ es irreducible, entonces $f(x)$ es separable.

Demostración. El caso $\deg f(x) = 1$ es inmediato porque $f(x)$ solo tiene una raíz (y por lo tanto no puede tener raíces múltiples). Por lo tanto, supongamos que $\deg f(x) \geq 2$.

Por la proposición anterior basta ver que $D_x f(x) \neq 0$. Sin embargo, esto es consecuencia inmediata de (i) que $\deg f(x) \geq 2$ y (ii) que para todo polinomio no cero $p(x)$ con coeficientes en un campo con característica 0 tenemos que

$$\deg D_x p(x) = \deg(p(x)) - 1.$$

□

$\mathbb{F}$ finito y $\mathrm{ch}(\mathbb{F}) = p \implies \mathbb{F} = \mathbb{F}^p$

Corolario 7

Supongamos que $\mathbb{F}$ es un campo finito con $\mathrm{ch}(\mathbb{F}) = p$. Si $a \in \mathbb{F}$, entonces existe $b \in \mathbb{F}$ tal que $a = b^p$. Abusando de la notación, podemos escribir lo anterior como $\mathbb{F} = \mathbb{F}^p$.

Demostración. Como el endomorfismo de Frobenius $\varphi : \mathbb{F} \to \mathbb{F}$ es inyectivo y $\mathbb{F}$ es finito, entonces φ también es suprayectivo[1]. Claramente, esto implica lo deseado. □

[1] Recuerda que para funciones entre conjuntos finitos de la misma cardinalidad, inyectividad es equivalente a suprayectividad

En campos finitos, irreducible $\implies$ separable

Proposición 8

Supongamos que $\mathbb{F}$ es un campo finito con $\text{ch}(\mathbb{F}) = p \neq 0$. Si $f(x) \in \mathbb{F}[x]$ es irreducible en $\mathbb{F}[x]$, entonces $f(x)$ es separable.

Demostración. Procedamos por contradicción. Es decir, supongamos que $f(x)$ es inseparable. Como $f(x)$ es irreducible (por la proposición 3), esto implica que $D_x f(x) = 0$. Mas aun, como $\text{ch}(F) = p \neq 0$ (por la proposición 4), esto implica que

$$f(x) = b_m x^{pm} + b_{m-1} x^{p(m-1)} + \cdots + b_1 x^p + b_0$$

para algunas $b_0, b_1, \ldots, b_m \in F$.

Ahora bien, como $\mathbb{F}$ es un campo finito con $\mathrm{ch}(\mathbb{F}) = p = 0$, entonces $\mathbb{F} = \mathbb{F}^p$ y por lo tanto para toda $k \in \{0, 1, \ldots, m\}$ existe $a_k \in \mathbb{F}$ tal que $a_k^p = b_k$.

Sustituyendo esto en la ecuación anterior y usando la proposición 2.13.4, obtenemos

$$\begin{aligned} f(x) &= a_m^p x^{pm} + a_{m-1}^p x^{p(m-1)} + \cdots + a_1^p x^p + a_0^p \\ &= (a_m x^m)^p + (a_{m-1} x^{m-1})^p + \cdots + (a_1 x)^p + a_0^p \\ &= \left(a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0 \right)^p . \end{aligned}$$

Contradiciendo la irreducibilidad de $f(x)$. Por lo tanto, $f(x)$ es separable. $\square$

Notemos que el único momento que en el que ocupamos la finitud de $\mathbb{F}$ fue para concluir que $\mathbb{F} = \mathbb{F}^p$ (verifícalo). Esto sugiere que introduzcamos la siguiente definición.

Campos perfectos

Definición

Supongamos que K es un campo con $\mathrm{ch}(F) = p \neq 0$. Decimos que K es **perfecto** si para toda $a \in K$ existe $b \in K$ tal que $a = b^p$.

Por la observacion anterior, la demostración de la proposición anterior también sirve para ver que en campos perfectos, irreducible $\implies$ separable.

El polinomio $f_{\text{sep}}(x)$

Proposición 9

Supongamos que F es un campo con $\text{ch}(F) = p \neq 0$. Si $f(x) \in F[x]$ es irreducible en $F[x]$, entonces existe un único entero $k \geq 0$ y un único polinomio $f_{\text{sep}}(x) \in F[x]$ que es irreducible en $F[x]$, es separable, y

$$f(x) = f_{\text{sep}}(x^{p^k}).$$

Demostración. Supongamos que $f(x) \in F[x]$ es irreducible.

Demostración de existencia.

Antes de empezar, notemos que si $p(x)$ es irreducible en $K[x]$ y $p(x) = q(x^n)$ con $n \geq 1$, entonces $q(x^n)$ también es irreducible en $K[x]$. En efecto, si $q(x) = a(x)b(x)$ con $a(x), b(x) \in K[x]$ de grado ≥ 1, entonces $f(x) = a(x^n)b(x^n)$ con $a(x^n), b(x^n) \in K[x]$ de grado ≥ 1, contradiciendo la irreducibilidad de $f(x)$.

Por lo tanto, para la proposición, basta probar la existencia de un $f_{\text{sep}}(x) \in F[x]$ separable tal que $f(x) = f_{\text{sep}}(x^{p^k})$ para alguna $k \in \mathbb{Z}_{\geq 1}$.

Con esto en mente, continuemos con la demostración de existencia.

Caso 1. $f(x)$ *es separable.*
Claramente $k = 0$ y $f_{\text{sep}}(x) = f(x)$ cumplen lo deseado.

Caso 2. $f(x)$ *es inseparable.*
En este caso, la proposición 3 implica que $D_x f(x) = 0$. Como $\text{ch}(F) = p \neq 0$, (por la proposición 5) esto implica que $f(x) = f_1(x^p)$ para algún *único* $f_1(x) \in F[x]$.

Caso 2.1. $f_1(x)$ *es separable.*
Claramente, $k = 1$ y $f_{\text{sep}}(x) = f_1(x)$ cumplen lo deseado.

Caso 2.2. $f_1(x)$ *es inseparable.*
Procediendo de la misma manera que en el caso 2, obtenemos un *único* polinomio $f_2(x) \in F[x]$ tal que $f_1(x) = f_2(x^p)$ y por lo tanto,

$$f(x) = f_1(x^p) = f_2((x^p)^p) = f_2(x^{p^2}).$$

Caso 2.2.1. $f_2(x)$ *es separable.*
Claramente, $k = 2$ y $f_{\text{sep}}(x) = f_2(x)$ cumplen lo deseado.

Caso 2.2.2. $f_2(x)$ *es inseparable.*

$$\vdots$$

Veamos que si continuamos de esta manera, eventualmente encontraremos una $k \in \mathbb{Z}_{\geq 1}$ tal que $f_k(x)$ es separable.

Para esto, supongamos lo contrario. En particular, tendremos una sucesión infinita de polinomios $\{f_i(x)\}_i$ tal que $f_i(x) = f_{i+1}(x^p)$ para toda i.

Por otro lado, es fácil verificar que si $p(x) = q(x^n)$ con $n \geq 2$, entonces $\deg p(x) > \deg q(x)$.

Como $f_i(x) = f_{i+1}(x)$ para toda i, entonces lo anterior implica que

$$0 < \cdots < \deg f_{i+1}(x) < \deg f_i(x) < \cdots \deg f_1(x) < \deg f(x).$$

Sin embargo, como $\{f_i(x)\}_i$ es infinita, esto es imposible.

Por lo tanto, existe una $k \in \mathbb{Z}_{\geq 1}$ tal que $f_k(x)$ es separable y como (por definición de los $f_i(x)$)

$$f(x) = f_1(x^p) = f_2(x^{p^2}) = \cdots = f_k(x^{p^k}),$$

entonces $f_{\text{sep}}(x) = f_k(x)$ cumple lo deseado.

Fin de la demostración de existencia.

Demostración de unicidad.

Supongamos que $n \in \mathbb{Z}_{\geq 1}$ y que $g(x) \in F[x]$ es irreducible en $F[x]$, es separable, y

$$f(x) = g(x^{p^n}).$$

En particular,

$$f(x) = g\left(\left(x^{p^{n-1}}\right)^p\right).$$

Ahora bien, como $f_1(x)$ es el *único* polinomio que satisface $f(x) = f_1(x^p)$, entonces

$$f_1(x) = g(x^{p^{n-1}}).$$

Continuando de esta manera, obtenemos que

$$f_i(x) = g(x^{p^{n-i}})$$

para toda i con $1 \leq i \leq k$ y $1 \leq i \leq n$.

Veamos que esto implica que $n \geq k$. Si $n < k$, entonces por lo anterior tendríamos

$$f_n(x) = g(x^{p^{n-n}}) = g(x).$$

Sin embargo, esto es imposible porque (por hipótesis) $g(x)$ es separable y (por definición) $f_i(x)$ es inseparable para toda $i \in \{1, \ldots, k-1\}$.

Por lo tanto, $n \geq k$ y podemos escribir

$$f_{\text{sep}}(x) = f_k(x) = g(x^{p^{n-k}}).$$

Usando esto, veamos que $f_{\text{sep}}(x) = g(x)$ demostrando que $n = k$. Para esto, supongamos lo contrario, es decir, $n > k$.

Como $\text{ch}(F) = 0$ y $n > k$, entonces

$$D_x f(x) = D_x \left(g(x^{p^{n-k}}) \right) = 0.$$

Sin embargo, esto es imposible porque $f_{\text{sep}}(x)$ es separable o equivalentemente, $\big(f(x), D_x f(x)\big) = 1$.

Fin de la demostración de unicidad. □