Unidad 1: Números Complejos y Polinomios
Álgebra y Geometría Analítica I (R-111)
Licenciatura en Ciencias de la Computación

Iker M. Canut

2020

1. Números Complejos

El conjunto de los números complejos es $\mathbb{C} = \{z = a+bi : \ a, b \in \mathbb{R}\}$, donde i es la **unidad imaginaria** que verifica $i^2 = -1$, pues $(0,1)\cdot(0,1) = (0\cdot 0 - 1\cdot 1, 0\cdot 1 + 1\cdot 0) = (-1, 0)$. Se nota, $(a, b) = (a + bi)$. Si $z \in \mathbb{C}$, $z = a + bi$ es la **forma binómica** de z.

La **parte real** de z es a, $Re\ z = a$, y la **parte imaginaria** de z es b, $Im\ z = b$.
$z = w \iff Re\ z = Re\ w \wedge Im\ z = Im\ w$.

Sea $z = a + bi$ y $w = c + di$, luego $z + w = (a + c) + (b + d)i$ y también $z \cdot w = (ac - bd) + (ad + bc)i$
La suma y el producto son *asociativos* y *conmutativos*, vale la propiedad *distributiva*, existen *elementos neutros* $(0, 0)$ y $(1, 0)$, existe el *elemento opuesto* $(-a, -b)$ y existe el *inverso*, $z^{-1} = (\dfrac{a}{a^2+b^2}, -\dfrac{b}{a^2+b^2})$.

Sea $z = a + bi \in \mathbb{C}$, llamamos **conjugado** de z al complejo $\overline{z} = a - bi$. Y llamamos **módulo** de z al real $|z| = \sqrt{a^2 + b^2}$. Además, $|z|^2 = z \cdot \overline{z}$ y también $z^{-1} = \dfrac{\overline{z}}{|z|^2}$. Luego, $\dfrac{z}{w} = \dfrac{ac+bd}{c^2+d^2} + \dfrac{bc-ad}{c^2+d^2}i$.

1.1. Propiedades

- $z^k \cdot z^n = z^{k+n}$
- $(z^k)^n = z^{k\cdot n}$
- $(z \cdot w)^n = z^n \cdot w^n$
- $\left(\dfrac{z}{w}\right)^n = \dfrac{z^n}{w^n}$
- $\overline{\overline{z}} = z$
- $\overline{z + w} = \overline{z} + \overline{w}$
- $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$
- Si $z \neq 0$, $\overline{z^{-1}} = (\overline{z})^{-1}$
- $z + \overline{z} = 2 \cdot Re\ z$
- $z - \overline{z} = 2 \cdot (Im\ z) \cdot i$
- $z = 0 \iff |z| = 0$
- $|z \cdot w| = |z| \cdot |w|$
- $|z| = |\overline{z}|$
- $|z| = |-z|$
- Si $z \neq 0$, $|z^{-1}| = |z|^{-1}$
- Si $z \neq 0$, $\left|\dfrac{z}{w}\right| = \dfrac{|z|}{|w|}$

1.2. Otras Formas

La **forma polar** de $z \in \mathbb{C}$ es $z = |z|_{arg\ z}$, donde $arg\ z$ es el **argumento** y es el único real tal que:

- $0 \leq arg\ z \leq 2\pi$
- $\cos(arg\ z) = \dfrac{a}{|z|}$
- $\sin(arg\ z) = \dfrac{b}{|z|}$

Sea $z = \rho_\theta$ y $w = \delta_\gamma$, entonces $\quad z \cdot w = (\rho \cdot \delta)_{\theta+\gamma}, \quad \dfrac{z}{w} = (\rho \cdot \delta)_{\theta-\gamma} \quad$ y $\quad z^n = \rho^n_{\theta\cdot n}$.

La **forma trigonométrica** de $z \in \mathbb{C}$ es $z = |z|(\cos arg\ z + i \sin arg\ z)$.
Sea $z = \rho(\cos\alpha + i\sin\alpha)$ y $w = \tau(\cos\beta + i\sin\beta)$, $z = w \iff (\rho = \tau) \wedge \alpha = \beta + 2k\pi,\ k \in \mathbb{Z}$.

Teorema de Moivre: Sean $z, w \in \mathbb{C}, z \neq 0, w \neq 0,\quad z = |z|(\cos\alpha + i\sin\alpha),\quad w = |w|(\cos\beta + i\sin\beta)$

$$z \cdot w = |z||w|[\cos(\alpha+\beta) + i\sin(\alpha+\beta)]$$

- $z^{-1} = |z|^{-1}[\cos(-\alpha) + i\sin(-\alpha)]$
- $\dfrac{z}{w} = \dfrac{|z|}{|w|}[\cos(\alpha-\beta) + i\sin(\alpha-\beta)]$
- $\overline{z} = |z|[\cos(-\alpha) + i\sin(-\alpha)]$
- $z^n = |z|^n[\cos(n\cdot\alpha) + i\sin(n\cdot\alpha)]$, con $n \in \mathbb{N}$

Si $w \in \mathbb{C}, w \neq 0$, una **raiz n-ésima** de w, con $n \in \mathbb{N}$, es un número z tal que $z^n = w$:

$$z = |z|^{\frac{1}{n}}\left[\cos\frac{arg\ w + 2k\pi}{n} + i\sin\frac{arg\ w + 2k\pi}{n}\right], \qquad 0 \leq k \leq n-1, k \in \mathbb{N}$$

La **notación exponencial** de z es $z = |z|e^{i\alpha}$. Se verifica que $\overline{e^{i\alpha}} = e^{\overline{i\alpha}} = e^{-i\alpha}$ y que $e^{i\alpha}\cdot e^{i\beta} = e^{i(\alpha+\beta)}$

$$\sqrt[n]{z} = \sqrt[n]{|z|}e^{\dfrac{i(\theta+2k\pi)}{n}}$$

2. Polinomios

Sea $\mathbb{K}$ el conjunto de reales $\mathbb{R}$ o de complejos $\mathbb{C}$, un polinomio con coeficientes en $\mathbb{K}$ es una expresión:

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 = \sum_{k=0}^{n} a_k x^k, \quad \text{con } a_k \in \mathbb{K},\ 0 \leq k \leq n,\ n \in \mathbb{N} \tag{1}$$

Denotamos por $\mathbb{K}[x]$ al conjunto de todos los polinomios con coeficientes en $\mathbb{K}$. Cada término de a forma $a_k x^k$ se denomina **monomio** y k es el **grado** de dicho monomio. Cada a_k es un **coeficiente**. Un polinomio dado por (1), con $a_n \neq 0$, tiene **grado** n. El polinomio **nulo**, $P(x) = 0$ no tiene grado.

Dados $P(x) = a_n x^n + ... + a_1 x + a_0$ y $Q(x) = b_m x^m + ... + b_1 x + b_0$, con $a_n \neq 0$ y $b_m \neq 0$.

- Dos polinomios son **iguales**, es decir, $P = Q \iff \begin{cases} n = m \\ a_k = b_k,\ \forall k = 0, ..., n = m \end{cases}$

- La **suma** $P+Q \begin{cases} \text{Si } n = m, & (P+Q)(x) = \sum_{k=0}^{n}(a_k + b_k)x^k \\ \text{Si } n > m, & P+Q = P + Q^*, \text{ donde } Q^* = 0x^n + 0x^{n-1} + ... + b_m x^m + ... + b_0 \\ \text{Si } n < m, & P+Q = P^* + Q, \text{ donde } P^* \text{ se define de manera análoga a } Q^* \end{cases}$

  La suma de polinomios es una operación cerrada en $\mathbb{C}[x]$, asociativa, conmutativa, con elemento neutro (polinomio nulo), tal que todo $P(x) \in \mathbb{C}[x]$ admite elemento opuesto, que denotamos $-P$. Siendo $(-P)(x) = (-a_n)x^n + ... + (-a_1)x + (-a_0)$. La **diferencia** entre P y Q es $P - Q = P + (-Q)$ Además, se verifica que $gr(P+Q) \leq \text{máx}\{gr(P), gr(Q)\}$

- El **producto** $(P \cdot Q)(x) = (a_n \cdot b_m)x^{n+m} + (a_n b_{m-1} + a_{m-1} b_m)x^{n+m-1} + ... + (a_1 b_0 + a_0 b_1)x + a_0 b_0$. Operación cerrada en $\mathbb{C}[x]$, asociativa, conmutativa y con elemento neutro (constante igual a 1). Además, si ninguno es nulo, se verifica que $gr(P \cdot Q) = gr(P) + gr(Q)$.

- **División**: Dados $P, Q \in \mathbb{C}[x]$, $Q \neq 0$, existen únicos polinomios C y R tales que $(R = 0 \vee gr\ R < gr\ Q) \wedge (P = C \cdot Q + R)$. Luego, C es el **cociente** y R el **resto**.

Demostración: Considerando el conjunto $A = \{P - H \cdot Q : H \in \mathbb{C}[x]\}$. El polinomio nulo puede estar en A, luego existe H' tal que $P - H' \cdot Q = 0$ y tomando $C = H'$, vale el teorema con $R = 0$; o el polinomio nulo no está en A, luego $\forall H \in \mathbb{C}[x][P - H \cdot Q \neq 0]$. Sea n_0 el mínimo de los grados de los polinomios que están en $A \Rightarrow$ existe $H_0 : gr(P - H_0 \cdot Q) = n_0$, y definimos $R_0 = P - H_0 \cdot Q$.
- Para ver que $gr(P_0) < gr(Q)$, suponemos $gr(P_0) \geq gr(Q)$. Sea $R_0 = \sum_{i=1}^{n_0} r_i x^i$ y que $Q = \sum_{i=0}^{m} q_i x^i$, con $gr(Q) = m$. Luego, sea $R' = R_0 - \frac{r_{n_0}}{q_m}x^{n_0 - m} \cdot Q = P - \left(H_0 + \frac{r_{n_0}}{q_m}x^{n0-m} \cdot Q\right)$. Se ve que $R' \in A$ pues $\left(H_0 + \frac{r_{n_0}}{q_m}x^{n_0-m}\right) \in \mathbb{C}[x]$. Tenemos que $gr\left(\frac{r_{n_0}}{q_m}x^{n_0-m} \cdot Q\right) = n_0 - m + m = n_0$. Resulta $gr(R') \leq n_0$, pero como no puede ser igual porque el término de grado n_0 seria 0, tenemos que $gr(R') < n_0$. Pero es absurdo porque $R' \in A$, y el grado mínimo de los polinomios es n_0. Luego, $n_0 < m$, y tomando $C = H_0$ y $R = R_0$, tenemos que $P = C \cdot Q + R$.
- Para demostrar la unicidad de C y R, suponemos C' y R' y tenemos que $P = C \cdot Q + R = C' \cdot Q + R' \Rightarrow (C - C') \cdot Q = (R' - R)$. Si fuese $C \neq C'$, entonces $gr((C - C') \cdot Q) = gr(C - C') + gr(Q) \geq gr(Q)$, pero por otra parte, $gr(R' - R) \leq \text{máx}\{gr(R'), gr(R)\} \leq gr(Q)$, y esto no puede ocurrir. Luego $C - C' = 0$ y $R' - R = 0$, y finalmente $C = C'$ y $R = R'$. ■

Corolario: Sean $P, Q \in \mathbb{C}[x]$, con $Q \neq 0, gr(P) \geq gr(Q) : P = C \cdot Q + R \Rightarrow gr(C) = gr(P) - gr(Q)$.

Regla de Rufini: $P(x) = a_n x^n + ... + a_1 x + a_0$ y $Q(x) = x - \alpha, \alpha \in \mathbb{C}$, entonces $P(x) = C(x) \cdot (x - \alpha) + R$
Con $C(x) = b_{n-1}x^{n-1} + ... + b_1 x + b_0$ y $R = a_0 + \alpha b_0$, donde $\{b_{n-1} = a_n \wedge b_i = a_{i+1} + \alpha b_{i+1}\}$
Demostración: Por el algoritmo de la división, sabemos que existe $C \in \mathbb{C}[x]$ tal que $P = C \cdot Q + R$. Luego, si $C(x) = b_{n-1}x^{n-1} + ... + b_1 x + b_0$, entonces:

$$P = C \cdot Q + R = b_{n-1}x^n + (b_{n-2} - \alpha b_{n-1}x^{n-1}) + ... + (b_0 + \alpha b_1)x - b_0 + R\alpha$$ ■

Dado $P \in \mathbb{K}[x]$ y $z \in \mathbb{C}$, la **evaluación** de P en z es el número complejo $P(z) = \sum_{k=0}^{n} a_k z^k$

Teorema del Resto: $P \in \mathbb{C}[x], gr(P) \geq 1, z \in \mathbb{C} \Rightarrow P(z)$ es el resto de dividir P por $Q(x) = x - z$.
Demostración: Sea $C(x)$ el cociente de dividir P por Q y r el resto, luego $P(x) = C(x) \cdot Q(x) + r$. Pero como $Q(z) = z - z = 0$, entonces $P(z) = C(z) \cdot 0 + r = r$ ■

Luego decimos que un polinomio P es **divisible** por Q si el resto de dividir P por Q es 0. Se nota $Q|P$. Entonces, P se **factoriza** como $C \cdot Q$, donde C es el cociente de la división de P por Q.

3. Factorización de Polinomios

Sea $P \in \mathbb{C}[x]$, decimos que un número complejo α es **raíz** de P si $P(\alpha) = 0$. Luego, α es una raíz de P si y solo si P es divisible por $Q(x) = x - \alpha$.

Sea $P \in \mathbb{C}[x], h \in \mathbb{N}$, decimos que α es una **raíz de multiplicidad h** de P si P es divisible por $(x-a)^h$ pero no por $(x-a)^{h+1}$. Es decir, $(x-a)^h|P$ y $(x-a)^{h+1} \nmid P$

Teorema Fundamental del Álgebra: Todo polinomio $P \in \mathbb{C}[x]$ de grado mayor o igual a 1, admite al menos una raiz compleja. ■
Corolario: Todo $P \in \mathbb{C}[x]$ de grado $n \geq 1$ admite exactamente n raices complejas, contadas con su multiplicidad. Por el TFA, sabemos que tiene 1 raiz. Luego, definimos $P_1 \in \mathbb{C}$ tal que $P(x) = P_1 \cdot (x - \alpha_1)$ y $gr(P_1) = gr(P) - 1 = n - 1$. Luego, aplicando el TFA a P_1, tenemos que existe una raiz compleja α_2, y encontramos un P_2. Continuamos de manera recursiva hasta encontrar las n raices. ■

Teorema de Descomposición Factorial: Sea $P = a_n x^n + ... + a_1 x + a_0$ y sean $\alpha_1, ..., \alpha_s$ las raices distintas de P, de multiplicidad $h_1, ..., h_n$ / $h_1 + ... + h_s = n$, entonces $P(x) = a_n (x - \alpha_1)^{h_1} ... (x - \alpha_s)^{h_s}$
Demostración: Tras $n-1$ pasos encontramos $n-1$ raices de P, que pueden llegar a repetirse. Luego, queda factorizado como $P(x) = (x - \alpha_1) \cdot (x - \alpha_2) \cdot ... \cdot (x - \alpha_{n-1}) \cdot C_{n-1}(x)$. Donde C_{n-1} tiene grado 1, es decir, $C_{n-1} = ax + b$ con $a \neq 0$, y $ax + b = a\left(x + \frac{b}{a}\right)$ y finalmente $\alpha_n = -\frac{b}{a}$, obteniendo asi $P(x) = a(x - \alpha_1) \cdot (x - \alpha_2) \cdot ... \cdot (x - \alpha_{n-1}) \cdot (x - \alpha_n)$ ■

Teorema: Sea $P \in \mathbb{R}[x]$, si $\alpha \in \mathbb{C}$ es una raiz de P, entonces $\overline{\alpha}$ también es una raiz de P.
Demostración: Del hecho que $a_i = \overline{a_i}$, pues cada a_i es un real, tenemos que:
$P(\overline{\alpha}) = a_n \overline{\alpha}^n + ... + a_1 \overline{\alpha} + a_0 = \overline{a_n x^n + ... + a_1 x + a_0} = \overline{0} = 0$.

Nota: Luego, todo polinomio a coeficientes reales tiene una cantidad par de raices complejas. Y se puede concluir que si tiene grado impar, tiene al menos una raiz real.
Nota: Además, todo polinomio a coeficientes reales puede factorizarse siempre como producto de polinomios lineales, o cuadráticos a coeficientes reales. En efecto, si $\alpha = a + ib$ es una raíz de P, luego $\overline{\alpha} = a - ib$ también es una raíz de P. Entonces $(x - \alpha)^h (x - \overline{\alpha})^h = [x^2 - (\alpha + \overline{\alpha})x + \alpha\overline{\alpha}]^h$

Teorema de Gauss: Sea $P(x) = a_x x^n + ... + a_1 x + a_0 \in \mathbb{Z}[x]$, con $a_0 \neq 0$, si $\alpha = \dfrac{r}{s}$ es una raiz racional de P, con r y s primos relativos, entonces r divide a a_0 y s divide a a_n.
Demostración: Como $P(\alpha) = 0$, tenemos que $\left(a_n \dfrac{r^n}{s^n} + ... + a_1 \dfrac{r}{s} + a_0\right) = 0$ y multiplicando ambos miembros por s^n, tenemos que $a_n r^n + ... + a_1 s^{n-1} r + a_0 s^n = 0$. **Sacando factor común r**, $r(a_n r^{n-1} + ... + a_1 s^{n-1}) = -a_0 s^n$. También, tenemos que $a_0 \neq 0, r \neq 0$ (0 no es raiz de P). Luego, $a_n r^{n-1} + ... + a_1 s^{n-1} \in \mathbb{Z}$ y por lo tanto $\dfrac{-a_0 s^n}{r} \in \mathbb{Z}$. No puede suceder que r divide a s^n pues son primos relativos, luego r divide a a_0. - Análogamente, **sacando factor comun s**, llegamos a que s divide a a_n. ■

Teorema: $a \in \mathbb{C}$ es raiz de $P \in \mathbb{C}[x]$ de multiplicidad $k \iff P(a) = P'(a) = ... = P^{(k-1)}(a) = 0$