Relaciones entre los coeficientes de un polinomio y sus raíces

Pablo L. De Nápoli

Departamento de Matemática
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires

Álgebra I - Primer cuatrimestre de 2020

Parte I

Polinomios cuadráticos

El caso de polinomios cuadráticos

Consideremos un polinomio cuadrático

$$P(X) = aX^2 + bX + c \ \in \mathbb{C}[X],$$

y llamemos α_1, α_2 a sus raíces. Entonces P admite la factorización:

$$P(X) = a(X - \alpha_1)(X - \alpha_2)$$

Si efectuamos el producto utilizando la propiedad distributiva, obtenemos:

$$P(X) = a(X^2 - (\alpha_1 + \alpha_2)X + \alpha_1\alpha_2)$$

Igualando los coeficientes, obtenemos las siguientes relaciones entre coeficientes y raíces:

$$S_1 = S_1(\alpha_1, \alpha_2) := \alpha_1 + \alpha_2 = -\frac{b}{a}$$

$$S_2 = S_2(\alpha_1, \alpha_2) := \alpha_1\alpha_2 = \frac{c}{a}$$

S_1 y S_2 se llaman las funciones simétricas elementales de las raíces.

Otras funciones simétricas

A partir de las funciones simétricas elementales podemos calcular otras funciones simétricas de las raíces como por ejemplo

$$C = C(\alpha_1, \alpha_2) := \alpha_1^2 + \alpha_2^2$$

ya que

$$S_1^2 = (\alpha_1 + \alpha_2)^2 = \alpha_1^2 + \alpha_2^2 + 2\alpha_1\alpha_2 = C + 2S_2$$

$$\Rightarrow C = S_1^2 - 2S_2$$

El discriminante

Similarmente, consideremos la función simétrica de las raíces dada por

$$D = D(\alpha_1, \alpha_2) = (\alpha_1 - \alpha_2)^2$$

Tenemos que

$$D = \alpha_1^2 - 2\alpha_1\alpha_2 + \alpha_2^2 = C - 2S_2 = S_1^2 - 4S_2$$

y usando las relaciones entre las funciones simétricas elementales y los coeficientes, encontramos que

$$D = \left(-\frac{b}{a}\right)^2 - 4\left(\frac{c}{a}\right) = \frac{b^2 - 4ac}{a^2}$$

El número $\Delta = b^2 - 4ac$ se conoce como el discriminante del polinomio P. Notemos que P tendrá una raíz doble si y sólo si $\Delta = 0$.

Fórmulas para las raíces

A partir de esto encontramos que

$$\alpha_1 - \alpha_2 = \pm\frac{\sqrt{\Delta}}{a}$$

Elegimos una de las raíces cuadradas de Δ y podemos suponer que el signo es $+$, intercambiando sinó los nombres de α_1 y α_2. Y como

$$S_1 = \alpha_1 + \alpha_2 = -\frac{b}{a}$$

Deducimos que

$$\alpha_1 = \frac{-b + \sqrt{\Delta}}{2a}, \quad \alpha_2 = \frac{-b - \sqrt{\Delta}}{2a}$$

Un ejemplo

Consideremos el polinomio $X^3 - 1 \in \mathbb{C}[X]$. Se factoriza como

$$X^3 - 1 = (X - 1)(X^2 + X + 1)$$

Deducimos que las raíces cúbicas primitivas de la unidad ω_1, ω_2 son exactamente las raíces del polinomio cuadrático

$$P = X^2 + X + 1$$

Deducimos que

$$G_2^* = \left\{ \omega_1 := -\frac{1}{2} + \frac{\sqrt{3}}{2} i, \omega_2 := -\frac{1}{2} - \frac{\sqrt{3}}{2} i \right\}$$

$$\Delta = -3, \omega_1 + \omega_2 = -1, \quad \omega_1 \cdot \omega_2 = 1$$

Algunas observaciones

- La fórmula para las raíces se puede aplicar sobre cualquier cuerpo K (no sólo los números complejos) siempre que $2 = 1 + 1 \neq 0$ en el cuerpo (para poder dividir por 2) y que Δ tenga una raíz cuadrada en K (sino nuestra ecuación cuadrática no tendrá raíces en K).
- Ejemplo: si $K = \mathbb{R}$ la ecuación cuadrática $X^2 + X + 1 = 0$ no tiene raíces porque $\Delta = -3$ no tiene raíces cuadradas reales (¡es negativo!).

Otros Ejemplo

La congruencia

$$X^2 + X + 1 \equiv 0 \pmod 7$$

tiene dos soluciones que podemos encontrar por el método anterior. Para ello notamos que $K = \mathbb{Z}_7 = \mathbb{Z}/7\mathbb{Z}$ es un cuerpo pues 7 es primo. Y que $2 \not\equiv 0 \pmod 7$. El inverso multiplicativo de $\overline{2}$ módulo 7 es $\overline{4}$

$$2 \times 4 \equiv 1 \pmod 7$$

Entonces $\Delta = -3$ tiene una raíz cuadrada en K pues

$$2^2 = 4 \equiv -3 \pmod 7$$

(Se dice que -3 es un resto cuadrático módulo 7.) Entonces

$$\alpha_1 = (-1+2)\cdot 4 = 4,\ \alpha_2 = (-1-2)\cdot 4 = -12 \equiv 2 \pmod 7$$

son las soluciones de esta congruencia.

Otros Ejemplo (2)

En cambio si miramos la misma congruencia módulo 5

$$X^2 + X + 1 \equiv 0 \pmod 5$$

no tiene soluciones.
De nuevo $K = \mathbb{Z}_5 = \mathbb{Z}/5\mathbb{Z}$ es un cuerpo pues 5 es primo. Y podemos dividir por 2 pues $2 \not\equiv 0 \pmod 5$ y $2 \times 3 \equiv 1 \pmod 5$. Así que la teoría anterior es aplicable en este ejemplo.
Pero ahora $\Delta = -3 \equiv 2 \pmod 5$ no tiene raíces cuadradas en K pues

$$0^2 \equiv 0, 1^2 \equiv 1, 2^2 \equiv 4, 3^2 = 9 \equiv 4, 4^2 \equiv 1 \pmod 5$$

Se dice que -3 es un no resto cuadrático módulo 5.
Concluimos que nuestra congruencia, no tiene soluciones.

Parte II

Relaciones entre coeficientes y raíces en general

El caso de polinomios cúbicos

$$P(X) = a_3X^3 + a_2X^2 + a_1X + a_0 \ \in \mathbb{C}[X]$$

Llamemos α_1, α_2, α_3 a sus raíces, P admite la factorización:

$$P(X) = a_3(X - \alpha_1)(X - \alpha_2)(X - \alpha_3)$$

Efectuando la distributiva tenemos que:

$$P(X) = a_3(X^3 - S_1X^2 + S_2X - S_3)$$

siendo

$$\begin{aligned} S_1 &= \alpha_1 + \alpha_2 + \alpha_3 \\ S_2 &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 \\ S_3 &= \alpha_1\alpha_2\alpha_3. \end{aligned}$$

Igulando los coeficientes obtenemos que:

$$S_1 = -\frac{a_2}{a_3}, \quad S_2 = \frac{a_1}{a_3}, \quad S_3 = -\frac{a_0}{a_3}$$

¿Y en general?

Podemos generalizar este hecho, para polinomios de grado arbitrario del siguiente modo. Sea $P \in \mathbb{C}[X]$ un polinomio de grado n

$$P(X) = \sum_{i=0}^{n} a_i X^i \ (a_n \neq 0)$$

y llamemos a $\alpha_1, \alpha_2, \ldots, \alpha_n$ a sus n raíces en $\mathbb{C}$, donde repetimos cada raíz tantas veces como indique su multiplicidad. Entonces, el polinomio P admite la factorización:

$$P(X) = a_n(X - \alpha_1)(X - \alpha_2)\cdots(X - \alpha_n)$$

Las funciones simétricas elementales, caso general

Efectuamos ahora la distributiva. Para ello, notamos que el término en X^k en este producto se debe formar sumando todos los productos que se obtienen eligiendo el término "X" en k de los factores, y el término "$-\alpha_i$" en $n-k$ de los factores. Es decir que el coeficiente de X^k debe ser:

$$(-1)^{n-k} S_{n-k}$$

donde notamos por S_k a la suma de todas los productos que se puedan formar considerando k de las n raíces $\alpha_1, \alpha_2, \ldots, \alpha_n$. Es decir que:

$$S_k = S_k(\alpha_1, \alpha_2, \ldots, \alpha_n) = \sum_{i_1, i_2, \ldots, i_k} \alpha_{i_1} \alpha_{i_2} \cdots \alpha_{i_k}$$

donde $1 \leq i_1, i_2, \ldots, i_k \leq n$, y los índices $i_1, i_2, \ldots, i_k$ son todos distintos.

Las funciones simétricas elementales, caso general(2)

Por ejemplo:

$$S_n = \alpha_1 \alpha_2 \ldots \alpha_n$$

es el producto de todas las raíces.

$$S_1 = \alpha_1 + \alpha_2 + \ldots + \alpha_n$$

es la suma de todas las raíces. Y

$$S_2 = \sum_{i<j} \alpha_i \alpha_j$$

es la suma de todos los posibles productos de dos de las raíces.
Las funciones S_k son polinomios en varias variables (de grado k), en las variables $\alpha_1, \alpha_2, \ldots, \alpha_n$. Y tienen la propiedad de que su valor no cambia si permutamos en cualquier orden las raíces (son polinomios simétricos).
Reciben el nombre de funciones simétricas elementales.

Fórmula General

$$\Rightarrow \; P(X) = a_n \sum_{k=0}^{n} (-1)^{n-k} S_{n-k} X^k$$

de donde, igualando los coeficiente, obtenemos la siguiente fórmula que relaciona los coeficientes del polinomio P con las funciones simétricas elementales de sus raíces:

Teorema

$$S_{n-k} = (-1)^{n-k} \frac{a_k}{a_n}$$

En particular para la suma de las raíces tenemos (tomando $k = n-1$) que:

$$S_1 = \alpha_1 + \alpha_2 + \ldots + \alpha_n = -\frac{a_{n-1}}{a_0}$$

y para el producto (tomando $k = 0$) que:

$$S_n = \alpha_1 \cdot \alpha_2 \cdots \alpha_n = (-1)^n \frac{a_0}{a_n}$$

Ejemplo: el binomio de Newton

Notemos que (por su definición) hay exactamente $\binom{n}{k}$ términos en la suma S_k. Si tomamos como P el polinomio

$$P = (X - \alpha)^n$$

(Es decir elegimos las n raíces iguales a α), tendremos que:

$$S_k = \binom{n}{k} \alpha^k$$

y como $a_n = 1$ la fórmula nos da que:

$$(X - \alpha)^n = \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} \alpha^{n-k} X^k$$

Es decir, que se obtiene como caso particular la fórmula del binomio de Newton.

Aplicación a las raíces de la unidad

Si aplicamos estos resultados al polinomio $P = X^n - 1$ podemos calcular de otra forma la suma y el producto de las reaíces n-ésimas de la unidad.

$$G_n = \{\omega_0, \omega_1, \ldots, \omega_{n-1}\}$$

Obtenemos:

$$S_1 = \omega_0 + \omega_1 + \ldots + \omega_{n-1} = \begin{cases} 1 & \text{si} \quad n = 1 \\ 0 & \text{si} \quad n > 1 \end{cases}$$

$$S_n = \omega_0 \cdot \omega_1 \cdots \omega_{k-1} = \begin{cases} 1 & \text{si} \quad n \quad \text{es impar} \\ -1 & \text{si} \quad n \quad \text{es par} \end{cases}$$

(proposición 6.4.13 del apunte de la profesora Kirck)

Otras funciones simétricas

Las funciones simétricas elementales pueden utilizarse para calcular otras funciones simétricas de las raíces. Ej:

$$C = \sum_{i=1}^{n} \alpha_i^2$$

Esta expresión C es un polinomio simétrico en $\alpha_1, \alpha_2, \ldots, \alpha_n$ de grado 2. Podemos expresar a este polinomio C en términos de S_1 y S_2 como sigue:

$$S_1^2 = \left(\sum_{i=1}^{n} \alpha_i\right)^2 = \sum_{i=1}^{n} \alpha_i^2 + 2 \sum_{1 \leq i < j \leq n} \alpha_i \alpha_j = C + 2S_2$$

En consecuncia,

$$C = S_1^2 - 2S_2$$

y por lo tanto C puede expresarse en función de los coeficientes del polinomio P:

$$C = \frac{a_{n-1}^2}{a_n^2} - 2\frac{a_{n-2}}{a_n}$$

Un resultado general

Teorema

Cualquier función polinomial simétrica de las raíces de un polinomio P puede expresarse como una función polinomial de las funcions simétricas elementales S_k, y por consiguiente como una función racional (un cociente de polinomios) de los coeficientes del polinomio P.

La demostración de este teorema está fuera del alcance de esta materia.

Una aplicación a la aritmética

Las fórmulas anteriores funcionan sobre cualquier cuerpo K en el que el polinomio tenga tantas raíces como su grado (contadas de acuerdo a su multiplicidad).
Veamos un ejemplo: si p es un número primo impar $\Rightarrow$ $K = \mathbb{Z}_p = \mathbb{Z}/(p\mathbb{Z})$ es un cuerpo, entonces el polinomio $X^{p-1} - 1$ tiene las $p - 1$ raíces

$$\overline{1}, \overline{2}, \ldots, \overline{p-2}, \overline{p-1}$$

por el teorema de Fermat, y su producto es

$$S_{p-1} = \overline{(p-1)!}$$

Por la fórmula anterior, deducimos que

$$(p-1)! \equiv (-1)^{p-1} \frac{(-1)}{1} \equiv -1 \pmod{p}$$

(teorema de Wilson, ejercicio 28 de la práctica 5)