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

Teoría sobre las 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,

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

$(G_n, \cdot)$ 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.

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)

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

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

Las potencias se repiten

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 ($n = 4$)

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

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

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

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

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

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

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

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:

$$\varphi(1) = 1$$

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

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

Parte II

Sumanndo las raíces de la unidad

Un ejercicio de la práctica 6

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.

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 $n > 1$, $\omega \neq 1$)

Sumando la raíces primitivas n-ésimas

Para resolver el ejercicio, notamos que la descomposición

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

nos da (por la propiedad asociativa de la suma) que:

$$\sum_{d|n} S^*(d) = S(n)$$

y como ya calculamos $S(n)$ podemos deducir el valor de $S^*(d)$.

Respuestas del ejercicio:

$$S^*(1) = S(1) = 1$$

$$S^*(1) + S^*(2) = 0 \Rightarrow S^*(2) = -1$$

$$S^*(1) + S^*(3) = 0 \Rightarrow S^*(3) = -1$$

$$S^*(1) + S^*(2) + S^*(4) = 0 \Rightarrow S^*(4) = 0$$

$$S^*(1)S^*(5) = 0 \Rightarrow S^*(5) = -1$$

$$S^*(1) + S^*(2) + S^*(4) + S^*(8) = 0 \Rightarrow S^*(8) = 0$$

$$S^*(1) + S^*(2) + S^*(5) + S^*(10) = 0 \Rightarrow S^*(10) = -1$$

Respuestas del ejercicio (2):

$$S^*(1) + S^*(3) + S^*(5) + S^*(15) = 0 \Rightarrow S^*(15) = 1$$

Y p es primo,

$$S^*(1) + S^*(p) = 0 \Rightarrow S^*(p) = -1$$

Estos ejemplos sugieren que en general, $S^*(n)$ depende de como sea la factorización en primos de n.

¿Y en general cuánto da la suma de las raíces primitivas n-ésimas?

Definamos la función μ de Möbius del siguiente modo:

$$\mu(n) = \begin{cases} 1 & \text{si} \quad n = 1 \\ 0 & \text{si} \quad \text{si } n \text{ es divisible por el cuadrado de algún primo} \\ (-1)^k & \text{si} \quad n = p_1 p_2 \dots p_k \text{ siendo los } p_i \text{ primos distintos} \end{cases}$$

entonces se tiene el siguiente

Teorema

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

$$S^*(n) = \mu(n)$$

Prueba del teorema (1)

La prueba se basa en que μ verifica la misma propiedad que $S^*(n)$,

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si} \quad n = 1 \\ 0 & \text{si} \quad n > 1 \end{cases}$$

Para $n = 1$ vale pues $\mu(1) = 1$. Si $n > 1$, supongamos que la factorización de n sea

$$n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} \quad \text{(primos distintos)}$$

Notemos que sólo los enteros d que no son divisibles a un cuadrado contribuyen a la suma. Es decir, nos van a interesar los divisores d de la forma

$$d = p_{j_1} p_{j_2} \dots p_{j_\ell}$$

donde los p_{j_s} son algunos de los primos en la factorización de n. Para ellos $\mu(d) = (-1)^\ell$. Pero para cada r ¿cúantos hay? $\binom{r}{\ell}$
Entonces

$$\sum_{d|n} \mu(d) = \sum_{\ell=0}^{r} (-1)^\ell \binom{r}{\ell} = (1-1)^r = 0$$

Prueba del teorema (2)

Ahora es fácil probar el teorema por inducción completa (teorema 2.5.7 del apunte) en n

- Si $n = 1$, $S^*(1) = \mu(1) = 1$.
- Si $n > 1$ y suponemos que $S^*(k) = \mu(k)$ para $k < n$, tenemos que

$$\sum_{d|n} S^*(d) = \sum_{d|n} \mu(d) = 0$$

Separamos en las sumas el término $d = n$

$$\sum_{d|n,d<n} S^*(d) + S^*(n) = \sum_{d|n,d<n} \mu(d) + \mu^*(n)$$

Pero de la hipótesis inductiva deducimos que

$$\sum_{d|n,d<n} S^*(d) = \sum_{d|n,d<n} \mu(d)$$

Luego sustituyendo, podemos concluir que $S^*(n) = \mu(n)$.