El campo de los números complejos

Mario Pineda Ruelas
Departamento de Matemáticas,
Universidad Autónoma Metropolitana-Iztapalapa
correo electrónico: mpr@xanum.uam.mx

Gabriel D. Villa Salvador
Departamento de Control Automático,
Centro de Investigación y de Estudios Avanzados, IPN
correo electrónico gvilla@ctrl.cinvestav.mx

1 Introducción

Si $a, b \in \mathbb{N}$, entonces la ecuación $x + a = b$ no siempre tiene solución en $\mathbb{N}$. Esta es una buena razón para extender al sistema de los números naturales $\mathbb{N}$ a otro sistema en el cual ecuaciones de la forma $x + a = b$ tengan solución. Así, usando una relación de equivalencia $\sim$ en el conjunto $\mathbb{N} \times \mathbb{N}$ y considerando el conjunto cociente $\mathbb{N} \times \mathbb{N}/\sim$ se construye el anillo de los enteros $\mathbb{Z}$ y se puede verificar fácilmente que las ecuaciones $x + a = b$ tienen solución en $\mathbb{Z}$. Sin embargo, $\mathbb{Z}$ también tiene su inconveniente. Si $a, b \in \mathbb{Z}$, entonces no todas las ecuaciones de la forma $ax = b$ tienen solución. Nuevamente, por medio de una relación de equivalencia $\sim$ en el conjunto $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ se construye el campo de los números racionales $\mathbb{Q}$ y aquí, las ecuaciones $ax = b$ se pueden resolver. Todos sabemos que si p es un número primo positivo, entonces $\sqrt{p}$ es un número irracional y por lo tanto la ecuación $x^2 = p$ no es soluble en $\mathbb{Q}$. Usando una relación de equivalencia en el conjunto de sucesiones de Cauchy de números racionales se construye al campo de los números reales $\mathbb{R}$ y en $\mathbb{R}$, las ecuaciones de la forma $x^2 = a$ con $a \geq 0$ tienen solución. Sin embargo, la ecuación $x^2 = -1$ no es soluble en $\mathbb{R}$. Aprovecharemos este *afortunado* suceso como pretexto para *agrandar* al campo de los números reales y para tener la garantía de poder resolver cualquier ecuación polinomial.

El objetivo fundamental de este capítulo es el de construir al campo de los números complejos $\mathbb{C}$, estudiar su aritmética, resolver cierto tipo de ecuaciones y como platillo principal, daremos una demostración del Teorema Fundamental del Álgebra sin usar el lenguaje del análisis complejo.

Vamos a suponer que el lector está familiarizado con las propiedades elementales de los números reales y con el concepto de continuidad de funciones de $\mathbb{R}^2$ en $\mathbb{R}^2$.

2 Aritmética de los complejos

Consideremos el plano cartesiano $\mathbb{R} \times \mathbb{R} = \{(a, b) : a, b \in \mathbb{R}\}$. En este conjunto definimos la suma y producto de pares ordenados como:

$$(a, b) + (x, y) = (a + x, b + y), \quad (a, b)(x, y) = (ax - by, ay + bx).$$

Teorema 2.1. *$\mathbb{R} \times \mathbb{R}$ con la suma y producto antes definidos, es un campo.*

Demostración: La asociatividad y conmutatividad de la suma son evidentes. El elemento $(0, 0)$ es el neutro aditivo. Si $(a, b) \in \mathbb{R} \times \mathbb{R}$, entonces $(-a, -b)$ es el inverso aditivo de (a, b).

El producto es asociativo y conmutativo. También, un simple cálculo muestra que $(1, 0)(x, y) = (x, y)$. Por lo tanto, el elemento $(1, 0)$ es el neutro multiplicativo. Si $(a, b) \neq (0, 0)$, entonces a ó b es $\neq 0$. Supongamos que al menos $a \neq 0$. Queremos ver que (a, b) tiene un inverso multiplicativo en $\mathbb{R} \times \mathbb{R}$. Sea $(x, y) \in \mathbb{R} \times \mathbb{R}$ tal que

$$(a, b)(x, y) = (ax - by, ay + bx) = (1, 0).$$

Resolviendo el sistema de ecuaciones

$$\begin{aligned} ax - by &= 1 \\ bx + ay &= 0, \end{aligned}$$

obtenemos que $x = \dfrac{a}{a^2 + b^2}$, $y = \dfrac{-b}{a^2 + b^2}$. Por lo anterior, si $(a, b) \neq (0, 0)$, entonces $(a, b)^{-1} = \left(\dfrac{a}{a^2 + b^2}, \dfrac{-b}{a^2 + b^2}\right)$.

La propiedad distributiva la dejamos como ejercicio.

□

Definición 2.2. *El conjunto $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ junto con la suma y producto definidos anteriormente se llama el campo de los números complejos.*

El término *plano complejo* se usa frecuentemente para referirse a los puntos de $\mathbb{R} \times \mathbb{R}$ vistos como números complejos.

Una observación importante es que en cualquier campo el neutro aditivo, el neutro multiplicativo, el inverso aditivo y el inverso multiplicativo son únicos con respecto a la propiedad que los define.

Teorema 2.3. *Consideremos La función $f : \mathbb{R} \to \mathbb{C}$ definida como $f(x) = (x, 0)$. Entonces:*

1. *f es inyectiva.*
2. *$f(x + y) = f(x) + f(y)$.*
3. *$f(xy) = f(x)f(y)$.*

Demostración: Es un fácil ejercicio para el lector.

□

Puesto que cualquier función es suprayectiva en su imagen, entonces el teorema anterior nos dice que el campo $\mathbb{C}$ contiene una copia de $\mathbb{R}$, de tal forma que sumar y multiplicar en $\mathbb{R}$ es equivalente a sumar y multiplicar en $f(\mathbb{R})$. Concretamente, estamos identificando a los números reales con el conjunto $\{(x, 0)\} \subset \mathbb{C}$. Más adelante veremos otras bondades de nuestro flamante campo.

Definición 2.4. *Si $z = (x, y) \in \mathbb{C}$, entonces x se llama la parte real de z y y se llama la parte imaginaria.*

Escribiremos $Re(z)$ y $Im(z)$ para indicar la parte real e imaginaria de z.

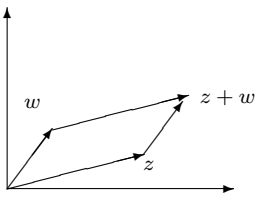
Sea $i = (0, 1)$. Entonces $i^2 = (-1, 0)$. Esto significa que la ecuación $x^2 = -1$ tiene solución en $\mathbb{C}$. Si $(x, y) \in \mathbb{C}$, entonces

$$(x, y) = (x, 0) + (0, y) = (x, 0) + (y, 0)(0, 1).$$

Según el teorema anterior, $(x, 0)$ y $(y, 0)$ los podemos identificar con los números reales x, y respectivamente. Por lo tanto, $(x, y) = x + yi$, donde $i = (0, 1)$ satisface $i^2 = -1$. En la definición 2.4 tenemos que si $z = x + yi$, entonces x es la parte real y y es la parte imaginaria de z. Esta forma de escribir al número complejo (x, y) como $x + yi$ es más cómoda. Así, la suma y poducto quedan establecidos como:

1. $(x + yi) + (a + bi) = (x + a) + (y + b)i$,
2. $(x + yi)(a + bi) = (xa - yb) + (xb + ya)i$.

Sean z, $w \in \mathbb{C}$. Es claro que $z + w$ coincide con la suma de los vectores que salen del origen $(0, 0)$ y que terminan en z y w respectivamente.



Uno de los problemas que nos motivaron a extender el campo de lo números reales es que la familia de ecuaciones $x^2 = a$ con $a < 0$ no son solubles en $\mathbb{R}$.

Definición 2.5. *Sea $z \in \mathbb{C}$. Diremos que w es una raíz cuadrada de z si $w^2 = z$.*

Teorema 2.6. *Cualquier número complejo $z = a + ib$ tiene al menos una raíz cuadrada.*

Demostración: Sea $x + iy$ tal que $(x + yi)^2 = a + bi$. Veamos que podemos escribir x y y en términos de z. Tenemos el siguiente sistema de ecuaciones:

$$\begin{aligned} x^2 - y^2 &= a \\ 2xy &= b. \end{aligned}$$

Por lo tanto $(x^2 + y^2)^2 = (x^2 - y^2)^2 + 4x^2y^2 = a^2 + b^2$ y así $x^2 + y^2 = \sqrt{a^2 + b^2}$. Sumando y restando nuestra última igualdad con la primera ecuación del sistema tenemos que:

$$\begin{aligned} x^2 &= \frac{1}{2}\big(a + \sqrt{a^2 + b^2}\big) \geq 0 \\ y^2 &= \frac{1}{2}\big(-a + \sqrt{a^2 + b^2}\big) \geq 0. \end{aligned}$$

Por lo tanto

$$\begin{aligned} x &= \pm\sqrt{\frac{1}{2}\big(a + \sqrt{a^2 + b^2}\big)} \\ y &= \pm\sqrt{\frac{1}{2}\big(-a + \sqrt{a^2 + b^2}\big)}. \end{aligned}$$

Aparentemente tenemos dos valores para x y dos valores para y. La segunda ecuación de nuestro sistema original nos indica como debemos escoger a x y y pues el producto xy debe tener el mismo signo que b.

□

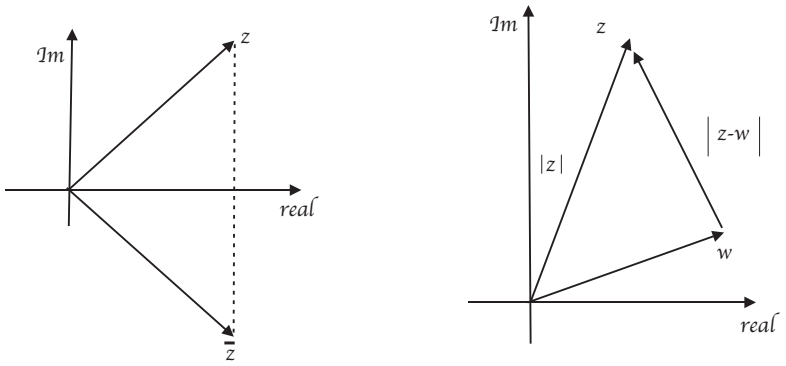
Ejemplo 2.7. *Sea $z = 3+4i$. Siguiendo la prueba del teorema anterior tenemos:*

$$x = \pm\sqrt{\frac{1}{2}\big(3+\sqrt{3^2+4^2}\big)} = 2$$
$$y = \pm\sqrt{\frac{1}{2}\big(-3+\sqrt{3^2+4^2}\big)} = 1.$$

Puesto que $xy > 0$, *claramente* $2+i$ *y* $-2-i$ *satisfacen*

$$(2+i)^2 = (-2-i)^2 = 3+3i.$$

Definición 2.8. *Si* $z = x+yi$, *entonces el conjugado de* z *es* $\overline{z} = x-yi$. *El número* $|z| = \sqrt{x^2+y^2}$ *es el módulo o norma de* z.



Geométricamente, $|z| = \sqrt{x^2+y^2}$ es la distancia del origen $(0,0)$ al punto $z = x+yi$. Es claro entonces que la distancia entre z y w es $|z-w|$.

Teorema 2.9. *Si* $z, w \in \mathbb{C}$, *entonces:*

1. $\overline{\overline{z}} = z$.
2. $\overline{z+w} = \overline{z} + \overline{w}$.
3. $\overline{zw} = \overline{z}\,\overline{w}$.
4. $z\overline{z} = |z|^2$.
5. $z = \overline{z}$ *si y sólo si* $z \in \mathbb{R}$.
6. $2Re(z) = z+\overline{z}$, $2iIm(z) = z-\overline{z}$.

7. $\overline{z^{-1}} = \overline{z}^{-1}$.

8. $z^{-1} = \dfrac{\overline{z}}{|z|^2}$.

9. $\overline{\left(\dfrac{w}{z}\right)} = \dfrac{\overline{w}}{\overline{z}}$.

Demostración: Es un fácil ejercicio de 1 a 6. Así que sólo demostraremos 7,8 y 9. Si $z \neq 0$, entonces por el inciso 3 tenemos que $1 = \overline{zz^{-1}} = \overline{z}\,\overline{z^{-1}}$. Por lo tanto $\overline{z^{-1}} = \overline{z}^{-1}$.

Para el inciso 8 notemos que gracias a que el inverso multiplicativo de z es único, entonces por 4 tenemos que $z\dfrac{\overline{z}}{|z|^2} = 1$. Así que necesariamente $z^{-1} = \dfrac{\overline{z}}{|z|^2}$.

Para la parte final notemos que $\dfrac{w}{z} = wz^{-1}$. Usando 3 y 8 obtenemos 9.

□

Teorema 2.10. *Sean $z, w \in \mathbb{C}$. Entonces:*

1. $|z| = 0$ *si y sólo si* $z = 0$.
2. $|z| = |\overline{z}|$.
3. $|zw| = |z||w|$.
4. *Si $z \neq 0$, entonces $|z^{-1}| = |z|^{-1}$. En particular,* $\left|\dfrac{w}{z}\right| = \dfrac{|w|}{|z|}$.
5. $|Re(z)| \leq |z|$ *y* $|Im(z)| \leq |z|$.
6. $|z + w| \leq |z| + |w|$.

Demostración: Los incisos 1, 2 y 3 son evidentes. El inciso 4 es consecuencia del inciso 7 del Teorema 2.9 y del inciso 3. En el inciso 5, $|Re(z)|$ indica el valor absoluto de $Re(z)$ y se sigue directamente si recordamos que la función raíz cuadrada es creciente. Así que sólo nos queda justificar la parte 6. Primero observemos que

$$|z + w|^2 = (z + w)\overline{(z + w)} = (z + w)(\overline{z} + \overline{w}) = z\overline{z} + z\overline{w} + w\overline{z} + w\overline{w}.$$

Pero $z\overline{w} = \overline{\overline{z}w}$, así $Re(z\overline{w}) = \dfrac{z\overline{w} + \overline{z}w}{2}$. Por lo tanto, usando el inciso 5 de este teorema tenemos

$$|z + w|^2 = z\overline{z} + z\overline{w} + w\overline{z} + w\overline{w} = |z|^2 + 2Re(z\overline{w}) + |w|^2 \leq |z|^2 + 2|z\overline{w}| + |w|^2,$$

así $|z+w|^2 \leq |z|^2+2|zw|+|w|^2 = (|z|+|w|)^2$, y por lo tanto $|z+w| \leq |z|+|w|$.

□

PROBLEMAS

1. Demostrar la asociatividad, conmutatividad de la suma y producto en $\mathbb{C}$.

2. Demostrar la propiedad distributiva en $\mathbb{C}$.

3. Demostrar el Teorema 2.1.

4. Usando los números complejos como pares ordenados de números reales, resolver la ecuación $x^2 = a$ con $a \in \mathbb{R}$ y $a < 0$.

5. Realizar las siguientes operaciones:

   a) $(-2 - 5i)(3 + i)$.

   b) $2i - (-3 + 2i)$.

   c) $(2 + 3i)(4 + i)$.

   d) $i^7 + i^{28}$.

6. Escribir en la forma $a + bi$ los siguientes números complejos:

   a) $\dfrac{1}{i}$.

   b) $\dfrac{2 + 3i}{-5 - i}$.

   c) $1 + \left(\dfrac{1}{1 + i}\right)^2$.

   d) $(-i)^n$ si $n \in \mathbb{N}$.

   e) $\dfrac{1}{-i} + \dfrac{i}{-1 + 2i}$.

   f) $\dfrac{1}{(8 + 6i)^2}$.

   g) $\dfrac{-i + 1}{i - 1} + \dfrac{i^4 + i^6 + i^8}{i + i^3 + i^5} - i$.

7. Sea $z = a + bi$. Encontrar $Re(z)$ y $Im(z)$ en las siguientes expresiones:

   a) $\dfrac{1}{z^2}$.

   b) $\dfrac{z + 1}{2z - 5}$.

   c) z^5.

8. Si $n \in \mathbb{Z}$, entonces $i^{4n} = 1,\ i^{4n+1} = i,\ i^{4n+2} = -1,\ i^{4n+3} = -i$.

9. Encontrar el conjugado de cada uno de los siguientes números y escribirlo en la forma $a + bi$.

   a) $\dfrac{1 - 2i}{4 + i}$.

b) $\dfrac{i}{1-2i}$.

c) $\dfrac{-x+yi}{x-yi}$.

10. Describir geométricamente los siguientes conjuntos:

    a) $\{z \in \mathbb{C} : |z-(4+i)| < 5\}$.

    b) $\{z \in \mathbb{C} : Im(z-2) = 0\}$.

    c) $\{z \in \mathbb{C} : Re(z) = 1\}$.

    d) $\{z \in \mathbb{C} : |z-(1+i)| + |z-(-1-i)| = 4\}$.

    e) $\{z \in \mathbb{C} : |z-(1+2i)| - |z-(-1+2i)| = 6\}$.

    f) $\{z \in \mathbb{C} : Re(z)Im(z) > 0\}$.

    g) $\{z \in \mathbb{C} : 2 < |z| \leq 4\}$.

11. Encontrar $z, w \in \mathbb{C}$ tales que:

    a) $z + iw = 1$.

    b) $iz + w = 1 + i$.

    c) $(2+i)z - iw = 2 - i$.

12. Encontrar una solución de la ecuación $\overline{z}^2 = z^2$.

13. (Teorema del Binomio). Sean $z, w \in \mathbb{C}$. Usar inducción para demostrar que si $n \in \mathbb{N}$, entonces:

$$(z+w)^n = \sum_{j=0}^{n} \binom{n}{j} z^{n-j} w^j$$

    donde $\binom{n}{j} = \dfrac{n!}{j!(n-j)!}$.

14. Usar el Teorema 2.6 para encontrar la raíz cuadrada de los siguientes números:

    a) $2i$.

    b) $3 - 9i$.

    c) $\cos\dfrac{\pi}{3} + i\,\mathrm{sen}\,\dfrac{\pi}{3}$.

15. Interpretar geométricamente $|z-w|$.

16. Encontrar los números complejos z, w que satisfacen $|z-w| \leq |z+w|$.

17. Verificar geométricamente que $(\cos\dfrac{\pi}{3} + i\,\mathrm{sen}\,\dfrac{\pi}{3})^n$, $n = 1, ..., 6$, son los vértices de un polígono regular inscrito en un circunferencia de radio 1.

18. Sea $z, r \in \mathbb{C} \setminus \{0\}$ tal que $Im(r) = 0$. Interpretar geométricamente el producto zr.

19. Sean $a, b, c \in \mathbb{C}$. Demostrar que si $a \neq 0$, la fórmula cuadrática usual resuelve la ecuación $az^2 + bz + c = 0$.

20. Resolver las siguientes ecuaciones:

    a) $x^2 + x + 1 = 0$
    b) $2z^2 + z + 1 = 0$.
    c) $(1 - i)z^2 + iz + 4 - i = 0$.

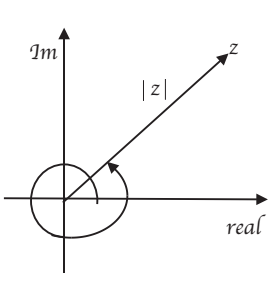
21. No todo es miel en la vida. Demostrar que el orden usual de $\mathbb{R}$ no puede ser extendido al campo $\mathbb{C}$. Sugerencia: Si así fuera, entonces $i > 0$ ó $i < 0$.

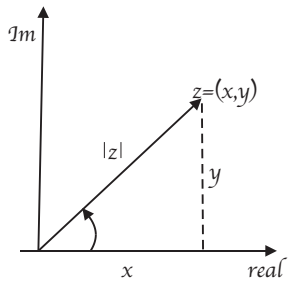
2.1 Raíces n-ésimas de un complejo

En el Teorema 2.6 demostramos, usando sólo las operaciones elementales de $\mathbb{C}$, que cualquier número complejo tiene raíz cuadrada. Usar ese método algebraico para demostrar que cualquier número complejo tiene raíces n-ésimas para cualquier entero positivo n, sería muy complicado pues nos llevaría a resolver un sistema algebraico de ecuaciones. En su lugar, vamos a dar la forma polar de un complejo, lo cual nos permitirá de paso, interpretar el producto y por lo tanto cualquier potencia entera de un número complejo.

Sea $z = (x, y) \in \mathbb{C}$. Observemos que z está determinado en forma única por el ángulo α que forma con la dirección positiva del eje real y por $|z|$, donde $0 \leq \alpha < 2\pi$. Sabemos que si sumamos múltiplos de 2π a α, aún tendremos el mismo número z. De la trigonometría básica tenemos que $x = |z| \cos \alpha$ y $y = |z| \operatorname{sen} \beta$. Por lo tanto podemos escribir $z = |z|(\cos \alpha + i \operatorname{sen} \alpha)$.

La expresión anterior se conoce como la representación polar de z. El ángulo α se conoce como el argumento de z y lo denotaremos $arg(z) = \alpha$.





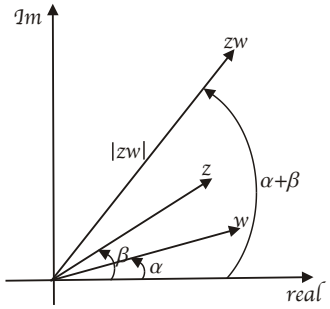
En particular, si $arg(z) = \alpha$, entonces $arg(\overline{z}) = 2\pi - \alpha$ y por lo tanto, si $z \neq 0$, entonces la representación polar de z^{-1} es

$$z^{-1} = |z|^{-1}((\cos(2\pi - \alpha) + i \operatorname{sen}(2\pi - \alpha)) = |z|^{-1}(\cos(-\alpha) + i \operatorname{sen}(-\alpha)).$$

Ahora podemos deducir una expresión para el producto. Si $z = |z|(\cos\alpha + i\,\mathrm{sen}\,\alpha)$ y $w = |w|(\cos\beta + i\,\mathrm{sen}\,\beta)$, entonces

$$\begin{aligned} zw =& |z||w|((\cos\alpha\cos\beta - \mathrm{sen}\,\alpha\,\mathrm{sen}\,\beta) + i(\cos\alpha\,\mathrm{sen}\,\beta + \mathrm{sen}\,\alpha\cos\beta)) \\ =& |z||w|(\cos(\alpha+\beta) + i\,\mathrm{sen}\,(\alpha+\beta)). \end{aligned}$$

Esta expresión es muy útil pues nos proporciona una interpretación geométrica del producto: el producto de z y w es el complejo cuya norma es $|z||w|$ y con argumento la suma de los argumentos de z y w.



También notemos que si $w \neq 0$, entonces

$$\begin{aligned} \frac{z}{w} = zw^{-1} =& |z|(\cos\alpha + i\,\mathrm{sen}\,\alpha)|w|^{-1}(\cos(-\beta) + i\,\mathrm{sen}\,(-\beta)) \\ =& \frac{|z|}{|w|}(\cos(\alpha-\beta) + i\,\mathrm{sen}\,(\alpha-\beta)). \end{aligned}$$

Teorema 2.11. [Teorema de D'Moivre] *Si* $z = |z|(\cos\alpha + i\,\mathrm{sen}\,\alpha) \neq 0$ *y* $n \in \mathbb{Z}$, *entonces* $z^n = |z|^n(\cos n\alpha + i\,\mathrm{sen}\,n\alpha)$.

Demostración: Haremos inducción para el caso $n > 0$. Si $n = 1$ el resultado es evidente. Supongamos que $z^n = |z|^n(\cos n\alpha + i\,\mathrm{sen}\,n\alpha)$. Entonces

$$\begin{aligned} z^{n+1} = z^n z =& |z|^n(\cos n\alpha + i\,\mathrm{sen}\,n\alpha)|z|(\cos\alpha + i\,\mathrm{sen}\,\alpha) \\ =& |z|^{n+1}(\cos(n\alpha+\alpha) + i\,\mathrm{sen}\,(n\alpha+\alpha)) \\ =& |z|^{n+1}(\cos((n+1)\alpha) + i\,\mathrm{sen}\,((n+1)\alpha)), \end{aligned}$$

y por lo tanto el teorema es cierto para $n \in \mathbb{N}$. Si $n < 0$ tenemos

$$\begin{aligned} z^n = (z^{-1})^{-n} =& |z|^n(\cos((-n)(-\alpha)) + i\,\mathrm{sen}((-n)(-\alpha))) \\ =& |z|^n(\cos n\alpha + i\,\mathrm{sen}\, n\alpha). \end{aligned}$$

□

Definición 2.12. *Sea $z \in \mathbb{C}$ y $n \in \mathbb{N}$. Diremos que w es una raíz n-ésima de z si $w^n = z$.*

Teorema 2.13. *Si $z \neq 0$ y $n \in \mathbb{N}$, entonces z tiene exactamente n raíces n-ésimas.*

Demostración: Sea $w = |w|(\cos\beta + i\,\mathrm{sen}\,\beta)$ y $z = |z|(\cos\alpha + i\,\mathrm{sen}\,\alpha)$ tal que $w^n = z$. De la igualdad

$$w^n = |w|^n(\cos n\beta + i\,\mathrm{sen}\, n\beta) = |z|(\cos\alpha + i\,\mathrm{sen}\,\alpha)$$

se sigue directamente que $|w| = |z|^{\frac{1}{n}}$ y $n\beta,\ \alpha$ difieren por un múltiplo entero de 2π. Lo anterior significa que $\beta = \dfrac{\alpha + 2k\pi}{n}$. Observemos que por el algoritmo de la división $k = nq + r$ con $0 \leq r < n$. Así tenemos

$$\beta = \frac{\alpha + 2k\pi}{n} = \frac{\alpha + 2(nq + r)\pi}{n} = \frac{\alpha + 2r\pi}{n} + 2q\pi$$

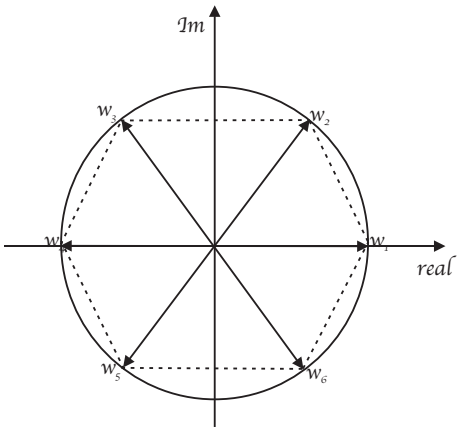
y por lo tanto es suficiente considerar los valores $k = 0, 1, ..., n-1$. Supongamos que para $0 \leq j, l \leq n-1$ se tiene $\dfrac{\alpha + 2j\pi}{n} = \dfrac{\alpha + 2l\pi}{n}$. Es claro entonces que $j = l$ y por lo tanto los valores de β son diferentes cuando $j \neq l$ y $0 \leq j, l \leq n-1$. □

El Teorema 2.13 describe en forma explícita la manera de encontrar las raíces n-ésimas de cualquier número complejo. Un caso particularmente importante es el de las raíces n-ésimas de 1. Observemos que si n es un entero par, entonces la ecuación $x^n = 1$ sólo tiene en $\mathbb{R}$ las soluciones $1, -1$. Si n es impar, entonces $x^n = 1$ sólo tiene una solución.

Ejemplo 2.14. *Según el teorema anterior, si $z = 1(\cos 0 + i\,\mathrm{sen}\,0)$, entonces los números*

$$w_k = \cos\frac{2k\pi}{n} + i\,\mathrm{sen}\,\frac{2k\pi}{n}, \quad 0 \leq k \leq n-1,$$

son las n-raíces diferentes de la unidad. Geométricamente lo que obtenemos es un polígono inscrito en una circunferencia de radio 1 con centro en el origen del plano complejo.



Teorema 2.15. *Sea* $\mu_n = \{w \in \mathbb{C} : w^n = 1\}$. *Si* $w_1, w_2 \in \mu_n$, *entonces* $w_1 w_2 \in \mu_n$ *y* $w_1^{-1} \in \mu_n$. *Si* $w_1 = \cos\dfrac{2\pi}{n} + i \operatorname{sen}\dfrac{2\pi}{n}$ *y* $w \in \mu_n$, *entonces existe* $k \in \mathbb{N}$ *tal que* $w = w_1^k$.

Demostración: Es claro que $(w_1 w_2)^n = (w_1^{-1})^n = 1$ y así $w_1 w_2$, $w_1^{-1} \in \mu_n$. La última parte se sigue de observar que por el ejemplo 2.14, necesariamente w es de la forma

$$\cos\frac{2k\pi}{n} + i \operatorname{sen}\frac{2k\pi}{n}$$

para algún $0 \leq k \leq n-1$. Por el Teorema de D'Moivre tenemos que $w = w_1^k$. □

La parte final del teorema anterior nos dice que cualquier elemento de μ_n es una potencia de w_1. El conjunto μ_n es un grupo cíclico de orden n y cualquier grupo cíclico con n elementos debe tener la *misma forma* que $\mathbb{Z}_n$.

PROBLEMAS

1. Escribir los siguientes números complejos en su forma polar:
   a) $-1 - i$.
   b) $\sqrt{3} + i$.
   c) $2 - 2i$.
   d) $\cos 26^o + i \operatorname{sen} 26^o$.
   e) $\dfrac{(a+bi)^n}{(x+yi)^m}$, con $n, m \in \mathbb{N}$.
2. Sea $z = |z|(\cos\alpha + i \operatorname{sen}\alpha)$. Demostrar que:

a) $\overline{z} = |z|(\cos(2\pi - \alpha) + i \operatorname{sen}(2\pi - \alpha))$.

b) $-z = |z|(\cos(\pi + \alpha) + i \operatorname{sen}(\pi + \alpha))$.

3. Encontrar el conjunto de soluciones de cada una de las siguientes ecuaciones y graficarlas:

   a) $w^8 = 1$.

   b) $w^6 = -1$.

   c) $w^4 = i$.

   d) $w^6 = -i$.

   e) $w^5 = 1 + i$.

   f) $w^6 = -2 + i$.

   g) $w^7 = 3 - 2i$.

4. En el ejercicio anterior ¿qué conjunto de soluciones de alguna de las ecuaciones satisface el Teorema 2.15?

5. Usar el Teorema de D'Moivre o el Teorema del Binomio para calcular las siguientes potencias:

   a) $(-1 - i)^9$.

   b) $(1 - i)^{12}$.

   c) $\left(\frac{-1}{2} - \frac{\sqrt{3}}{2}\right)^6$.

   d) $(\cos 35^o - i \operatorname{sen} 35^o)^{-25}$.

   e) $(2 + i)^n$.

6. Sea $a \neq 0$. Para encontrar las soluciones de la ecuación $az^2 + bz + c = 0$ utilizamos la fórmula $\dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$. El Teorema 2.13 nos afirma que el número $b^2 - 4ac$ tiene dos raíces cuadradas w_1, w_2. Entonces, para cada uno de estos números, la fórmula $\dfrac{-b \pm w_i}{2a}$, $i = 1, 2$ proporciona dos soluciones de $az^2 + bz + c = 0$. Aparentemente tenemos cuatro soluciones. ¿Qué está pasando? ¿cuál es el detalle fino que se debe aclarar? ¿sólo alguna de las w_i nos sirve?

7. Encontrar las raíces sextas de $3 + 2i$ y graficarlas. ¿Se nota algún parecido geométrico con las raíces sextas de 1?

8. Sea $n > 1$ tal que $\displaystyle\sum_{d|n} d > n$. Demostrar que si $d \mid n$ y $x^d = 1$, entonces $x^n = 1$. Puesto que para cada d existen exactamente d raíces de 1, entonces aparentemente existen al menos $\displaystyle\sum_{d|n} d$ raíces n-ésimas de 1. ¿En qué contradice esto al Teorema 2.13?

9. Sea $z, v \in \mathbb{C}$ tal que $v^n = z$ y $w_1 = \cos\dfrac{2\pi}{n} + i\,\text{sen}\,\dfrac{2\pi}{n}$ la raíz que aparece en el Teorema 2.15. Demostrar que $v, w_1 v, w_1^2 v, ..., w_1^{n-1} v$ son las raíces n-ésimas de z.

10. Sea w una raíz n-ésima de 1. Si w satisface que $w^m \neq 1$ para $0 < m < n$, entonces w se llama *n-raíz primitiva de la unidad*. Demostrar que:

    a) El número w_1 que aparece en el Teorema 2.15 es una n-raíz primitiva de 1.

    b) Si w es una n-raíz primitiva de 1, entonces $1, w, w^2, ..., w^{n-1}$ son todas las raíces n-ésimas de 1.

    c) Si w es una n-raíz primitiva de 1, entonces w^l es una n-raíz primitiva de 1 si y sólo si n, l son primos relativos.

    d) Concluir que 1 tiene $\varphi(n)$-raíces primitivas, donde $\varphi(n)$ es la función de Euler.

    e) Si w es una n-raíz primitiva de 1, entonces $1 + w + \cdots + w^{n-1} = 0$.

11. Sea $w_1 = \cos\dfrac{2\pi}{n} + i\,\text{sen}\,\dfrac{2\pi}{n}$ y $f : \mu_n \to \mathbb{Z}_n$ definida como $f(w_1^k) = k$. Demostrar que f es biyectiva y $f(w_1^k w_1^j) = f(w_1^k) + f(w_1^j)$.

12. El plano complejo está dividido de manera natural en cuatro cuadrantes. Para $k = 1, 2, 3, 4$, formalmente z está en el k-ésimo cuadrante si y sólo si $\dfrac{(k-1)\pi}{2} \leq arg(z) < \dfrac{k\pi}{2}$. El lector entiende muy bien qué significa que dos números complejos se encuentran en cuadrantes opuestos. Si z se encuentra en el cuadrante j escribimos $c(z) = j$. Entonces z y w están en cuadrantes opuestos si y sólo si $|c(z) - c(w)| = 2$. Justificar geométricamente que si z, w están en cuadrantes opuestos, entonces $|z|, |w| \leq |z - w|$. ¿Es cierta la afirmación inversa?

3 Divisibilidad en $\mathbb{F}[x]$

En el Capítulo 2, sección 2.5, estudiamos las raíces de polinomios con coeficientes en un campo finito $\mathbb{F}_p$. En esta sección vamos a estudiar polinomios con coeficientes en $\mathbb{C}$ o en algunos casos, con coeficientes en $\mathbb{Z}, \mathbb{Q}$ ó $\mathbb{R}$, sus raíces y principalmente las propiedades algebraicas que tales estructuras tienen. Notaremos la similitud con el anillo de los enteros $\mathbb{Z}$.

En este momento, sólo conocemos los campos $\mathbb{F}_p, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. En realidad existe una gran variedad de campos, por ejemplo, si p es un número primo, entonces

$$\mathbb{Q}(\sqrt{p}) = \{a + b\sqrt{p} \,:\, a, b \in \mathbb{Q}\}$$

es un campo con las operaciones usuales de los números reales o complejos. Se puede mostrar fácilmente que si $p_1 \neq p_2$ son dos primos diferentes, entonces $\mathbb{Q}(\sqrt{p_1}) \neq \mathbb{Q}(\sqrt{p_2})$. Puesto que existe una infinidad de números primos, entonces existe, al menos, una infinidad de campos. Por supuesto que no son todos y para no hacer mención específica a un campo en particular, usaremos la letra $\mathbb{F}$ para denotar cualquier campo. Cuando sea necesario haremos mención explícita del campo en cuestión.

Definición 3.1. *Un anillo es un conjunto $A \neq \emptyset$ con dos operaciones, que les podemos llamar suma y producto. Con la operación suma es un grupo abeliano. Con respecto al producto, éste debe ser asociativo y se deben cumplir las leyes distributivas $a(b+c) = ab + ac$ y $(b+c)a = ba + ca$.*

En general, en un anillo no necesariamente su producto conmuta y no necesariamente tiene 1. En todo lo que sigue, los anillos conmutan con el producto, tienen 1 y se vale la ley de la cancelación para el producto. Un ejemplo de anillo sin 1 es $2\mathbb{Z}$. El conjunto $M_{2\times 2}(\mathbb{F}) = \{\text{matrices de tamaño } 2 \times 2 \text{ con entradas en } \mathbb{F}\}$ con la suma y producto usual de matrices, es un anillo con 1(la matriz identidad) y no conmuta el producto ($\mathbb{F}$ es un campo).

Definición 3.2. *Sea $\mathbb{F}$ un campo. El anillo de polinomios con coeficientes en $\mathbb{F}$ es el conjunto $\mathbb{F}[x] = \{a_0 + a_1x + \cdots + a_nx^n : a_i \in \mathbb{F},\ n \in \mathbb{N}_0\}$. Si $f(x) = \sum_{i=0}^{n} a_ix^i \in \mathbb{F}[x]$, entonces a los números a_i les llamaremos los coeficientes de $f(x)$ y si $a_n \neq 0$, entonces diremos que $f(x)$ es un polinomio de grado n y que a_n es el coeficiente líder de $f(x)$. Escribiremos $gr(f(x)) = n$ para indicar que $f(x)$ es un polinomio de grado n. Si $f(x) = a_0$, entonces diremos que $f(x)$ es un polinomio constante. En este caso, si $a_0 \neq 0$ tenemos que $gr(f(x)) = 0$. Al polinomio constante 0 le asignamos grado $-\infty$.*

Sean $f(x) = a_0 + a_1x + \cdots + a_rx^n$ y $h(x) = b_0 + b_1x + \cdots + b_sx^m$ dos polinomios. Convenimos en que $f(x) = h(x)$ si y sólo si $r = s$ y $a_i = b_i$. El polinomio *cero* es el que tiene todos sus coeficientes $= 0$. Al polinomio $f(x)$ lo llamaremos *mónico* si su coeficiente líder es 1.

Nuestro conjunto $\mathbb{F}[x]$ satisface claramente la definición de anillo con la suma y producto usual de polinomios. Esto justifica el nombre *anillo* de polinomios. Concretamente, si $f(x) = a_0+a_1x+\ldots+a_nx^n$ y $h(x) = b_0+b_1x+\ldots+b_mx^m \in \mathbb{F}[x]$, entonces

$$f(x) + h(x) = c_0 + c_1x + \ldots + c_sx^s,$$

donde $s = \max\{m, n\}$ y para $0 \leq k \leq \max\{m, n\}$ tenemos $c_k = a_k + b_k$. El producto de polinomios proviene esencialmente de dos leyes básicas que gobiernan a la aritmética; la asociatividad y la distributividad. Así,

$$f(x)h(x) = a_0b_0 + (a_1b_0 + a_0b_1)x + \ldots + (a_0b_k + a_1b_{k-1} + \ldots + a_kb_0)x^k + \ldots$$

o en forma abreviada

$$f(x)h(x) = c_0 + c_1x + \cdots + c_{n+m}x^{n+m},$$

donde $c_k = \sum_{i=0}^{k} a_ib_{k-i}$, para $0 \leq i \leq n+m$. En particular, el coeficiente de x^{n+m} es a_nb_m pues $a_i = 0$ para $i > n$ y $b_j = 0$ para $j > m$.

Teorema 3.3. *Sean $f(x), h(x) \in \mathbb{F}[x]$. Entonces*

1. $gr(f(x) + h(x)) \leq \max\{gr(f(x)),\, gr(h(x))\}$,
2. $gr(f(x)h(x)) = gr(f(x)) + gr(h(x))$.

Demostración: Sean $f(x) = \sum_{i=0}^{n} a_ix^i$, $h(x) = \sum_{i=0}^{m} b_ix^i$ donde $gr(f(x)) = n$ y $gr((h(x)) = m$. Supongamos que $n \leq m$. Entonces $\max\{n, m\} = m$. Podemos escribir

$$f(x) = a_0 + a_1x + \cdots + a_nx^n + 0x^{n+1} + \cdots + 0x^m.$$

Por lo tanto

$$f(x)+h(x) = (a_0+b_0)+(a_1+b_1)x+\cdots+(a_n+b_n)x^n+b_{n+1}x^{n+1}+\cdots+b_mx^m.$$

Así tenemos que $gr(f(x) + h(x)) \leq \max\{gr(f(x)),\, gr(h(x))\}$.

Para el producto primero observemos que el coeficiente c_k de x^k satisface

$$c_k = a_0b_k + a_1b_{k-1} + \ldots + a_kb_0.$$

Por lo tanto, es claro que si $f(x)$ ó $h(x)$ es el polinomio 0, entonces $f(x)h(x) = 0$ y así $gr(f(x)h(x)) = gr(0) = -\infty$. Por lo anterior podemos suponer que $f(x) \neq 0 \neq h(x)$. En este caso, $a_n \neq 0$ y $a_i = 0$ para $i > n$. También $b_m \neq 0$ y $b_i = 0$ para $i > m$. Sea j tal que $j \leq n \leq m$. Entonces para $k > n + m$ tenemos que

$$c_k = a_0b_k + \cdots + a_jb_{k-j} + \cdots + a_nb_{k-n} + a_{n+1}b_{k-(n+1)} + \cdots$$

Notamos que a partir de $i \geq n + 1$ los números $a_i = 0$ y puesto que $k - j > m$, entonces los $b_{k-j} = 0$. En resumen, $c_k = 0$ si $k > n + m$ y puesto que $c_{n+m} = a_nb_m \neq 0$, entonces se sigue la segunda afirmación del teorema.

□

En la sección 2.5 del capítulo 2 demostramos, entre otras cosas, el Algoritmo de la división y el Teorema del Factor. Concretamente tenemos

Teorema 3.4. [Algoritmo de la división] *Si* $f(x),\ g(x) \in \mathbb{F}[x]$ *con* $g(x) \neq 0$, *entonces existen únicos* $q(x),\ r(x) \in \mathbb{F}[x]$ *tales que*

$$f(x) = g(x)q(x) + r(x), \ \ con \ \ r(x) = 0 \ \ ó \ \ gr(r(x)) < gr(g(x)).$$

Demostración: Es un fácil ejercicio para el lector.

□

Corolario 3.5. [Teorema del Residuo] *Sea* $f(x) \in \mathbb{F}[x]$ *y* $a \in \mathbb{F}$. *Sea* $f(x) = (x-a)q(x) + r(x)$. *Entonces* $r(x)$ *es el polinomio constante* $f(a)$.

Demostración: Puesto que $r(x) = 0$ ó $gr(r(x)) = 0$, tenemos $r(x) = 0$ ó $r(x)$ es un polinomio constante $\neq 0$.

□

Definición 3.6. *En el algoritmo de la división, si* $r(x) = 0$, *entonces diremos que* $g(x)$ *divide a* $f(x)$ *y escribiremos* $g(x) \mid f(x)$.

Corolario 3.7. [Teorema del Factor] *Sea* $f(x) \in \mathbb{F}[x]$ *no constante. Entonces* $a \in \mathbb{F}$ *es raíz de* $f(x)$ *si y sólo si* $x - a \mid f(x)$.

Demostración: Es consecuencia inmediata del Teorema del Residuo.

□

Teorema 3.8. *Sea* $\mathbb{F}$ *cualquier campo. Si* $a(x), b(x), c(x) \in \mathbb{F}[x]$ *y* $\delta \in \mathbb{F}^*$, *entonces:*

1. *Si* $a(x) \neq 0$, *entonces* $a(x) \mid 0$, $\delta \mid a(x)$ *y* $a(x) \mid \delta a(x)$.
2. *Si* $a(x) \mid b(x)$ *y* $b(x) \mid c(x)$, *entonces* $a(x) \mid c(x)$.
3. *Si* $a(x) \mid b(x)$ *y* $a(x) \mid c(x)$, *entonces* $a(x) \mid r(x)b(x) + s(x)c(x)$ *para cualquier* $r(x), s(x) \in \mathbb{F}[x]$.
4. *Si* $b(x) \neq 0$ *y* $a(x) \mid b(x)$, *entonces* $gr(a(x)) \leq gr(b(x))$.
5. *Si* $a(x) \mid b(x)$ *y* $b(x) \mid a(x)$, *entonces* $gr(a(x)) = gr(b(x))$.

Demostración: Es un fácil ejercicio para el lector.

□

Una diferencia que tiene $\mathbb{F}[x]$ con $\mathbb{Z}$, es que si $a(x) \neq 0$, entonces para $\delta \neq 0$ se tiene que $a(x) = \delta^{-1}(\delta a(x))$ y por lo tanto $a(x)$ tiene una infinidad de divisores (si $\mathbb{F}$ no es finito).

Gracias a que en el anillo de polinomios $\mathbb{F}[x]$ se puede dividir para obtener un cociente y un residuo únicos podemos desarrollar el concepto de máximo común divisor.

Definición 3.9. *Sean $f(x), h(x) \in \mathbb{F}[x]$ con $f(x) \neq 0 \neq h(x)$. El polinomio $g(x)$ es un divisor común de $f(x)$ y $h(x)$ si $g(x) \mid f(x)$ y $g(x) \mid h(x)$.*

Teorema 3.10. *Sean $f(x), h(x) \in \mathbb{F}[x]$ con $f(x) \neq 0 \neq h(x)$. Entonces existe $g(x) \in \mathbb{F}[x]$ tal que*

1. *$g(x) \mid f(x)$ y $g(x) \mid h(x)$.*
2. *Si $d(x) \mid f(x)$ y $d(x) \mid h(x)$, entonces $d(x) \mid g(x)$.*

Demostración: Sea $S = \{f(x)s(x) + h(x)r(x) : s(x), r(x) \in \mathbb{F}[x] \setminus \{0\}\}$. Si denotamos por $S_0 = \{gr(h(x)) : h(x) \in S\}$, entonces es claro que $S_0 \subseteq \mathbb{N}_0$ y $S_0 \neq \emptyset$. Por el **PBO**, existe $g(x) \in S$ tal que $gr(g(x)) \leq h(x)$ para cualquier $h(x) \in S$. Vamos a mostrar que $g(x)$ satisface la primera afirmación del teorema. La segunda afirmación es evidente. Supongamos que $g(x) \nmid f(x)$. Entonces por el algoritmo de la división tenemos

$$f(x) = g(x)q(x) + r(x) \quad \text{con } r(x) \neq 0 \text{ y } gr(r(x)) < gr(g(x)).$$

Puesto que $g(x) \in S$, tenemos que $g(x) = f(x)a(x) + h(x)b(x)$ para ciertos $a(x), b(x) \in \mathbb{F}[x]$. Por lo tanto

$$\begin{aligned} r(x) = f(x) - g(x)q(x) &= f(x) - (f(x)a(x) + h(x)b(x))q(x) \\ &= f(x)(1 - a(x)q(x)) + h(x)(-b(x)q(x)), \end{aligned}$$

así $r(x) \in S$ y $gr(r(x)) < gr(g(x))$, lo cual no es posible pues $g(x)$ es un polinomio en S de grado menor. Por lo tanto $g(x) \mid f(x)$ y por analogía $g(x) \mid h(x)$.

□

Definición 3.11. *Al polinomio $g(x)$ del teorema anterior lo llamaremos máximo común divisor de $f(x)$ y $h(x)$.*

Notemos que el máximo común divisor de dos polinomios no es único, pues si $g(x)$ satisface el teorema anterior y $\delta \neq 0$, entonces $\delta g(x)$ también satisface el teorema. Si $g(x) = a_0 + a_1x + \cdots + a_nx^n$, entonces $a_n^{-1}g(x)$ es un polinomio mónico y a éste lo denotaremos como $\text{mcd}(f(x), h(x))$. En este sentido el máximo común divisor de dos polinomios es único.

Definición 3.12. *Los polinomios $f(x)$ y $h(x)$ los llamaremos primos relativos si $\text{mcd}(f(x), h(x)) = 1$.*

En el curso de la demostración del Teorema 3.10 resultó que el mcd de $f(x)$ y $h(x)$ es una $\mathbb{F}[x]$- combinación lineal de ellos. Ahora la pregunta que nos hacemos es ¿cómo encontrar esa $\mathbb{F}[x]$-combinación lineal? Seguramente la respuesta ya la adivinaron.

Teorema 3.13. [Algoritmo de Euclides en $\mathbb{F}[x]$] *Sean $f(x), h(x) \in \mathbb{F}[x]$ con al menos $f(x)$ ó $h(x)$ diferente del polinomio 0. Al aplicar el algoritmo de la división varias veces obtenemos*

$$\begin{aligned}
f(x) &= h(x)q_1(x) + r_1(x), \ \ con \ \ gr(r_1(x)) < gr(h(x), \\
h(x) &= r_1(x)q_2(x) + r_2(x), \qquad gr(r_2(x)) < gr(r_1(x)), \\
r_1(x) &= r_2(x)q_3(x) + r_3(x), \qquad gr(r_3(x)) < gr(r_2(x)), \\
&\vdots \quad \vdots \\
r_{k-2}(x) &= r_{k-1}(x)q_k(x) + r_k(x), \qquad gr(r_k(x)) < gr(r_{k-1}(x)), \\
r_{k-1}(x) &= r_k(x)q_{k+1}(x) + r_{k+1}(x), \qquad r_{k+1}(x) = 0.
\end{aligned}$$

Si $r_k(x)$ es el último residuo $\neq 0$ y si escribimos $r_k(x) = a_0 + a_1x + \cdots + a_nx^n$, entonces $a_n^{-1}r_k(x) = \text{mcd}(f(x), h(x))$.

Demostración: Basta demostrar que $r_k(x)$ satisface el Teorema 3.10 y que este proceso es finito en el sentido que en algún momento obtendremos como residuo al polinomio $r_{k+1}(x) = 0$. En efecto, la sucesión de enteros positivos

$$0 < gr(r_k(x)) < \cdots < gr(r_2(x)) < gr(r_1(x)) < gr(h(x)$$

es finita y por lo tanto el proceso es finito. El resto de la prueba es bastante fácil. Si revisas la demostración del algoritmo de Euclides en $\mathbb{Z}$, podrás ingeniártela para terminar la prueba.

□

Calcular *a mano* el mcd de dos polinomios no ofrece dificultades si el grado de los polinomios es razonablemente pequeño. Con simples manipulaciones algebraicas y siguiendo el algoritmo de Euclides se puede llegar *fácilmente* al resultado. Algunos paquetes computacionales como *Mathematica* y *Maple* lo calculan eficientemente, sin embargo, todos están basados en el Teorema 3.13 o en alguna variación de él. Lo ideal sería escribir un programa en C^{++} o algún otro lenguaje para calcular el mcd de dos o más polinomios.

Ejemplo 3.14. *En $\mathbb{R}[x]$ consideremos los polinomios $f(x) = \sqrt{2} + 3x - x^7$ y*

$h(x) = 1 + x^2$. *Entonces*

$$\begin{aligned}\sqrt{2} + 3x - x^7 &= (1 + x^2)(-x + x^3 - x^5) + (\sqrt{2} + 4x),\\ 1 + x^2 &= (\sqrt{2} + 4x)\Big(- \frac{\sqrt{2}}{16} + \frac{x}{4}\Big) + \frac{9}{8},\\ \sqrt{2} + 4x &= \frac{9}{8}\Big(\frac{8\sqrt{2}}{9} + \frac{32}{9}x\Big) + 0\end{aligned}$$

Por lo tanto $\mathrm{mcd}(\sqrt{2} + 3x - x^7, 1 + x^2) = 1$. *Despejando* $\dfrac{9}{8}$ *y sustituyendo en la primera igualdad obtenemos la combinación lineal del mcd:*

$$1 = h(x)\Big(\frac{8}{9} + \frac{\sqrt{2}x}{18} - \frac{2x^2}{9} - \frac{\sqrt{2}x^3}{18} + \frac{2x^4}{9} + \frac{\sqrt{2}x^5}{18} - \frac{2x^6}{9}\Big) + f(x)\Big(\frac{\sqrt{2}}{18} - \frac{2x}{9}\Big).$$

Ejemplo 3.15. *Sean* $f(x) = -1+x^4$, $h(x) = i+x+ix^3+x^4$ *en* $\mathbb{C}[x]$. *Entonces*

$$\begin{aligned}i + x + ix^3 + x^4 &= (-1 + x^4)1 + ((1 + i) + x + ix^3),\\ -1 + x^4 &= ((1 + i) + x + ix^3)(-ix) + (-1 + (-1 + i)x + ix^2),\\ (1 + i) + x + ix^3 &= (-1 + (-1 + i)x + ix^2)(x + (-1 - i)) + 0\end{aligned}$$

Por lo tanto, el polinomio $-1 + (-1 + i)x + ix^2$ *satisface el Teorema 3.13. Así que* $\mathrm{mcd}(f(x), h(x)) = -i(-1 + (-1 + i)x + ix^2) = i + (1 + i)x + x^2$. *De paso* $\mathrm{mcd}(f(x), h(x)) = f(x)(-i - x) + h(x)x$.

Ejemplo 3.16. *Sean* $f(x) = 1-2x-3x^3+6x^4+x^5-2x^6$ *y* $h(x) = 1-x-2x^2$ *en* $\mathbb{F}_7[x]$. *Entonces*

$$\begin{aligned}f(x) &= h(x)(-2 + 2x - 2x^2 - x^3 + x^4) + (3 - 6x),\\ h(x) &= (3 - 6x)(\frac{1}{3} + \frac{x}{3}) + 0 = (3 - 6x)(5 + 5x) + 0.\end{aligned}$$

Por lo tanto $3 - 6x$ *satisface el Teorema 3.13 y así* $\mathrm{mcd}(f(x), h(x)) = 3 + x$. *Observemos que* $\dfrac{1}{3} = (3)^{-1} = 5$ *y* $-6 = 1 \pmod 7$.

Recordemos que $f(x) \in \mathbb{F}[x]$ es irreducible si $f(x)$ no es constante y siempre que $f(x) = h(x)g(x)$ con $h(x), g(x) \in \mathbb{F}[x]$, entonces alguno de los factores es un polinomio constante. Cualquier polinomio admite *factorizaciones triviales* $f(x) = a(a^{-1}f(x))$ con $a \neq 0$. Así, un polinomio es irreducible si sólo admite factorizaciones triviales. Por lo tanto, un polinomio *reducible* será aquel que admite al menos una factorización $f(x) = h(x)g(x)$, donde $h(x)$ y $g(x)$ no son constantes. Por lo anterior, un polinomio irreducible es el equivalente a un número primo en $\mathbb{Z}$. Veamos algunos ejemplos.

Ejemplo 3.17. *Sea p un número primo y $n \in \mathbb{N}$ con $n \geq 2$. La familia de polinomios $f(x) = -p + x^n$ tiene coeficientes en $\mathbb{Q}$ y son irreducibles en $\mathbb{Q}[x]$.*

Ejemplo 3.18. *Sea $a \in \mathbb{R}$ con $a > \frac{1}{4}$. La familia de polinomios $f(x) = a+x+x^2$ son irreducibles en $\mathbb{R}[x]$.*

Según los dos ejemplos anteriores, en $\mathbb{Q}[x]$ y en $\mathbb{R}[x]$ existe una infinidad de polinomios irreducibles. En general, tenemos el Teorema de Euclides para $\mathbb{F}[x]$.

Teorema 3.19. [Teorema de Euclides para $\mathbb{F}[x]$] *Sea $\mathbb{F}$ un campo infinito. Entonces existe una infinidad de polinomios irreducibles en $\mathbb{F}[x]$.*

Demostración: Para $a, b \in \mathbb{F}$ se tiene que los polinomios $f(x) = a + bx$ son irreducibles.

□

Si el campo $\mathbb{F}$ es finito, digamos que tiene p elementos, el Teorema de Euclides también es válido, de hecho, existen polinomios irreducibles de cualquier grado en $\mathbb{F}_p[x]$, sólo que no tenemos la teoría para justificarlo. Usualmente, en un curso de Teoría de Galois se puede justificar esto.

Notemos que el Ejemplo 3.17 nos dice que en $\mathbb{Q}[x]$ existen polinomios irreducibles de cualquier grado. El Ejemplo 3.18 y el Teorema 3.19 nos dice que en $\mathbb{R}[x]$ existen los de grado uno y algunos de grado dos. En $\mathbb{R}[x]$ podemos clasificar a todos los irreducibles y en la sección que sigue clasificaremos a los irreducibles en $\mathbb{C}[x]$. Para clasificar a los irreducibles de $\mathbb{R}[x]$ será útil considerar que un polinomio con coeficientes reales tiene coeficientes complejos y que cualquier número complejo tiene raíz cuadrada, cúbica, etc. Antes veamos la versión del Teorema Fundamental de la Aritmética para $\mathbb{F}[x]$, donde $\mathbb{F}$ es cualquier campo.

Lema 3.20. *Sea $f(x) \in \mathbb{F}[x]$ y $f(x)$ no constante. Entonces existe $\pi(x) \in \mathbb{F}[x]$ irreducible tal que $\pi(x) \mid f(x)$.*

Demostración: Inducción dobre el grado de $f(x)$. Si $gr(f(x)) = 1$, entonces $f(x)$ es irreducible y $f(x) \mid f(x)$. Supongamos que nuestra afirmación es cierta para todos los polinomios de grado $< gr(f(x)) = n$. Si $f(x)$ es irreducible, entonces terminamos. Si $f(x)$ es reducible, entonces $f(x) = h(x)g(x)$ con $1 \leq gr(h(x)), gr(g(x)) < n$. Por hipótesis de inducción $h(x)$ admite un factor irreducible $\pi(x)$ (que puede ser él mismo) y terminamos.

□

Corolario 3.21. *Sea $f(x) \in \mathbb{F}[x]$ y $f(x)$ no constante. Existe un número finito $\pi_1(x), \pi_2(x), \ldots, \pi_r(x)$ de polinomios irreducibles en $\mathbb{F}[x]$ tal que*

$$f(x) = \pi_1(x) \cdot \pi_2(x) \cdots \pi_r(x).$$

Demostración: Si $f(x)$ es irreducible no hay nada que probar. Supongamos que $f(x)$ es reducible y sea $\pi_1(x)$ irreducible tal que $f(x) = \pi_1(x)h_1(x)$. Si $h_1(x)$ es irreducible, terminamos. Si $h_1(x)$ es reducible, sea $\pi_2(x)$ irreducible tal que $h_1(x) = \pi_2(x)h_2(x)$. Así tenemos $f(x) = \pi_1(x)\pi_2(x)h_2(x)$. Aplicando el mismo argumento a $h_2(x), h_3(x), \ldots$, observamos que este proceso debe terminar en un número finito de pasos pues $1 \leq gr(\pi_i(x)) < gr(f(x))$.

□

El corolario anterior no nos asegura que la factorización en irreducibles es única. Este *defecto* se debe fundamentalmente a que si $\pi(x)$ es irreducible y $c \in \mathbb{F}^*$, entonces $c\pi(x)$ también es irreducible.

Teorema 3.22. *Sea $\pi(x) \in \mathbb{F}[x]$ irreducible tal que $\pi(x) \mid a(x)b(x)$. Entonces $\pi(x) \mid a(x)$ o $\pi(x) \mid b(x)$.*

Demostración: Sea $a(x)b(x) = \pi(x)t(x)$. Supongamos que $\pi(x) \nmid a(x)$. Vamos a demostrar que $\pi(x) \mid b(x)$. Si $\pi(x) \nmid a(x)$, entonces $\pi(x) \neq ca(x)$ para cualquier $c \in \mathbb{F}^*$ y $a(x)$ no es un polinomio constante. También $a(x) \nmid \pi(x)$ pues de lo contrario tendríamos que $\pi(x) = a(x)h(x)$ y como $a(x)$ no es constante y $\pi(x)$ es irreducible, entonces $h(x)$ es constante, lo cual es contrario a nuestra suposición $\pi(x) \nmid a(x)$. Por lo anterior $\text{mcd}(\pi(x), a(x)) = 1$. Así, por la demostración del Teorema 3.10 existe $r(x), s(x) \in \mathbb{F}[x]$ tal que

$$1 = \pi(x)r(x) + a(x)s(x).$$

Por lo tanto $b(x) = \pi(x)\Big(r(x)b(x) + t(x)s(x)\Big)$ y $\pi(x) \mid b(x)$.

□

Corolario 3.23. *Sean $\pi_1(x), \pi_2(x), \pi_3(x) \in \mathbb{F}[x]$ irreducibles tal que $\pi_1(x) \mid \pi_2(x)\pi_3(x)$. Entonces existe $\delta \in \mathbb{F}^*$ tal que $\pi_1(x) = \delta\pi_2(x)$ o $\pi_1(x) = \delta\pi_3(x)$.*

Demostración: Sin pérdida de generalidad supongamos que $\pi_1(x) \mid \pi_2(x)$. Entonces $\pi_2(x) = \pi_1(x)h(x)$, para algún $h(x) \in \mathbb{F}[x]$. Puesto que $\pi_2(x)$ es irreducible y $\pi_1(x)$ no es constante, entonces $h(x)$ es constante.

□

Sea $f(x) = a_0 + a_1x + \cdots + a_nx^n$. De la definición de producto de polinomios y del Corolario 3.21 se sigue inmediatamente que el producto de los coeficientes líderes de los $\pi_i(x)$'s es a_n. Si escribimos $f(x) = a_n(b_0 + b_1x + \cdots + x^n)$ y aplicamos nuevamente el Corolario 3.21 al polinomio $b_0 + b_1x + \cdots + x^n$ obtendremos que $f(x) = a_n(\pi_1(x) \cdot \pi_2(x) \cdots \pi_r(x))$.

Lema 3.24. *Sean $\pi_1(x), \pi_2(x)$ mónicos irreducibles tal que $\pi_1(x) \mid \pi_2(x)$. Entonces $\pi_1(x) = \pi_2(x)$.*

Demostración: Tenemos que $\pi_2(x) = \delta\pi_1(x)$. Puesto que $\pi_2(x)$ y $\pi_1(x)$ son mónicos tenemos que $\delta = 1$ y por tanto $\pi_1(x) = \pi_2(x)$.

□

Teorema 3.25. [Teorema Fundamental de la Aritmética en $\mathbb{F}[x]$] *Sea $f(x) \in \mathbb{F}[x] \setminus \mathbb{F}$. Si $f(x) = a_n(\pi_1(x) \cdot \pi_2(x) \cdots \pi_r(x)) = a_n(\pi_1'(x) \cdot \pi_2'(x) \cdots \pi_s'(x))$, donde a_n es el coeficiente líder de $f(x)$ y $\pi_i(x), \pi_j'(x)$ son mónicos irreducibles, entonces $r = s$ y si fuera necesario reordenar el producto, $\pi_i(x) = \pi_i'(x)$, para $1 \leq i \leq r \leq s$.*

Demostración: De la igualdad $\pi_1(x) \cdot \pi_2(x) \cdots \pi_r(x) = \pi_1'(x) \cdot \pi_2'(x) \cdots \pi_s'(x)$ se sigue que $\pi_1(x) \mid \pi_1'(x) \cdot \pi_2'(x) \cdots \pi_s'(x)$. Por el Teorema 3.22 podemos suponer que $\pi_1(x) \mid \pi_1'(x)$. Por el Lema 3.24 tenemos que $\pi_1(x) = \pi_1'(x)$. Así que $\pi_2(x) \cdot \pi_3(x) \cdots \pi_r(x) = \pi_2'(x) \cdot \pi_3'(x) \cdots \pi_s'(x)$. Supongamos que $r < s$. Aplicando el mismo argumento llegamos a que

$$\pi_1(x) = \pi_1'(x),\ \pi_2(x) = \pi_2'(x), \ldots, \pi_r(x) = \pi_r'(x),$$

y

$$1 = \pi_{r+1}'(x) \cdot \pi_{r+2}'(x) \cdots \pi_s'(x)$$

lo cual no es posible. Por lo tanto $r \geq s$. Si $r > s$ obtenemos la misma conclusión y así $r = s$.

□

Resumiendo: si los coeficientes de un polinomio están en un campo, entonces es posible factorizar como producto de irreducibles, pero ¿cómo se hace esta factorización? Invitamos al lector a que estudie las fórmulas para resolver ecuaciones polinomiales de grado $2, 3$ ó 4 en el caso $\mathbb{F} = \mathbb{C}$. Si el grado del polinomio es ≥ 5, es posible que no haya fórmulas. La existencia o no existencia de fórmulas es una pregunta a la que responde la Teoría de Galois.

¿Se conocen los irreducibles en $\mathbb{F}[x]$? En $\mathbb{C}[x]$ la respuesta la daremos en la siguiente sección y la clasificación de los irreducibles en $\mathbb{R}[x]$ la posponemos hasta la sección final de este capítulo.

PROBLEMAS

1. Sea p un número primo y $\mathbb{Q}(\sqrt{p}) = \{a + b\sqrt{p} : a, b \in \mathbb{Q}\}$.
   a) Demostrar que $\mathbb{Q} \subset \mathbb{Q}(\sqrt{p})$.
   b) Demostrar que $\mathbb{Q}(\sqrt{p})$ es un campo con la suma y producto usual de números reales.

c) Demostrar que $\mathbb{Q}(\sqrt{p})$ es un espacio vectorial de dimensión 2 sobre $\mathbb{Q}$.

d) Si q es un número primo y $p \neq q$, entonces $\mathbb{Q}(\sqrt{p}) \neq \mathbb{Q}(\sqrt{q})$.

2. Demostrar el Teorema 3.10 suponiendo que $f(x) \neq 0$ ó $h(x) \neq 0$, pero no ambos son idénticamente 0.

3. Sean $f(x)$ y $h(x)$ polinomios mónicos tal que $f(x) \mid h(x)$ y $h(x) \mid f(x)$. Demostrar que $f(x) = h(x)$.

4. Encontrar el mcd de los siguientes pares de polinomios:

a) $f(x) = 3 + 2ix^2 + x^4$ y $h(x) = -i + x$ en $\mathbb{C}[x]$.

b) $f(x) = 1 + x^4$ y $h(x) = 1 + ix^2 + x^3$ en $\mathbb{C}[x]$.

c) $f(x) = -2 + x^4$ y $h(x) = 4 + x^3 + x^5$ en $\mathbb{F}_7[x]$.

d) $f(x) = 7 - x^2$ y $h(x) = 7 + 7x + 6x^2 + 6x^3 - x^4 + x^5$ en $\mathbb{R}[x]$.

e) $f(x = 1 + 2x + 2x^2 + 12x^3$ y $h(x) = 1 + x + x^4 + x^5$ en $\mathbb{F}_{11}[x]$.

f) $f(x) = -2i + 3x^2 + 2ix^4 - 3x^6$ y $h(x) = i + x + ix^3 + x^4$ en $\mathbb{C}[x]$.

5. Demostrar el Teorema 3.13.

6. Sean $f(x), h(x) \in \mathbb{F}[x]$ tal que $f(x) \mid h(x)$. Encontrar $\text{mcd}(f(x), h(x))$.

7. Demostrar que si $\pi(x)$ es irreducible en $\mathbb{F}[x]$ y $\delta \in \mathbb{F}^*$, entonces $\delta\pi(x)$ también es irreducible.

8. Sean L y M dos campos tal que $L \subseteq M$.

a) Demostrar que $L[x] \subseteq M[x]$.

b) Si $\pi(x) \in L[x]$ es irreducible, entonces ¿$\pi(x)$ es irreducible visto como polinomio en $M[x]$?

c) Si $\pi(x) \in M[x]$ es irreducible y $\pi(x) \in L[x]$, entonces ¿$\pi(x)$ es irreducible visto como polinomio en $L[x]$?

9. Sean $f(x), h(x) \in \mathbb{F}[x]$ dos polinomios mónicos. ¿El producto $f(x)h(x)$ es mónico? Si $f(x)h(x)$ es mónico, ¿entonces $f(x)$ y $h(x)$ son mónicos?

10. Sea $f(x) \in \mathbb{C}[x]$. Si $h(x)$ es otro polinomio, entonces calcular $g(x) = \text{mcd}(f(x), h(x))$ te proporciona un factor de $f(x)$. Si $g(x)$ no es constante, entonces has obtenido un factor de $f(x)$ ¿Cómo escoger $h(x)$ de tal forma que $g(x)$ no sea constante? Este podría ser un método para encontrar factores de un polinomio dado. La respuesta no la conocemos.

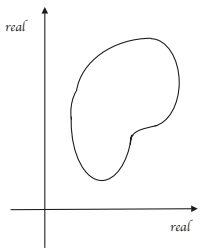
4 El Teorema Fundamental del Álgebra

La razón que nos inspiró a construir el campo $\mathbb{C}$ fue que no podíamos resolver la ecuación $1 + x^2 = 0$ sólo conociendo a $\mathbb{R}$. Tuvimos que construir un campo, en nuestro caso, tuvimos que *adjuntar* el número imaginario i al campo $\mathbb{R}$ para obtener $\mathbb{C}$. Con esta construcción, el polinomio $1 + x^2$ ya tiene solución. ¿Tendremos que repetir el proceso cada que nos aparezca algún polinomio en $\mathbb{R}[x]$ sin raíces reales? La respuesta es no. La enorme ventaja que ofrece $\mathbb{C}$ sobre $\mathbb{R}$ es precisamente que cualquier polinomio no constante en $\mathbb{C}[x]$ tiene todas sus raíces en $\mathbb{C}$, no hay que ir a buscarlas a otro lado.

El Teorema Fundamental del Álgebra (TFA) afirma que cualquier polinomio no constante en $\mathbb{C}[x]$, tiene todas sus raíces en $\mathbb{C}$. Este importante resultado tiene su origen en la aritmética. La matemática, entre los siglos XIII y XVIII, estaba preocupada fundamentalmente en resolver ecuaciones polinomiales, era una matemática casi algorítmica. En 1799, Gauss da la primera demostración en su tesis doctoral del TFA. En la actualidad se conocen decenas de demostraciones y siempre podemos encontrar alguna en cualquier libro de variable compleja. Existen también demostraciones topológicas y algunas llamadas "*elementales*" las cuales, todas usan algún resultado elemental del cálculo. Por supuesto que también hay demostraciones puramente algebraicas y que se basan en teoría de Galois o álgebra lineal.

La prueba del TFA que aquí presentaremos es elemental. Usaremos un resultado conocido: El Teorema del Valor Extremo. Creemos que cualquier persona que entienda bien el concepto de continuidad de una función de $\mathbb{R}^2$ en $\mathbb{R}^2$ no tendrá problemas para asimilar e incluso disfrutar la prueba que ofrecemos.

Primero explicaremos algunos conceptos que nos ayudarán a entender el curso de la demostración del TFA. Un subconjunto $D \subset \mathbb{R}^2$ es *cerrado* si D contiene a su frontera, por ejemplo, un disco cerrado de radio $r > 0$ o el semiplano superior incluyendo al eje real. Diremos que D es *acotado* si existe un disco C de radio finito tal que $D \subset C$. En general, en cualquier espacio euclideano, los conjuntos cerrados y acotados se llaman conjuntos *compactos*. Un resultado conocido nos asegura que si $f : D \subset \mathbb{R}^2 \to \mathbb{R}^2$ es una función continua y $D \subset \mathbb{R}^2$ es compacto, entonces $f(D) \subset \mathbb{R}^2$ también es compacto. Esta es una propiedad maravillosa que tienen las funciones continuas. En particular, si $f(x) \in \mathbb{C}[x]$, entonces para $z \in \mathbb{C}$ tenemos que $f : \mathbb{C} \to \mathbb{C}$ definida por la evaluación del polinomio en z es una función continua. Sea $D \subseteq \mathbb{C}$ y $|\ \ | : D \to [0, \infty)$ la función norma. Esta función también es continua.



Teorema 4.1. [Teorema del Valor Extremo] *Sea $D \subset \mathbb{R}^2$ cerrado y acotado. Si $f : D \to \mathbb{R}$ es una función continua, entonces f alcanza un valor máximo absoluto y un mínimo absoluto en D.*

Demostración: Ver T. Apostol [**?**] página 391 Teorema 9.9.

□

Antes de comenzar la prueba del TFA tendremos que justificar un par de lemas auxiliares.

Lema 4.2. *Sea $f(x) \in \mathbb{C}[x]$. Entonces $|f(x)|$ alcanza un valor mínimo z_0 en el plano complejo.*

Demostración: Si $f(x)$ es constante, entonces la afirmación es evidente. Así que podemos suponer que $f(x)$ no es un polinomio constante. Observemos que si $|z| \to \infty$, entonces por la desigualdad del triángulo $|f(z)| \to \infty$. Esto significa que la función módulo $|f(z)|$ no puede alcanzar un valor mínimo si $|z|$ es muy grande. Para $r > 0$ suficientemente grande restringimos $f(z)$ al disco $D = \{z \in \mathbb{C} : |z| \leq r\}$. Entonces por el Teorema del Valor Extremo, $f(x)$ alcanza un valor mínimo en D.

□

Lema 4.3. *Sea $f(x) \in \mathbb{C}[x]$ no constante tal que $f(0) = 1$. Entonces 1 no es el valor mínimo de la función $|f(x)|$.*

Demostración: Sea k la menor potencia positiva de x que aparece en $f(x)$. Entonces

$$f(x) = 1 + ax^k + x^{k+1}g(x),$$

donde $g(x)$ es algún polinomio en $\mathbb{C}[x]$. Puesto que cualquier número complejo tiene raíces k-ésimas, escogemos $\alpha \in \mathbb{C}$ tal que $\alpha^k = -\frac{1}{a}$. Evaluando $f(x)$ en αx tenemos que $f(x)$ se transforma en la expresión

$$f(\alpha x) = a + a(\alpha^k)x^k + x^{k+1}h(x) = 1 - x^k + x^{k+1}h(x),$$

donde $h(x)$ es algún polinomio en $\mathbb{C}[x]$. La relación entre $f(x)$ y $f(\alpha x)$ es que ambas son continuas y mandan subconjuntos compactos de $\mathbb{R}^2$ en subconjuntos compactos de $\mathbb{R}^2$. Aprovecharemos este cambio de variable para suponer sin pérdida de generalidad que

$$f(x) = 1 - x^k + x^{k+1}h(x),$$

para algún $h(x) \in \mathbb{C}[x]$. Por lo tanto, para todo $x \in \mathbb{C}$ tenemos

$$|f(x)| \leq |1 - x^k| + |x^{k+1}||h(x)|.$$

En particular, si $Im(x) = 0$ y $x > 0$ es suficientemente pequeño tenemos

$$|f(x)| \leq |1 - x^k| + x^{k+1}|h(x)| \leq 1 - x^k + x^{k+1}|h(x)| = 1 - x^k(1 - x|h(x)|).$$

Observemos que si $x \to 0^+$, entonces $x|h(x)| \to 0$ y $0 < x^k(1 - x|h(x)|) < 1$. Sea $x_0 > 0$ suficientemente pequeño y tal que $x_0|h(x_0)| < 1$. Entonces

$$|f(x_0)| < 1 = |f(0)|,$$

y así, 1 no es el valor mínimo que toma la función $|f(x)|$.

□

Corolario 4.4. *Sea $f(x) \in \mathbb{C}[x]$ no constante y $x_0 \in \mathbb{C}$ tal que $f(x_0) \neq 0$. Entonces $|f(x_0)|$ no es el valor mínimo de $|f(x)|$.*

Demostración: Sea $f(x) \in \mathbb{C}[x] \setminus \mathbb{C}$ tal que $f(x_0) \neq 0$. Si hacemos el cambio de variable x por $x + x_0$, entonces estamos moviendo x_0 al origen de $\mathbb{R}^2$. Este cambio de variable es muy conveniente porque $f(x + x_0)$ simplemente traslada los subconjuntos compactos del plano complejo en subconjuntos compactos idénticos. Por lo tanto podemos suponer sin pérdidad de generalidad que $x_0 = 0$ y $f(0) \neq 0$. Sea k la menor potencia positiva de x que aparece en $f(x)$. Entonces tenemos que

$$f(x) = a_0 + a_k x^k + x^{k+1}h(x),$$

para algún $h(x) \in \mathbb{C}[x]$. Observemos que los polinomios $\frac{1}{a_0}f(x)$ y $f(x)$ tienen exactamente el mismo grado, las mismas raíces y

$$\frac{1}{a_0}f(x) = 1 + b_k x^k + x^{k+1}h_1(x).$$

Por lo anterior podemos suponer sin pérdidad de generalidad que $f(0) = 1$ y

$$f(x) = 1 + b_k x^k + x^{k+1}h_1(x).$$

Ahora aplicamos el Lema 4.3

□

Teorema 4.5. [Teorema Fundamental del Álgebra] *(D'Lambert-Gauss) Si $f(x) \in \mathbb{C}[x] \setminus \mathbb{C}$, entonces $f(x)$ tiene una raíz en $\mathbb{C}$.*

Demostración: Sea $f(x) \in \mathbb{C}[x]$ no constante. Por el Lema 4.2 $|f(x)|$ alcanza un valor mínimo en algún punto $x_0 \in \mathbb{C}$. Usando el Corolario 4.4 necesariamente se cumple que $|f(x_0)| = 0$ y por lo tanto $f(x_0) = 0$.

□

Corolario 4.6. *Si $f(x) \in \mathbb{C}[x] \setminus \mathbb{C}$, entonces $f(x)$ tiene todas sus raíces en $\mathbb{C}$.*

Demostración: Sea $x_0 \in \mathbb{C}$ una raíz de $f(x)$. Entonces $f(x) = (x - x_0)h(x)$ para algún $h(x) \in \mathbb{C}[x]$ y $gr(h(x)) = gr(f(x)) - 1$. Ahora aplicamos el TFA al polinomio $h(x)$.

□

Corolario 4.7. *Cualquier polinomio no constante en* $\mathbb{C}[x]$ *se puede escribir como un producto de polinomios de grado* 1 *en* $\mathbb{C}[x]$.

Demostración: Sea $f(x) \in \mathbb{C}[x]$ no constante y $gr(f(x)) = n$. Probaremos el resultado por medio de inducción sobre n. Si $gr(f(x)) = 1$, entonces el resultado obviamente es cierto. Supongamos que el TFA es cierto para cualquier polinomio no constante en $\mathbb{C}[x]$ y de grado $\leq n-1$. Puesto que $gr(f(x)) = n$, entonces por el TFA, $f(x)$ tiene una raíz $x_0 \in \mathbb{C}$ y $f(x) = (x - x_0)g(x)$, donde $g(x) \in \mathbb{C}[x]$ tiene grado $n - 1$. Por hipótesis de inducción tenemos que $g(x)$ es producto de polinomios de grado 1. Así que $f(x)$ es producto de polinomios lineales.

□

Corolario 4.8. *Los únicos irreducibles en* $\mathbb{C}[x]$ *son los polinomios de grado* 1.

□

4.1 Clasificación de irreducibles en $\mathbb{R}[x]$

En esta sección vamos a aprovechar la teoría que hemos desarrollado para decir explícitamente quienes son los irreducibles en $\mathbb{R}[x]$.

Lema 4.9. *Sea* $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{R}[x]$ *y* $z_0 \in \mathbb{C}$ *tal que* $f(z_0) = 0$. *Entonces* $\overline{z}_0$ *también es raíz de* $f(x)$.

Demostración: Puesto que $a_i \in \mathbb{R}$, entonces usando las propiedades de la conjugación tenemos

$$\overline{f(z_0)} = \overline{a_0 + a_1z_0 + \cdots + a_nz_0^n} = a_0 + a_1\overline{z_0} + \cdots + a_n\overline{z_0}^n = f(\overline{z_0}).$$

Por lo anterior, $f(\overline{z_0}) = 0$.

□

El resultado anterior no es válido si algún coeficiente de $f(x)$ es un número complejo con parte imaginaria $\neq 0$. Por ejemplo, las raíces de $i + x^2$ son

$$z = \frac{-1}{\sqrt{2}} + \frac{i}{\sqrt{2}} \quad \text{y} \quad w = \frac{1}{\sqrt{2}} - \frac{i}{\sqrt{2}},$$

y claramente $z \neq \overline{w}$.

Corolario 4.10. *Si $f(x) \in \mathbb{R}[x]$ es de grado impar, entonces $f(x)$ es reducible.*

Demostración: Las raíces complejas de $f(x)$ aparecen por pares. Así que necesariamente $f(x)$ tiene al menos una raíz real.

□

Un criterio útil para decidir si un polinomio cuadrático en $\mathbb{R}[x]$ es irreducible es el siguiente:

Lema 4.11. *Sea $f(x) = c + bx + ax^2 \in \mathbb{R}[x]$ con $a \neq 0$. Entonces $f(x)$ es irreducible si y sólo si $b^2 - 4ac < 0$.*

Demostración: El TFA nos asegura que $f(x)$ tiene dos raíces en $\mathbb{C}$. Claramente si alguna de ellas está en $\mathbb{R}$, entonces por el Teorema del Factor la otra también está en $\mathbb{R}$. Así tenemos que $f(x)$ es irreducible en $\mathbb{R}[x]$ si y sólo si $f(x)$ no tiene raíces reales. Sea $r = \dfrac{-b + \sqrt{b^2 - 4ac}}{2a}$ una raíz de $f(x)$. Entonces $r \in \mathbb{R}$ si y sólo si $2ar + b = \sqrt{b^2 - 4ac} \in \mathbb{R}$. Esto último se cumple si y sólo si $b^2 - 4ac \geq 0$.

□

Teorema 4.12. [Clasificación de irreducibles en $\mathbb{R}[x]$] *Los únicos irreducibles en $\mathbb{R}[x]$ son los de grado 1 y los cuadráticos del lema anterior.*

Demostración: Sea $f(x) \in \mathbb{R}[x]$ irreducible y $gr(f(x)) = n$ con $n > 2$. Por el Corolario 4.10 necesariamente el grado de $f(x)$ es par y por lo tanto las raíces de $f(x)$ son complejas con parte imaginaria $\neq 0$. Sean $z_1, \overline{z_1}, z_2, \overline{z_2}, \ldots, z_s, \overline{z_s}$ las raíces de $f(x)$. Si $z_j = a + bi$, entonces el polinomio cuadrático

$$(x - z_j)(x - \overline{z_j}) = x^2 - 2ax + (a^2 + b^2) \in \mathbb{R}[x]$$

es un factor de $f(x)$. Así que $f(x)$ sólo tienen como raíces a z_1 y $\overline{z_1}$ y por lo tanto $gr(f(x)) = 2$.

□

Corolario 4.13. *Cualquier polinomio $f(x) \in \mathbb{R}[x]$ con $gr(f(x)) \geq 2$ se puede escribir en forma única como producto de polinomios de grado 1 y polinomios de grado 2.*

Demostración: Aplicar los Teoremas 3.25 y 4.12.

□

¿Y los irreducibles en $\mathbb{Q}[x]$? No conocemos en la literatura algún trabajo en donde se de una lista completa de los irreducibles en $\mathbb{Q}[x]$. Sólo podemos afirmar en este momento que hay irreducibles de cualquier grado, por ejemplo; la familia $\{x^n - p : n \geq 2,\ p \text{ primo}\}$ son algunos de ellos.

PROBLEMAS

1. Sea $f(x) \in \mathbb{R}[x]$ tal que $gr(f(x))$ es par y $f(x)$ tiene al menos una raíz real. Demostrar que $f(x)$ tiene al menos dos raíces reales.
2. Sea $f(x) = a\Big((x-b)^2 + c^2\Big) \in \mathbb{R}[x]$ con $a \neq 0 \neq c$. Mostrar que $f(x)$ es irreducible en $\mathbb{R}[x]$.
3. Sea $z \in \mathbb{C}$. Demostrar que $f(x) = (x-z)(x-\overline{z}) \in \mathbb{R}[x]$.
4. Criterio de irreducibilidad de Eisentein. Sea $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$. Si existe un primo p tal que $p \mid a_i$ para $0 \leq i < n$ y $p^2 \nmid a_0$, $p \nmid a_n$, entonces $f(x)$ es irreducible en $\mathbb{Q}[x]$.
5. $f(x) \in \mathbb{Z}[x]$ es irreducible si y sólo si $f(x+1)$ es irreducible.
6. Sea p un número primo y $f(x) = 1 + x + ... + x^{p-1}$. Usar el criterio de Eisenstein y el problema anterior para demostrar que $f(x) \in \mathbb{Z}[x]$ es irreducible.
7. ¿Para qué valores de $c \in \mathbb{Q}$ es $-1 + x$ un factor de $c + x + 2x^2 + x^3$ en $\mathbb{Q}[x]$?
8. ¿Para qué valores de $c \in \mathbb{C}$ es $i + x$ un factor de $c - 2ix + x^6$ en $\mathbb{C}[x]$?
9. ¿Cómo es la gráfica de un polinomio cuadrático irreducible en $\mathbb{R}[x]$?
10. Demostrar que existe un único polinomio $f(x) \in \mathbb{R}[x]$ de grado 2 tal que $f(1) = 2$, $f(2) = 3$ y $f(3) = 0$.
11. Sean $\alpha_0, \alpha_1, ..., \alpha_n, \beta_0, \beta_1, ..., \beta_n \in \mathbb{C}$ tal que $\alpha_i \neq \alpha_j$ si $i \neq j$. Demostrar que existe un único polinomio $f(x) \in \mathbb{C}[x]$ tal que $f(\alpha_i) = \beta_i$ y grado de $f(x) \leq n$. Sugerencia: Si $f(x) = a_0 + a_1 x + ... + a_n x^n$, entonces resolver el sistema $(f(\alpha_i) = \beta_i)$ en las indeterminadas a_i.
12. Sean $\alpha_0, \alpha_1, ..., \alpha_n, \beta_0, \beta_1, ..., \beta_n \in \mathbb{C}$ como en el problema anterior y $f(x) = \sum_{k=0}^{n} \dfrac{\beta_k (x-\alpha_0)\cdots(x-\alpha_{k-1})(x-\alpha_{k+1})\cdots(x-\alpha_n)}{(\alpha_k-\alpha_0)\cdots(\alpha_k-\alpha_{k-1})(\alpha_k-\alpha_{k+1})\cdots(\alpha_k-\alpha_n)}$. Demostrar que $f(\alpha_i) = \beta_i$. ¿Tiene algo que ver este polinomio con el del problema anterior? El polinomio $f(x)$ se conoce como *la fórmula de Interpolación de Lagrange.*
13. Sea $f(x) = a_0 + a_1 x + ... + a_n x^n \in \mathbb{C}[x]$. Definimos el conjugado de $f(x)$ como $\overline{f(x)} = \overline{a_0} + \overline{a_1} x + ... + \overline{a_n} x^n$. Demostrar que si $f(x), h(x) \in \mathbb{C}[x]$, entonces $\overline{f(x)h(x)} = \overline{f(x)}\,\overline{h(x)}$.
14. Sean $f(x), h(x), g(x) \in \mathbb{C}[x]$ tal que $f(x) = h(x)g(x)$. Demostrar que si cualesquiera dos polinomios de $f(x), h(x), g(x)$ están en $\mathbb{R}[x]$, entonces el tercero también está en $\mathbb{R}[x]$.