Polinomios simétricos

Facultad de Ciencias UNAM

Introducción

En esta sección, interrumpimos (de nuevo) nuestro estudio de polinomios separables para demostrar un resultado que sera muy útil en el futuro.

Supongamos que F es un campo y que

$$f(x) = x^3 + a_1 x^2 + a_2 x + a_3 \in F[x]. \tag{1}$$

Si $\alpha_1, \alpha_2, \alpha_3$ son raíces de $f(x)$, sabemos que también podemos escribir

$$f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3).$$

Si desarrollamos esta expresión (multiplicando de la manera usual) obtenemos

$$f(x) = x^3 - (\alpha_1 + \alpha_2 + \alpha_3)\, x^2 + (\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3)\, x - \alpha_1\alpha_2\alpha_3. \tag{2}$$

Juntando (1) y (2) obtenemos

$$\begin{aligned} a_1 &= -(\alpha_1 + \alpha_2 + \alpha_3) \\ a_2 &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 \\ a_3 &= -\alpha_1\alpha_2\alpha_3 \end{aligned}$$

Si procedemos de la misma manera para un polinomio de grado 4 veremos que sucede algo muy similar. Específicamente, si

$$f(x) = x^4 + a_1 x^3 + a_2 x^2 + a_3 x + a_4 \in F[x]$$

y $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ son raíces de $f(x)$, es fácil verificar que

$$\begin{aligned}
a_1 &= -\left(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4\right) \\
a_2 &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4 \\
a_3 &= -\left(\alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \alpha_1\alpha_3\alpha_4 + \alpha_2\alpha_3\alpha_4\right) \\
a_4 &= \alpha_1\alpha_2\alpha_3\alpha_4
\end{aligned}$$

Sin tomar en cuenta el signo, pareciera que a_1 es la suma de todas las raíces, a_2 es la suma de todas las "parejas" de raíces, a_3 es la suma de todas las "tripletas" de raíces, y a_4 es la suma de todas las cuádruplas de raíces.

En lo que sigue veremos que esta idea es correcta para cualquier grado. Para esto, antes introducimos una definición.

Polinomios simétricos elementales

Definición

Supongamos que F es un campo y que $x_1, \ldots, x_n$ son variables indeterminadas. Los siguientes elementos de $F[x_1, \ldots, x_n]$ son llamados los **polinomios simétricos elementales** de $F[x_1, \ldots, x_n]$.

$$\begin{aligned}
\sigma_1(x_1, \ldots, x_n) &= x_1 + x_2 + \cdots + x_n \\
\sigma_2(x_1, \ldots, x_n) &= \sum_{1 \le i < j \le n} x_i x_j \\
&\vdots \\
\sigma_j(x_1, \ldots, x_n) &= \sum_{1 \le i_1 < \cdots < i_j \le n} x_{i_1} x_{i_2} \cdots x_{i_j} \\
&\vdots \\
\sigma_n(x_1, \ldots, x_n) &= x_1 x_2 \cdots x_n
\end{aligned}$$

La utilidad de los polinomios simétricos elementales

Proposición 1

Supongamos que $x_1, \ldots, x_n$ son variables indeterminadas. Si x es otra variable indeterminada, entonces

$$(x - x_1) \cdots (x - x_n) = x^n - \sigma_1 x^{n-1} + \cdots + (-1)^j \sigma_j x^{n-j} + \cdots + (-1)^n \sigma_n$$

donde $\sigma_j = \sigma_j(x_1, \ldots, x_n)$.

Demostración. Como es de esperarse, la demostración es consecuencia de desarrollar el lado izquierdo de la ecuación y luego encontrar el coeficiente de cada una de las potencias de x.

Para esto, observa que podemos reescribir $(x - x_1) \cdots (x - x_n)$ usando el siguiente procedimiento (el cual es fácil de verificar por inducción sobre n):

1. Para cada uno de los n factores $x - x_i$ escoge x ó $-x_i$.
2. Toma el producto de estas n elecciones.
3. Suma estos productos sobre todas las posibles formas de hacer las n elecciones.

En otras palabras,

$$(x - x_1) \cdots (x - x_n) = \sum_{\xi_i \in \{x, -x_i\}} \xi_1 \xi_2 \cdots \xi_n$$

Notemos que los términos de $(x - x_1) \cdots (x - x_n)$ que involucran a x^{n-j} son aquellos productos que corresponden a escoger x exactamente $n - j$ veces en el paso 1.

En particular, si fijamos una elección que involucra a x^{n-j} y suponemos que $i_1, \ldots, i_j$ son los índices de los factores en donde *no* escogimos a x, entonces el producto de esta elección es

$$(-x_{i_1})(-x_{i_2})\cdots\left(-x_{i_j}\right)x^{n-j} = (-1)^j x_{i_1}\cdots x_{i_j} x^{n-j}.$$

Por supuesto, esta elección corresponde a $\xi_{i_k} = x_{i_k}$ para toda i_k y $\xi_i = x$ para toda $i \notin \{i_1, \ldots, i_j\}$.

Finalmente, cuando sumamos sobre todas las posibles formas de hacer las n elecciones (como indica el paso 3), entonces lo anterior implica que el coeficiente de x^{n-j} es

$$(-1)^j \sum_{1\leq i_1<\cdots<i_j\leq n} x_{i_1}x_{i_2}\cdots x_{i_j} = (-1)^j \sigma_j.$$

$\square$

Los coeficientes de un polinomio mónico en términos de sus raíces

Corolario 2

Supongamos que F es campo, que

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

y que K/F es una extensión de campos en donde $f(x)$ se descompone. Si $\alpha_1, \ldots, \alpha_n \in K$ son las raíces de $f(x)$, entonces

$$a_k = (-1)^k \sigma_j(\alpha_1, \ldots, \alpha_n)$$

para toda $k \in \{1, \ldots, n\}$.

Demostración. Evaluando $x_1 = \alpha_1, \ldots, x_n = \alpha_n$ en la proposición anterior obtenemos

$$\begin{aligned}(x-\alpha_1)\cdots(x-\alpha_n) = x^n - \sigma_1(\alpha_1,\ldots,\alpha_n)x^{n-1} + \cdots \\ + (-1)^{n-1}\sigma_{n-1}(\alpha_1,\ldots,\alpha_n)x + (-1)^n\sigma_n(\alpha_1,\ldots,\alpha_n) \quad (3)\end{aligned}$$

Pero como $\alpha_1, \ldots, \alpha_n$ son las raíces de $f(x)$, entonces el lado izquierdo de (3) es $f(x)$. Usando esto y comparando los coeficientes del lado derecho de (3) con los coeficientes de

$$f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x + a_n$$

obtenemos lo deseado. $\square$

Comentario

Supongamos que F es un campo, que

$$f(x) = x^4 + a_1 x^3 + a_2 x^2 + a_3 x + a_4 \in F[x],$$

y que K/F es una extensión en donde $f(x)$ se descompone. En la introducción vimos que si $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in K$ son raíces de $f(x)$, entonces

$$\begin{aligned}
a_1 &= -(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4) \\
a_2 &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4 \\
a_3 &= -(\alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \alpha_1\alpha_3\alpha_4 + \alpha_2\alpha_3\alpha_4) \\
a_4 &= \alpha_1\alpha_2\alpha_3\alpha_4
\end{aligned}$$

Como $f(x)$ tiene coeficientes en F, lo anterior implica que los elementos que están en el lado derecho de las ecuaciones anteriores también pertenecen a F. Esto es interesante porque en principio solo sabíamos que estos elementos pertenecen a K.

Si nos quedamos viendo a estos elementos, veremos que todos tienen la siguiente propiedad: *podemos intercambiar cualesquiera dos α_i's sin alterar el elemento.*

Por ejemplo, si intercambiamos α_1 y α_2 en a_2, el elemento resultante sigue siendo a_2. En efecto,

$$\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4 =$$
$$\alpha_2\alpha_1 + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_3\alpha_4.$$

En contraste,

$$\alpha_1\alpha_2 + \alpha_1 \neq \alpha_2\alpha_1 + \alpha_2$$

es un ejemplo de que la situación anterior no siempre sucede.

El objetivo de esta sección es demostrar que la observacion hecha al inicio de este comentario (de que los elementos del lado derecho de las ecuaciones pertenecen a F) es un caso particular de un resultado que involucra a estos elementos en donde podemos intercambiar cualesquiera dos α_i's. Para esto, necesitaremos la siguiente definición.

Polinomios simétricos

Definición

Supongamos que F es un campo y que $x_1, \ldots, x_n$ son variables indeterminadas. Un polinomio $f(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$ es **simétrico** si

$$f\left(x_{\tau(1)}, \ldots, x_{\tau(n)}\right) = f(x_1, \ldots, x_n)$$

para toda $\tau \in S_n$.

Cabe recalcar que esta definición depende de las variables que estemos considerando. Por ejemplo, el polinomio $x_1x_2 \in F[x_1, x_2]$ es simétrico pero el polinomio $x_1x_2 \in F[x_1, x_2, x_3]$ no es simétrico (considera $\tau = (23)$). Por eso, también decimos que un polinomio es *simétrico en* $x_1, \ldots, x_n$.

Ejemplos de polinomios simétricos

Supongamos que F es un campo.

- Es fácil verificar que la suma, resta, y multiplicación de polinomios simétricos es un polinomio simétrico y por lo tanto, el conjunto de polinomios simétricos en $F[x_1, \ldots, x_n]$ forma un subanillo de $F[x_1, \ldots, x_n]$ el cual denotamos $F_{\text{sim}}[x_1, \ldots, x_n]$.
- Si $c \in F$ es una constante, entonces el siguiente polinomio en $F[x_1, \ldots, x_n]$ es simétrico.

$$(c - x_1)(c - x_2) \cdots (c - x_n)$$

- Los siguientes polinomios en $F[x_1, x_2, x_3, x_4]$ son simétricos.

$$\begin{aligned}
\sigma_1(x_1, x_2, x_3, x_4) &= -(x_1 + x_2 + x_3 + x_4) \\
\sigma_2(x_1, x_2, x_3, x_4) &= x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 \\
\sigma_3(x_1, x_2, x_3, x_4) &= -(x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4) \\
\sigma_4(x_1, x_2, x_3, x_4) &= x_1x_2x_3x_4
\end{aligned}$$

  En lo que sigue, veremos que esto es cierto en general.

Los polinomios simétricos elementales son simétricos

Proposición 3

Supongamos que F es un campo y que $x_1, \ldots, x_n$ son variables indeterminadas. Entonces $\sigma_j(x_1, \ldots, x_n)$ es simétrico para toda $j \in \{1, \ldots, n\}$.

Demostración. Supongamos que $\tau \in S_n$. Entonces por la proposición 1

$$
\begin{aligned}
x^n - \sigma_1(x_{\tau(1)}, \ldots, x_{\tau(n)})x^{n-1} + \cdots + (-1)^j \sigma_j(x_{\tau(1)}, \ldots, x_{\tau(n)})x^{n-j} + \cdots \\
+(-1)^n \sigma_n(x_{\tau(1)}, \ldots, x_{\tau(n)}) = \\
(x - x_{\tau(1)})(x - x_{\tau(2)}) \cdots (x - x_{\tau(n)}) = \\
(x - x_1)(x - x_2) \cdots (x - x_n) = \\
x^n - \sigma_1(x_1, \ldots, x_n)x^{n-1} + \cdots + (-1)^j \sigma_j(x_1, \ldots, x_n)x^{n-j} + \cdots \\
+(-1)^n \sigma_n(x_1, \ldots, x_n)
\end{aligned}
$$

y por lo tanto,

$$
(-1)^j \sigma_j(x_{\tau(1)}, \ldots, x_{\tau(n)})x^{n-j} = (-1)^j \sigma_j(x_1, \ldots, x_n)x^{n-j}
$$

para toda $j \in \{1, \ldots, n\}$. Usando esto, obtenemos lo deseado. $\square$

El teorema fundamental de los polinomios simétricos

Proposición 4

Supongamos que F es un campo y que $x_1, \ldots, x_n$ son variables indeterminadas. Si $p(x_1, \ldots, x_n) \in F_{\text{sim}}[x_1, \ldots, x_n]$, entonces podemos escribir

$$p(x_1, \ldots, x_n) = c_1 f_1(x_1, \ldots, x_n) + \cdots + c_m f_m(x_1, \ldots, x_n)$$

donde $c_1, \ldots, c_m \in F$ y los $f_j(x_1, \ldots, x_n)$ son de la siguiente forma

$$f_j(x_1, \ldots, x_n) = \sigma_1^{k_{j,1}}(x_1, \ldots, x_n) \cdots \sigma_n^{k_{j,n}}(x_1, \ldots, x_n), \quad k_{j,i} \in \mathbb{Z}_{\geq 0}$$

Si omitimos los "$(x_1, \ldots, x_n)$", entonces podemos escribir las igualdades anteriores como

$$\begin{aligned} p &= c_1 f_1 + \cdots c_m f_m \\ &= c_1(\sigma_1^{k_{1,1}} \cdots \sigma_n^{k_{1,n}}) + \cdots + c_m(\sigma_1^{k_{m,1}} \cdots \sigma_n^{k_{m,n}}) \end{aligned}$$

Comentario

La demostración del teorema fundamental de los polinomios simétricos es larga y ocupa un método que no ocuparemos en este curso. Por eso, la omitimos y referimos al lector interesado a Cox, Galois Theory, Theorem 2.2.2.

Finalizamos esta sección presentando el resultado que en la introducción mencionamos sera muy útil en el futuro.

Corolario 5

Supongamos que F es un campo, que $f(x) \in F[x]$ es mónico con grado $n > 0$, que K/F es una extensión de campos en donde $f(x)$ se descompone, y que $\alpha_1, \dots, \alpha_n \in K$ son raíces de $f(x)$.

Si $p(x_1, \dots, x_n) \in F[x_1, \dots, x_n]$ es simétrico, entonces

$$p(\alpha_1, \dots, \alpha_n) \in F.$$

Demostración. Como $p(x_1, \dots, x_n)$ es simetrico, el teorema fundamental de los polinomios simetricos implica que podemos escribir

$$p = c_1(\sigma_1^{k_{1,1}} \cdots \sigma_n^{k_{1,n}}) + \cdots + c_m(\sigma_1^{k_{m,1}} \cdots \sigma_n^{k_{m,n}}) \tag{4}$$

con $c_j \in F$ y $k_{j,i} \in \mathbb{Z}_{\geq 0}$.

Ahora bien, como $\sigma_j(\alpha_1, \dots, \alpha_n) \in F$ para toda $j \in \{1, \dots, n\}$, entonces al evaluar $x_1 = \alpha_1, \dots, x_n = \alpha_n$ en (4) obtenemos lo deseado. $\square$