Polinomios (parte 3)

Pablo L. De Nápoli

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

Álgebra I - Segundo cuatrimestre de 2020

Reapaso de la clase anterior: Polinomios irreducibles

Definición

Sea $P \in K[X]$ un polinomio no constante. Diremos que el polinomio P es irreducible en $K[X]$ si no es posible factorizarlo en la forma $P = Q \cdot S$ donde Q y S son polinomios en $K[X]$ no contantes.

- Un polinomio de grado 1 es siempre irreducible en $K[X]$.
- Un polinomio P es divisible por $X - a$ si y sólo si a es una raíz de P.
- Un polinomio de grado 2 o 3 es irreducible en $K[X]$ si y sólo si no tiene raíces en K.
  Ejemplo: $X^2 + 1$ es irreducible en $\mathbb{R}[X]$ pero no en $\mathbb{C}[X]$ donde se factoriza como
  $$X^2 + 1 = (X + i)(X - i)$$
  Vemos que la noción de polinomio irreducible depende del cuerpo K en el que estemos trabajando.

Reapaso de la clase anterior: Polinomios irreducibles (2)

- En general, un polinomio irreducible en $K[X]$ no puede tener raíces en K. Pero la recíproca no es cierta.$(X^2+1)^2 = X^4+2X^2+1$ no es irreducible en $\mathbb{R}[X]$ aunque no tiene raíces en $\mathbb{R}$.

- Si $P \in K[X]$ es un polinomio, y $\alpha_1, \alpha_2, \ldots, \alpha_r$ son raíces distintas de P, entonces P admite la factorización siguiente:

$$P(X) = (X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_r)Q(X)$$

Si $gr(P) = r$, Q es el coeficiente principal del polinomio P (el que acompaña a X^r).
Ejemplo: miremos el polinomio X^4-1. Sus raíces en $\mathbb{C}$ son las raíces cuartas de la unidad $G_4 = \{1, i, -1, -i\}$. Luego

$$X^4 - 1 = (X-1)(x+1)(X-i)(X+i)$$

Reapaso de la clase anterior: Teorema de factorización

Al final de la clase pasada mencionamos el teorema de factorización única para polinomios.

Teorema

Cada polinomio $P \in K[X]$ se puede factorizar de manera única en la forma:

$$P = k \cdot P_1 \cdot P_2 \cdots P_r$$

siendo k una constante no nula de K, y los P_i polinomios irreducibles en $K[X]$.
La factorización es única en el sentido de que cualquier otra factorización sólo puede diferir en el orden de los factores, en el valor de la constante k y en la multiplicación de alguno de los factores P_i por una constante no nula de K (ajustando adecuadamente el valor de la constante k).

Raíces dobles de ecuaciones cuadráticas

Recordemos que en el caso de las ecuaciones cuadráticas:

$$P = aX^2 + bX + c = 0$$

las dos raíces α_1, α_2 que proporciona la fórmula para resolver ecuaciones de segundo grado coinciden cuando el discriminante $\Delta = b^2 - 4ac$ de la ecuación se anula, y tenemos en este caso:

$$\alpha_1 = \alpha_2 = \frac{-b}{2a}$$

y el polinomio P se factoriza en la forma:

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

Decimos en este caso que el polinomio P tiene a α_1 como raíz doble.
Ejemplo: $P = X^2 + 2X + 1 = (X + 1)^2$ tiene a -1 como raíz doble.

Multiplicidad de un raíz

Generalizando este ejemplo, introducimos la siguiente definición:

Definición

Sea $P \in K[X]$ un polinomio, y sea $a \in K$ una raíz de P. Decimos que a es una raíz de P de multiplicidad m ($m \in \mathbb{N}$) si P admite la factorización:

$$P(X) = (X - a)^m Q(X)$$

donde el polinomio Q no se anula en $X = a$, o sea $Q(a) \neq 0$. Si $m = 1$ se dice que a es una raíz simple, si $m = 2$ que es doble, etcétera.

Ejemplo: El polinomio $P = X^3 - 4X^2 + 5X - 2$ tiene a 1 como raíz doble y a 2 como raíz simple, ya que se factoriza en $\mathbb{Q}[X]$ como

$$P = (X - 1)^2(X - 2)$$

Una consecuencia inmediata de la definición

Corolario

Si P es un polinomio que tiene en K las raíces: $a_1, a_2, \ldots, a_r$ con multiplicidades $m_1, m_2, \ldots m_r$, entonces P admite la factorización

$$P(X) = (X - a_1)^{m_1}(X - a_2)^{m_2} \cdots (X - a_r)^{m_r} Q(X)$$

donde $Q(a_i) \neq 0$ para $0 \leq i \leq r$.

Ejemplo: consideremos $P = X^4 - 1$ en $\mathbb{R}[X]$. Tiene dos raíces simples en $\mathbb{R}$, 1 y -1 Se factoriza como:

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

donde el polinomio $X^4 + 1$ no se anula en $\mathbb{R}$.

Derivada de un polinomio

Definición

Sea $P \in K[X]$ un polinomio.

$$P = \sum_{k=0}^{n} a_k X^k$$

entonces, definimos el polinomio derivado P' por:

$$P' = \sum_{k=1}^{n} k a_k X^{k-1}$$

Esta noción de derivada puramente formal, conserva las propiedades usuales de la derivada, como la regla para derivar una suma o un producto:

$$(P+Q)' = P' + Q', \quad (P \cdot Q)' = P' \cdot Q + P \cdot Q'$$

Derivada n-ésima de un polinomio

Inductivamente, podemos definir también la derivada n-ésima $P^{(n)}$ del polinomio P de la siguiente manera:

$$\begin{cases} P^{(0)} &= P \\ P^{(n+1)} &= (P^n)' \end{cases}$$

Derivando un polinomio usando SageMath

```
sage: p=(x-1)^2*(x-2)
sage: expand(p)
x^3 - 4*x^2 + 5*x - 2
sage: expand(diff(p,x))
3*x^2 - 8*x + 5
sage: expand(diff(p,x,x))
6*x - 8
sage: expand(diff(p,x,x,x))
6
```

Fórmula de Taylor para polinomios

Haremos a partir de aquí la hipótesis de que K es un cuerpo de característica cero, Esto significa que

$$\overbrace{1+1+\cdots+1}^{n \text{ veces}} \neq 0 \text{ en } K$$

Esto se cumple si $K=\mathbb{Q}$, $K=\mathbb{R}$ o $K=\mathbb{C}$ pero no si $K=\mathbb{Z}_n$.

Teorema (Fórmula de Taylor para polinomios)

Si K es un cuerpo de característica cero y $P \in K[X]$ es un polinomio con $gr(P) \leq n$ y $a \in K$, tenemos que:

$$P(X)=\sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k$$

Notemos que esta fórmula es exacta: no hay resto.

Demostración de la fórmula de Taylor: Monomios

Para demostrar la fórmula de Taylor, primero la demostramos para monomios de la forma $P = X^m$. En este caso las derivadas de P valen:

$$P'(X) = mX^{m-1}$$

$$P^{(2)}(X) = m(m-1)X^{m-2}$$

$$P^{(3)}(X) = m(m-1)(m-2)X^{m-3}$$

y siguiendo de esta manera, podemos demostrar inductivamente que:

$$P^{(k)}(X) = m(m-1)(m-2)\dots(m-k+1)X^{m-k} \text{ si } k \leq m$$

mientras que

$$P^{(k)}(X) = 0 \text{ si } k > m$$

Demostración de la fórmula de Taylor: Monomios (2)

Entonces, recordando la expresión de los números combinatorios:

$$\binom{m}{k} = \frac{m(m-1)(m-2)\cdots(m-k+1)}{k!} \quad (0 \leq k \leq m)$$

y el teorema del binomio de Newton[1], vemos que:

$$\sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k = \sum_{k=0}^{m} \binom{m}{k} a^k (X-a)^k = (a+(X-a))^m = X^m$$

Con lo que hemos comprobado que la fórmula de Taylor es cierta para monomios.

[1] Aquí estamos utilizando el teorema del binomio aplicado a elemtos del anillo $K[X]$. En general, el teorema del binomio es válido en cualquier anillo conmutativo.

Demostración de la fórmula de Taylor: Caso general

Observamos que cualquier polinomio es una combinación lineal de potencias de X y que la expresión que aparece en el segundo miembro de la fórmula de Taylor es lineal en el polinomio P. Si

$$P = \sum_{i=0}^{m} a_i X_i$$

y notamos $P_i(X) = X^i$ entonces

$$\sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k = \sum_{k=0}^{n} \frac{1}{k!} \left(\sum_{i=0}^{m} a_i P_i^{(k)}(a) \right) (X-a)^k$$

$$= \sum_{i=0}^{m} a_i \left(\sum_{k=0}^{n} \frac{P_i^{(k)}(a)}{k!}(X-a)^k \right)$$

que por el caso anteriormente demostrado del teorema es:

$$= \sum_{i=0}^{m} a_i P_i(X) = P$$

Caracterización de la multiplicidad con derivadas

Teorema

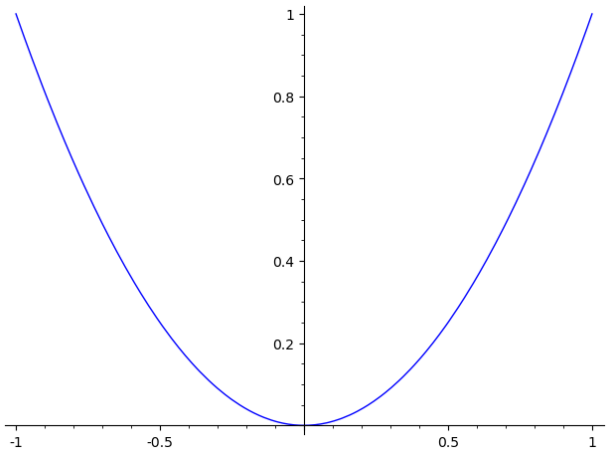
Sea $P \in K[X]$ un polinomio, y $a \in K$. Entonces, a es una raíz de P de multiplicidad m si y sólo si $P(a) = P'(a) = P^{(2)}(a) = \ldots = P^{(m-1)}(a) = 0$ pero $P^{(m)}(a) \neq 0$. Dicho de otro modo, la multiplicidad de a como raíz de P viene dada por el orden de la primer derivada de P que no se anula cuando la especializamos en $X = a$.

Raíces dobles de polinomios cuadráticos y derivadas

Volvamos a consideremos el polinomio cuadrático

$$P(X) = aX^2 + bX + c$$

Entonces $P'(X) = 2aX + b$, que se anula en $x_0 = \frac{-b}{2a}$. El teorema dice que tendremos una raíz doble ($m = 2$) en $x = x_0$ si y sólo si x_0 es raíz de P y de P'. ¡Cuando $K = \mathbb{R}$ podemos dibujarlo! x_0 es la coordenada x del vértice de la parábola que corresponde al polinomio P (¡es donde P alcanza su mínimo/máximo!) y será una raíz doble cuando dicho vértice esté sobre el eje x.

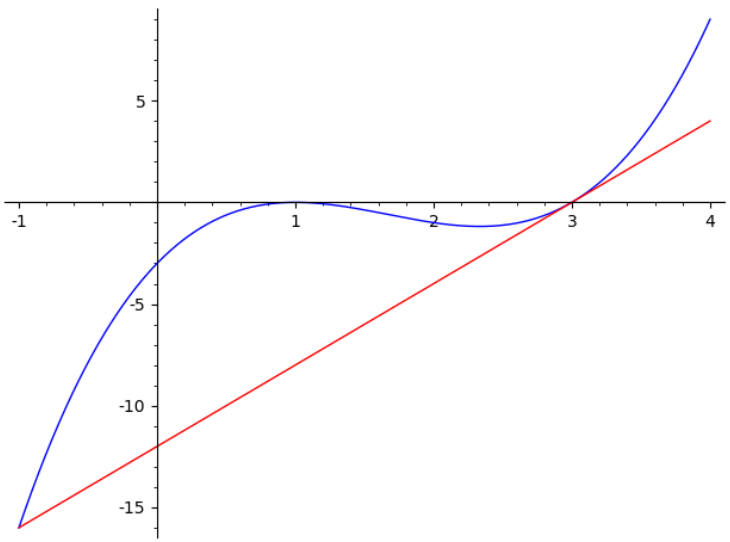


Ejemplo: $(X+1)^2 = X^2 + 2X + 1$ tiene una raíz doble en $x_0 = -1$.

Una ecuación cúbica

Consideremos el polinomio $P(X) = X^3 - 5X^2 + 7X - 3$. Entonces $P'(X) = 3X^2 - 10X + 7$ y $P^{(2)}(X) = 6X - 10$. Entonces $X = 1$ es raíz doble, pues $P(1) = 0$, $P'(1) = 0$ y $P''(1) = -4 \neq 0$. Mientras que 3 es raíz simple, ya que $P(3) = 0$ pero $P'(3) = 4 \neq 0$. En consecuencia, la factorización de P es:

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



Dibujamos este polinomio y su recta tangente en $x_0 = 3$ que es

$$Y = P(3) + P'(3)(X - 3) = 4X - 12$$

Vemos que en $X = 1$ (raíz doble) la recta tangente es horizontal mientras que en $x_0 = 3$ (raíz simple) no lo es.

Demostración del teorema sobre la multiplicidad (1)

Supongamos primero que $P(a) = P'(a) = P^{(2)}(a) = \ldots = P^{(m-1)}(a) = 0$ pero $P^{(m)}(a) \neq 0$. Entonces, utilizando la fórmula de Taylor tenemos que:

$$P(X) = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k = \sum_{k=m}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k$$

Entonces sacando un factor común $(X-a)^m$, podemos escribir

$$P(X) = (X-a)^m Q(X)$$

siendo $Q(X)$ el polinomio:

$$Q(X) = \sum_{k=m}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^{k-m}$$

y como

$$Q(a) = \frac{P^{(m)}(a)}{k!} \neq 0$$

deducimos que a es una raíz de multiplicidad m.

Demostración del teorema sobre la multiplicidad (2)

Ahora probaremos la afirmación recíproca, a saber que si a es una raíz de multiplicidad m, entonces: $P(a) = P'(a) = P^{(2)}(a) = \ldots = P^{(m-1)}(a) = 0$ pero $P^{(m)}(a) \neq 0$. Para ello, utilizaremos inducción en $m \in \mathbb{N}$:

Si $m = 1$, estamos suponiendo que a es una raíz simple de P, y tenemos la factorización:

$$P(X) = (X - a)Q(X)$$

con $Q(a) \neq 0$. En consecuencia, derivando con la regla del producto:

$$P'(X) = Q(X) + Q'(X)(X - a)$$

y cuando especializamos en $X = a$, obtenemos que:

$$P'(a) = Q(a) \neq 0$$

Demostración del teorema sobre la multiplicidad (3)

Ahora hagamos el paso inductivo: es decir supongamos que el teorema es cierto para raíces de multiplicidad $m-1$, y probemos que entonces también es verdadero para raíces de multiplicidad m.
Si a es una raíz de P de multiplicidad m, entonces P admite la factorización

$$P(X) = (X-a)^m Q(X) \text{ con } Q(a) \neq 0$$

Derivando nuevamente con la regla del producto:

$$P'(X) = m(X-a)^{m-1} Q(X) + (X-a)^m Q'(X)$$

Sacando factor común $(X-a)^{m-1}$, obtenemos:

$$P'(X) = (X-a)^{m-1} Q_1(X)$$

donde $Q_1(X) = mQ(X) + (X-a)Q'(X)$. Luego:

$$Q_1(a) = mQ(a) \neq 0$$

En consecuencia, a es raíz de multiplicidad $m-1$ de P'.

Demostración del teorema sobre la multiplicidad (4)

Luego, por hipótesis inductiva, las derivadas de P' se anulan en a hasta el orden $m-2$:

$$(P')'(a) = (P')^{(2)}(a) = \ldots = (P')^{(m-2)}(a) = 0$$

pero

$$(P')^{(m-1)}(a) \neq 0$$

Pero esto precisamente significa que:

$$P(a) = P'(a) = P^{(2)}(a) = \ldots = P^{(m-1)}(a) = 0$$

pero $P^{(m)}(a) \neq 0$. En virtud del principio de inducción, esto demuestra el teorema para todo $m \in \mathbb{N}$.

Otro ejemplo

Volvamos a mirar el polinomio $X^n - 1 \in \mathbb{C}[X]$, cuyas raíces son las raíces n-ésimas de la unidad

$$\omega_k = e^{\frac{2\pi ik}{n}} \quad k = 0, 1, 2, \ldots, n - ,1$$

Entonces como $P'(X) = nX^{n-1}$ y $P'(\omega_k) = n\omega_k^{n-1} \neq 0$, deducimos que las ω_k son raíces simples. Como dijimos en la clase anterior, P admite la factorización

$$P = \prod_{k=0}^{n-1} (X - \omega_k)$$

El Teorema Fundamental del Álgebra

Teorema (Teorema Fundamental del Álgebra)

Todo polinomio con coeficiente complejos $P \in \mathbb{C}[X]$ no constante, tiene alguna raíz en el cuerpo de los números complejos, es decir existe $\alpha \in \mathbb{C}$ tal que $P(\alpha) = 0$.

El Teorema Fundamental del Álgebra (2)

Corolario

Todo polinomio con coeficiente complejos

$$P = \sum_{k=0}^{n} a_k X^k \in \mathbb{C}[X] \ (a_i \in \mathbb{C}, a_n \neq 0)$$

no constante se factoriza como producto de polinomios lineales, en la forma:

$$P(X) = a_n(X - \alpha_1)^{m_1}(X - \alpha_2)^{m_2} \cdots (X - \alpha_r)^{m_r}$$

donde $\alpha_1, \alpha_2, \ldots, \alpha_r$ *son las distintas raíces complejas de* P, $m_1, m_2, \ldots, m_r$ *son las correspondientes multiplicidades, y* a_n *es el coeficiente principal del polinomio* P.

Demostración

Como vimos antes

$$P(X) = (X - \alpha_1)^{m_1}(X - \alpha_2)^{m_2} \dots (X - \alpha_r)^{m_r} Q(X)$$

donde $\alpha_1, \alpha_2, \dots \alpha_r$ son las raíces de P en $\mathbb{C}$ y $Q(\alpha_i) \neq 0$ para $0 \leq i \leq r$.
Afirmamos que Q debe ser constante: si suponemos que no, por 4, Q debe tener alguna raíz $\alpha \in \mathbb{C}$, pero toda raíz de Q es raíz de P. Luego $\alpha = \alpha_i$ para algún i, lo que es una contradicción pues $Q(\alpha_i) \neq 0$.
Como Q debe ser constante, al igualar los coeficientes principales de ambos miembros, deducimos que Q debe coincidir con el coeficiente principal de P.

El Teorema Fundamental del Álgebra (3)

Comparando los grados de ambos miembros, en la descomposición del corolario anterior deducimos que:

$$n = \text{gr}(P) = m_1 + m_2 + \ldots + m_r$$

Observemos que esta suma representa la cantidad de raíces de P, si contamos las raíces múltiples de acuerdo con su multiplicidad. Esto nos proporciona el siguiente corolario:

Corolario

Un polinomio $P \in \mathbb{C}[X]$ de grado n tiene exactamente n raíces complejas, si las contamos de acuerdo con su multiplicidad.

En particular, hemmo demostrado que en $\mathbb{C}[X]$ los únicos polinomios irreducibles son los lineales (de grado 1).

Un ejemplo

Miremos el polinomio $P = X^4 + 1$ cuando $K = \mathbb{C}$.
Como $X^4 + 1 = 0 \Leftrightarrow X^4 = -1$, sus raíces en $\mathbb{C}$ serán las raíces cuartas de -1.
Como $-1 = 1 \cdot e^{\pi i}$, estas raíces serán

$$\omega_k = e^{\frac{(2k+1)\pi i}{4}} \text{ para } k = 0, 1, 2, 3$$

$$\omega_0 = e^{\frac{\pi i}{4}} = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}\, i, \quad \omega_1 = e^{\frac{3}{4}\pi i} = -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}\, i$$

$$\omega_2 = e^{\frac{5}{4}\pi i} = -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}\, i \quad \omega_3 = e^{\frac{7}{4}\pi i} = \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}\, i$$

$$X^4 + 1 = (X - \omega_0)(X - \omega_1)(X - \omega_2)(X - \omega_3)$$

¡En la computadora!

Factorizando en $\mathbb{C}[X]$ usando SageMath

```
sage: CX=PolynomialRing(CC,"x")
sage: p=CX(x^4+1)
sage: p.roots()
[(-0.707106781186548 - 0.707106781186548*I, 1),
 (-0.707106781186548 + 0.707106781186548*I, 1),
 (0.707106781186548 - 0.707106781186548*I, 1),
 (0.707106781186548 + 0.707106781186548*I, 1)]
sage: p.factor()
(x - 0.707106781186548 - 0.707106781186548*I)
* (x - 0.707106781186548 + 0.707106781186548*I)
* (x + 0.707106781186548 - 0.707106781186548*I)
* (x + 0.707106781186548 + 0.707106781186548*I)
sage: sqrt(2.0)/2.0
0.707106781186548
```

Una observación

Notemos que las raíces del ejemplo anterior son exactamente las raíces primitvas de la unidad de orden 8, es decir $G_8^* = \{\alpha_0, \alpha_1, \alpha_2, \alpha_3\}$.
De hecho,

$$\omega_k = e^{\frac{(2k+1)\pi i}{4}} = e^{\frac{(2k+1)2\pi i}{8}} \text{ para } k = 0, 1, 2, 3$$

y cuando k recorre estos valores $2k + 1$ recorre los valores

$$\{1, 3, 5, 7\}$$

que son exactamente los enteros entre 1 y 7 que son coprimos con 8.

Complejos conjugados

Recordamos que si $z = a + bi$ es un número complejo, su complejo conjugado $\overline{z}$ se define por $\overline{z} = a - bi$. La operación de tomar el complejo conjugado tiene varias propiedades importantes:

1. $z = \overline{z}$ si y sólo si $z \in \mathbb{R}$
2. Si $z, w \in \mathbb{C}$ entonces

$$\overline{z + w} = \overline{z} + \overline{w}$$

$$\overline{z \cdot w} = \overline{z} \cdot \overline{w}$$

3. $z + \overline{z} = 2\mathrm{Re}(z)$ y $z \cdot \overline{z} = |z|^2$ son números reales.

Raíces complejas de polinomios cuadráticos

Recordemos que si $P = aX^2 + bX + c$ es un polinomio cuadrático con coeficientes reales y discriminante $\Delta = b^2 - 4ac$ negativo, P tiene dos raíces complejas conjugadas dadas por: siendo

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

y

$$\alpha_2 = \frac{-b - \sqrt{-\Delta}\, i}{2a}$$

Así pues, las raíces complejas de un polinomio cuadrático forman un par de raíces conjugadas.

Generalizando este hecho

Ahora generalizaremos este hecho a polinomios con coeficientes reales de mayor grado. Consideremos para ello un polinomio con coeficientes complejos:

$$P(X) = \sum_{i=0}^{n} a_k X^k \in \mathbb{C}[X]$$

y definimos el polinomio conjugado $\overline{P}$ por

$$\overline{P}(X) = \sum_{k=0}^{n} \overline{a_k}\, X^i$$

Como consecuencia de las propieedades antes mencionadas del conjugado, si $z \in \mathbb{C}$ tenemos que:

$$\overline{P(z)} = \overline{P}(\overline{z})$$

y si $P, Q \in \mathbb{C}[X]$ son polinomios:

$$\overline{P+Q} = \overline{P} + \overline{Q}, \quad \overline{P \cdot Q} = \overline{P} \cdot \overline{Q}$$

Generalizando este hecho (2)

En particular, si los coeficientes de P son reales (esto es $P \in \mathbb{R}[X]$), tendremos que $\overline{P} = P$, y resulta que:

$$\overline{P(z)} = P(\overline{z})$$

En particular si $P(z) = 0$, tenemos que $P(\overline{z}) = 0$, es decir, hemos demostrado que las raíces complejas de un polinomio con coeficientes reales se presentan de a pares de raíces conjugadas:

Proposición

Sea $P \in \mathbb{R}[X]$ un polinomio con coeficientes reales. Si $z = a + bi$ es una raíz de P, entonces su complejo conjugado $z = a - bi$ también es raíz de P

Raíces conjugadas y multiplicidad

Similarmente podemos demostrar,

Proposición

Sea $P \in \mathbb{R}[X]$ un polinomio con coeficientes reales. Si $z = a + bi$ es una raíz de P con multiplicidad m , entonces su complejo conjugado $z = a - bi$ también es raíz de P con multiplicidad m.

Demostración

Como z es raíz de P con multiplicidad m, P admite la factorización:

$$P(X) = (X - z)^m Q(X)$$

donde $Q(z) \neq 0$. Utilizando la operación de "tomar el polinomio conjugado" que definimos antes, tenemos:

$$\overline{P}(X) = \overline{(X - z)^m Q(X)} = \overline{(X - z)^m} \cdot \overline{Q}(X) = (X - \overline{z})^m \overline{Q}(X)$$

Pero como P tiene coeficientes reales, $\overline{P} = P$ y como

$$P(\overline{z}) = 0, \overline{Q}(\overline{z}) = \overline{Q(z)} \neq 0$$

esto dice que $\overline{z}$ es una raíz de P de multiplicidad m.

Fractorización en $\mathbb{R}[X]$

Podemos utilizar este hecho para obtener la factorización de un polinomio en $\mathbb{R}[X]$ a partir de su factorización compleja.

Sea como antes $P \in \mathbb{R}[X]$ y llamemos $\alpha_1, \alpha_2, \ldots \alpha_r$ a sus raíces reales (distintas). También consideremos sus raíces complejas (con parte imaginaria no nula), que por el razonamiento anterior, se presentan en pares de raíces conjugadas:

$$\beta_1, \overline{\beta_1}, \beta_2, \overline{\beta_2}, \ldots, \beta_s, \overline{\beta_s}$$

Por otra parte, llameos m_k a la multiplicidad de α_k como raíz de P y f_k a la multiplicidad de β_k como raíz de P (que por la proposición 2 también es la multiplicidad de $\overline{\beta_k}$. Entonces: P admite en $\mathbb{C}[X]$ la factorización dada

$$P = a_n(X-\alpha_1)^{m_1}(X-\alpha_2)^{m_2}\cdots(X-\alpha_r)^{m_r}$$
$$\cdot(X-\beta_1)^{f_1}(X-\overline{\beta_1})^{f_1}(X-\beta_2)^{f_2}(X-\overline{\beta_2})^{f_2}\cdots(X-\beta_s)^{f_2}(X-\overline{\beta_s})^{f_s}$$

Fractorización en $\mathbb{R}[X]$ (2)

Para obtener su factorización en $\mathbb{R}[X]$, debemos agrupar los factores correspondientes a cada par de raíces conjugadas: para ello observamos que

$$Q_{\beta_k}(X) = (X - \beta_k)(X - \overline{\beta_k}) = X^2 - 2\,\mathrm{Re}(\beta_k)X + |\beta_k|^2$$

es un polinomio cuadrático con coeficientes reales (y discriminante negativo, pues no tiene raíces reales).
En definitiva, hemos demostrado el teorema siguiente:

Teorema

Si $P \in \mathbb{R}[X]$ es un polinomio con coeficientes reales, entonces P admite la siguiente factorización en $\mathbb{R}[X]$:

$$P = a_n(X - \alpha_1)^{m_1}(X - \alpha_2)^{m_2} \cdots (X - \alpha_r)^{m_r} \cdot Q_{\beta_1}^{f_1} Q_{\beta_2}^{f_2} \cdots Q_{\beta_s}^{f_s}$$

donde a_n es el coeficiente principal de P, las α_k son las raíces reales de P y los Q_{β_i} son polinomios cuadráticos con coeficientes reales y discriminante negativo (correspondientes a cada par de raíces complejas de P).

Fractorización en $\mathbb{R}[X]$ (3)

En particular, vemos que en $\mathbb{R}[X]$ los polinomios irreducibles son los lineales (de grado 1) y los polinomios cuadráticos (de grado 2) con discriminante negativo.

Volvamos a mirar el ejemplo $P = X^4 + 1$

Y factoricémoslo en $\mathbb{R}[X]$. Recordamos que las raíces eran

$$\omega_0 = e^{\frac{\pi i}{4}} = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}\, i, \quad \omega_1 = e^{\frac{3}{4}\pi i} = -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}\, i$$

$$\omega_2 = e^{\frac{5}{4}\pi i} = -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}\, i \overline{\omega_1} \quad \omega_3 = e^{\frac{7}{4}\pi i} = \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}\, i = \overline{\omega_0}$$

$$X^4+1 = (X-\omega_0)(X-\omega_1)(X-\omega_2)(X-\omega_3) = (X^2-\sqrt{2}X+1)(X^2+\sqrt{2}X+1)$$

Cada uno de estos factores cuadráticos es irreducible en $\mathbb{R}[X]$ (ya que son polinomios cuadráticos sin raíces rales).

¡En la computadora!

Factorizando en $\mathbb{R}[X]$ usando SageMath

```
sage: RX=PolynomialRing(RR,"x")
sage: p=RX(x^4+1)
sage: p.roots()
[]
sage: p.factor()
(x^2 - 1.41421356237310*x + 1.00000000000000) *
(x^2 + 1.41421356237310*x + 1.00000000000000)
```

¿Y en $\mathbb{Q}[X]$?

En $\mathbb{Q}[X]$ el polinomio X^4+1 es irreducible, ya que si tuviera alguna factorización no trivial la misma serviría también en $\mathbb{R}[X]$. Pero la factorización como producto de irreducibles es única y vimos que en $\mathbb{R}$ es

$$X^4+1=(X^2-\sqrt{2}X+1)(X^2+\sqrt{2}X+1)$$

Dado que $\sqrt{2}\notin\mathbb{Q}$, esta factorización no sirve en $\mathbb{Q}[X]$.

Factorizando en $\mathbb{Q}[X]$ usando SageMath

```
sage: QX=PolynomialRing(QQ,"x")
sage: p=QX(x^4+1)
sage: p.factor()
x^4+1
```