Las Raíces de la Unidad

Pablo L. De Nápoli

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

Álgebra I - Primer cuatrimestre de 2020

Parte I

La forma polar o trigonométrica de los números complejos

Forma polar de los números complejos

- Fórmula de Euler:

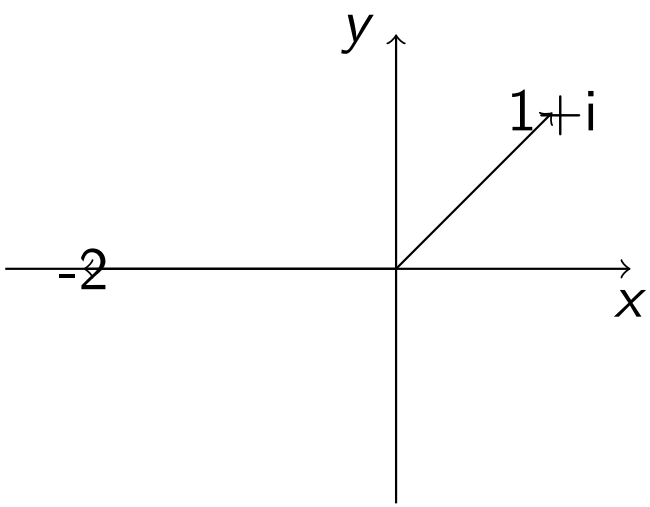
$$e^{ix} = \cos x + i \operatorname{sen} x$$

Notamos $\mathbb{C}^* = \mathbb{C} - \{0\}$. Si $z = x + iy \in \mathbb{C}^*$ es un número complejo no nulo, introduciendo coordenadas polares (r, θ) donde

$$r = |z| = \sqrt{x^2 + y^2}$$

es el módulo del complejo z, y θ su argumento, lo podemos escribir en la forma polar o trigonométrica.

$$z = r \cdot e^{i\theta}$$



Ejemplos:

$$-2 = 2 \cdot e^{i\pi}$$

$$1 + i = \sqrt{2} \cdot e^{i\pi/4}$$

Igualdad de complejos en forma polar

Notemos que el argumento θ no está unívocamente determinado.
Sean $z, w \in \mathbb{C}^*$. Si $z = r \cdot e^{i\theta}$ y $w = \tilde{r} \cdot e^{i\tilde{\theta}}$

$$z = w \Leftrightarrow |z| = |w| \wedge \theta \equiv \tilde{\theta} \pmod{2\pi}$$

donde

$$\theta \equiv \tilde{\theta} \pmod{2\pi} \Leftrightarrow \exists k \in \mathbb{Z} : \theta - \tilde{\theta} = 2\pi\ k$$

Ejemplo:

$$1 + i = \sqrt{2} \cdot e^{i\pi/4} = \sqrt{2} \cdot e^{\frac{17}{4}\pi i}$$

pues

$$\frac{\pi}{4} - \frac{17}{4}\pi = 4\pi$$

Para normalizar podemos tomar $0 \leq \theta < 2\pi$ (como hace el apunte).

Producto y potencias de complejos en la forma polar

Teorema (Teorema de De Moivre con la notación exponencial)

Si $z = r \cdot e^{i\theta}$ y $w = \tilde{r} \cdot e^{i\tilde{\theta}}$, son dos números complejos expresados en la forma trigonométrica, entonces

$$z \cdot w = (r \cdot \tilde{r}) \cdot e^{i(\theta+\tilde{\theta})}$$

Corolorario

Para $n \in \mathbb{N}$,

$$z^n = r^n \cdot e^{in\theta}$$

Ejemplo: si queremos calcular $(1+i)^{20}$, como $1 + i = \sqrt{2} \cdot e^{i\pi/4}$ tenemos

$$20 \cdot \frac{1}{4}\pi = 5\pi \equiv \pi \pmod{2\pi}$$

luego

$$(1+i)^{20} = (\sqrt{2})^{20} e^{20 \cdot \frac{1}{4}\pi i} = 2^{10} \cdot e^{\pi i} = -1024$$

Raíces n-ésimas de los números complejos

Encontrar las raices n-ésimas de un complejo $z \in \mathbb{C}^*$ es resolver la ecuación

$$\omega^n = z$$

El siguiente teorema afirma que para cada $z \in C^*$ hay exactamente n soluciones.

Teorema (6.4.1 en el apunte)

Sea $n \in N$ y sea $z = s \cdot e^{i\varphi} \in \mathbb{C}^*$, con $s \in \mathbb{R}_{>0}$ y $0 \leq \varphi < 2$. Entonces z tiene n raíces n -ésimas $\omega_0, \omega_1, \ldots \omega_{n-1} \in \mathbb{C}$, donde

$$\omega_k = s^{1/n} \cdot e^{\theta_k i}$$

siendo

$$\theta_k = \frac{\varphi + 2k\pi}{n} \quad \text{para } 0 \leq k \leq n-1$$

Parte II

Raíces de la unidad

Las raíces n-ésimas de la unidad

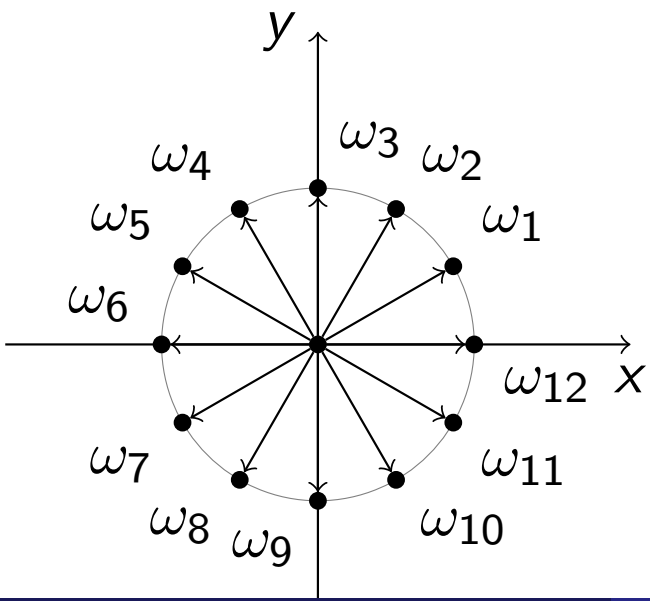
Definición

Decimos que $z \in \mathbb{C}$ *es una raíz n-ésima de la unidad si* $z^n = 1$. *Notamos*

$$G_n = \{z \in \mathbb{C} : z^n = 1\}$$

al conjunto de raíces n-ésimas de la unidad. Explícitamente,

$$G_n = \left\{\omega_k = e^{2\pi i \frac{k}{n}} : k \in \mathbb{N}, 0 \leq k < n-1\right\} \Rightarrow \#(G_n) = n$$



Ejemplo con $n = 12$.

¿Qué tienen de especial las raíces de la unidad?

$(G_n, \cdot)$ es un grupo abeliano:

- $1 \in G_n$.
- si $z, w \in G_n \Rightarrow z \cdot w \in G_n$.
- si $z \in G_n$, $z^{-1} = \frac{1}{z} \in G_n$.

Referencia: Sección 6.4.1 del apunte de la profesora Krick.

Ejemplo: si $n = 4$, $G_4 = \{\omega_0 = 1, \omega_1 = i, \omega_2 = -1, \omega_3 = -i\}$. Notemos que $\omega_k = i^k$. Notamos la similitud entre la tabla de G_4 y la de $\mathbb{Z}_4$.

$\cdot$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

Las raíces n-ésimas primitivas de la unidad

Dentro de las raíces n-ésimas de la unidad, distinguimos unas especiales que llamamos raíces primitivas n-ésimas de la unidad.

Existen varias maneras de definirlas. En el apunte, se adopta la siguiente definición

Definición (6.4.7)

Sea $n \in \mathbb{N}$ se dice que $\omega \in \mathbb{C}$ es una raíz primitiva n-ésima de la unidad si ω es un generador de G_n o sea si

$$G_n = \{1, \omega, \omega^2, \ldots, \omega^{n-1}\}$$

Notemos G_n^* al conjunto de raíces primitivas n-ésimas de la unidad. (El apunte no usa esta notación pero nos va a ser cómoda)

Ejemplo: Si $n = 4$, vimos que $G_4 = \{1, i, -1, -i\} = \{1, i, i^2, i^3\}$ luego i es una raíz primitiva de órden 4.

Una reformulación que nos va a ser útil

Dado un número complejo no nulo $z \in C$ definimos su orden (multiplicativo)

$$\text{orden}(z) = \text{mín}\{k \in \mathbb{N} : z^k = 1\}$$

si $z^k = 1$ para algún $k \in \mathbb{N}$, y $orden(z) = \infty$ si no.
Entonces

$$G_n = \{z \in \mathbb{C} - \{0\} : 1 \leq \text{orden}(z) \leq n\}$$

$$G_n^* = \{z \in \mathbb{C} - \{0\} : \text{orden}(z) = n\}$$

Una conexión clave con la aritmética de los enteros

Propisición

Si orden$(z) = d$, entonces $z^k = 1$ si y sólo sí $d|k$.

Para verlo, efectuamos la división entera

$$k = q \cdot d + r \quad \text{con} \quad 0 \leq r < d$$

tenemos

$$z^k = (z^d)^q \cdot z^r = z^r$$

- Si $d|k \Rightarrow r = 0 \Rightarrow z^k = 1$.
- Recíprocamente si $z^k = 1$, entonces $z^r = 1$ pero como $0 \leq r < d$, debe ser $r = 0$ (por la definición de orden) es decir que $d|k$.

Las potencias se repiten

El siguiente coroloario dice que si z es un raíz primitiva de la unidad de orden d, sus potencias se repiten módulo d.

Corolorario

Si $orden(z) = d$, *entonces*

$$z^j = z^k \text{ sí y sólo si } j \equiv k \pmod{d}$$

Pues

$$z^j = z^k \Leftrightarrow z^{j-k} = 1 \Leftrightarrow d|j-k \Leftrightarrow j \equiv k \pmod{d}$$

Una descomposición importante

Otra consecuencia de la propiedad anterior es:

Corolorario

- $z \in G_n$ *sí y sólo si* $orden(z) | n$
- *Tenemos la descomposición*

$$G_n = \bigcup_{d|n} G_d^*$$

(esta unión es disjunta)

Un ejemplo: raíces cuartas ($n = 4$)

$$G_4 = \{1, i, -1, -i\}$$

$$1^1 = 1 \Rightarrow \text{orden}(1) = 1$$

$$(-1)^1 = -1, (-1)^2 = 1 \Rightarrow \text{orden}(-1) = 2$$

$$i^1 = i, i^2 = -1, i^3 = -i, i^4 = 1 \Rightarrow \text{orden}(i) = 4$$

$$(-i)^1 = -i, (-i)^2 = -1, (-i)^3 = i, (-i)^4 = 1 \Rightarrow \text{orden}(-i) = 4$$

Luego

$$G_4 = G_1^* \cup G_2^* \cup G_4^*$$

donde

$$G_1^* = \{1\}, G_2^* = \{-1\}, G_4^* = \{i, -i\}$$

¿Cómo calculamos el orden de una raíz n-ésima ?

Ahora supongamos que tenemos una raíz n-ésima dada explícitamente por

$$\omega_k = e^{2\pi i \frac{k}{n}}$$

¿Cómo calculamos su orden? La fracción k/n puede no ser irreducible pero podemos considerar una fracción equivalente

$$\frac{k}{n} = \frac{k'}{n'}$$

escribiendo $k' = k : d$, $n' = n : d$ donde $d = (k : n)$.
k' y n' serán ahora coprimos (por la proposición 4.5.13 del apunte).

¿Cómo calculamos el orden de una raíz n-ésima ? (2)

Hecha esta reducción, vemos que

$$\omega_k = e^{2\pi i \frac{k'}{n'}}$$

En consecuencia,

$$\omega_k^j = e^{2\pi i \frac{k'j}{n'}}$$

$$\omega_k^j = 1 \Leftrightarrow \frac{k'j}{n'} \in \mathbb{Z} \Leftrightarrow n' | k'j$$

pero como k' y n' son coprimos, por la proposición 4.5.12 del apunte deducimos que

$$\omega_k^j = 1 \Leftrightarrow n' | j$$

Es decir que

$$\text{orden}(\omega_k) = n'$$

Descripción explícita de las raíces primitivas

En particular $\text{orden}(\omega_k) = n \Leftrightarrow n = n' \Leftrightarrow d = 1$. Deducimos que:

Propisición (6.4.11 en el apunte)

$$G_n^* = \left\{ \omega_k = e^{2\pi i \frac{k}{n}} \text{ con } 0 \leq k \leq n-1 \text{ y } k \text{ coprimo con } n \right\}$$

Ejemplo: si $n = 4$

$$\begin{array}{lll} \omega_0 = 1 & \frac{0}{4} = \frac{0}{1} & \Rightarrow \textit{orden}(\omega_0) = 1 \\ \omega_1 = i & \frac{1}{4} \text{ es irreducible} & \Rightarrow \textit{orden}(\omega_1) = 4 \\ \omega_2 = -1 & \frac{2}{4} = \frac{1}{2} & \Rightarrow \textit{orden}(\omega_2) = 2 \\ \omega_3 = -i & \frac{3}{4} \text{ es irreducible} & \Rightarrow \textit{orden}(\omega_3) = 4 \end{array}$$

¿Cúantas raíces primitivas n-ésimas de la unidad hay?

Si definimos la indicatriz de Euler $\varphi(n)$ como la cantidad de enteros k que cumplen $0 \leq k \leq n-1$ y son coprimos con n, tendremos entonces

$$\#(G_n^*) = \varphi(n)$$

(Notamos que coincide con el cardinal de Z_n^*). La descomposición

$$G_n = \bigcup_{d|n} G_d^*$$

nos va a dar que

$$\sum_{d|n} \varphi(d) = n \text{ para todo } n \in \mathbb{N}$$

Esta propiedad permite calcular $\varphi(n)$ recursivamente. Ejemplos:

$$\varphi(1) = 1$$

$$\varphi(1) + \varphi(2) = 2 \Rightarrow \varphi(2) = 1$$

$$\varphi(1) + \varphi(2) + \varphi(4) = 4 \Rightarrow \varphi(4) = 2$$

Bonus track: ¿Cúanto vale la indicatriz de Euler?

Teorema

Para todo $n \in \mathbb{N}$, tenemos que:

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

donde el producto se extiende sobre los divisores primos de n.

Hay una demostración en mi apunte de enteros. La idea de esa demostración es probar primero

Teorema (Propiedad multiplicativa)

Si m_1 y m_2 son coprimos y $m = m_1 \cdot m_2$, entonces:

$$\varphi(m) = \varphi(m_1)\varphi(m_2)$$

usando el teorema chino del resto.

Bonus track: El teorema de Fermat-Euler

Teorema (Euler)

Si $n \in \mathbb{N}$ y $a \in \mathbb{Z}$ es coprimo con n, entonces

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Hay una demostración en mi apunte de enteros. Cuando n es primo, $\varphi(n) = n - 1$ y se reduce al teorema de Fermat.

Ejemplo: si $n = 8$, $\varphi(8) = 4$, y obtenemos que

$$a^4 \equiv 1 \pmod{8}$$

cuando a es coprimo con 8, es decir impar.

Sumando todas las raíces n-ésimas

Propisición (6.4.13 en el apunte)

$$S(n) = \sum_{\omega \in G_n} \omega = \begin{cases} 1 & si \quad n = 1 \\ 0 & si \quad n > 1 \end{cases}$$

Demostración: Si $n = 1$, $G_1 = \{1\}$ luego $S(1) = 1$.
Si $n > 1$ y ω es una raíz primitiva n-ésima cualquiera,

$$G_n = \{1, \omega, \omega^2, \ldots, \omega^{n-1}\}$$

luego

$$S(n) = \sum_{k=0}^{n-1} \omega^k = \frac{\omega^n - 1}{\omega - 1} = 0$$

(acá usamos que como $n > 1$, $\omega \neq 1$)

Un ejercicio de la práctica 6

Recomiendo que intenten resolver este ejercicio

Ejercicio (Ejercicio 11 en la práctica 6)

i) *Calcular la suma de las raíces n-ésimas primitivas de la unidad para* $n = 2, 3, 4, 5, 8, 10, 15$.

ii) *Calcular la suma de las raíces p-ésimas primitivas de la unidad para p primo.*

Definamos dos funciones

$$S(n) = \sum_{\omega \in G_n} \omega$$

$$S^*(n) = \sum_{\omega \in G_n^*} \omega$$

El ejercicio nos pide calcular $S^*(n)$ para algunos valores de n. ¿Qué relación tienen S y S^* ?
(solución en uno de mis videos en nuestro canal de Youtube)