Lectura 7: Raíces de la unidad

7.1. Polígonos

Antes de presentar el tema de raíces de unidad, es importante identificar el concepto de polígono desde un punto de vista mucho más algebraico y menos geométrico. De manera intuitiva, entendemos un polígono como un conjunto de aristas y vértices en el plano, sin embargo, cuando usamos un sistema de coordenadas podemos deshacernos de los aristas al ser el conjunto de vértices suficiente para describir las lineas entre ellos. Podemos concluir que son los vértices la información más importante para la definición de un polígono. Aunque nuestra discusión incluya sólo a los vértices, será mucho más limitada pues por fines prácticos, deseamos únicamente definir el concepto de polígono cuyos vértices estén contenidos en la circunferencia de radio 1.

Definición 7.1. Sea $\theta_0, \ldots, \theta_{n-1}$ una sucesión de números reales distintos entre sí. La sucesión se dice *inscribe un polígono de n lados en la circunferencia unitaria* si

$$\theta_0 < \theta_1 < \ldots < \theta_{n-1}$$

y para todo $1 \leq k < n$

$$0 \leq \theta_k < 2\pi.$$

Puede extrañar la descripción anterior, sin embargo la secuencia de números representa solamente los ángulos de los puntos en coordenadas polares usando como radio siempre 1. Esto quiere decir que los vértices estarán dados por los puntos en coordenadas cartesianas

$$x_k = (\cos\theta_k, \operatorname{sen}\theta_k),$$

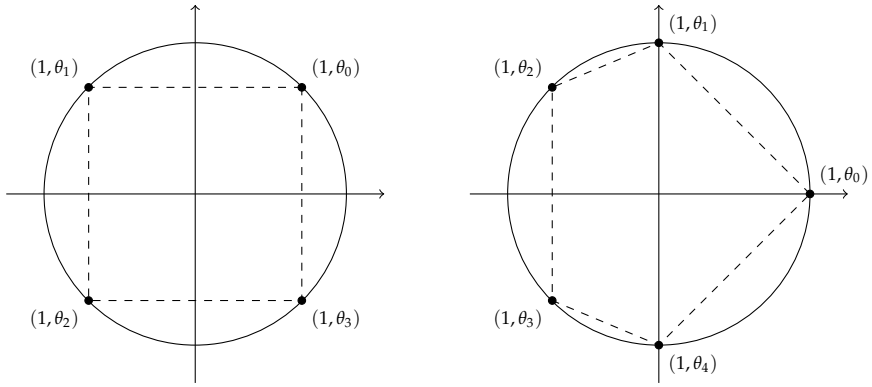
mientras las aristas serán los segmentos de linea entre los puntos x_k y x_{k+1} tomando $x_n = x_0$. Sin embargo, es de notarse que esta definición tiene algunas posibilidades curiosas. Para una ilustración de esto se pueden revisar las figuras 1a y 1b. Por supuesto, buscamos distinguir los polígonos en los cuales su vértices equidistan uno de otro, estos serán llamados *polígonos regulares*. Es interesante notar que podemos definir una secuencia muy sencilla que entrega polígonos regulares de n lados tomando

$$\theta_k = \frac{2\pi k}{n};$$

en otras palabras, tomando la sucesión

$$0, \frac{2\pi}{n}, \frac{4\pi}{n}, \frac{6\pi}{n}, \ldots, \frac{2\pi(n-1)}{n}.$$

Esta sucesión, es la formalización de la técnica por la cual es costumbre enseñarnos el trazado de un polígono regular con regla y compás. El siguiente teorema justifica esta técnica.



(a) Un polígono regular de 4 lados. (b) Un polígono de 5 lados.

Figura 1: Ejemplos de polígonos en el círculo unitario.

Teorema 7.1. *La sucesión $\theta_k = 2\pi k/n$ definida para $0 \leq k < n$ forma un polígono regular.*

Demostración. Debemos identificar primero que la sucesión indicada define un polígono, en el cual los puntos en coordenadas cartesianas están dados por

$$x_k = (\cos\theta_k, \operatorname{sen}\theta_k).$$

Si definimos $x_n = x_1$, afirmamos que $|x_{k+1} - x_k|^2$ es una constante para todo $0 \leq k < n$. En efecto, usando la identidad pitagórica y la diferencia de cosenos, podemos calcular

$$\begin{aligned} |x_{k+1} - x_k|^2 &= (\cos(\theta_{k+1}) - \cos(\theta_k))^2 + (\operatorname{sen}(\theta_{k+1}) - \operatorname{sen}(\theta_k))^2 \\ &= 2 - 2\cos(\theta_{k+1})\cos(\theta_k) - 2\operatorname{sen}(\theta_{k+1})\operatorname{sen}(\theta_k) \\ &= 2 - 2\cos(\theta_{k+1} - \theta_k) \end{aligned}$$

y como

$$\theta_{k+1} - \theta_k = \frac{2\pi(k+1)}{n} - \frac{2\pi k}{n} = \frac{2\pi}{n},$$

debemos tener que

$$|x_{k+1} - x_k|^2 = 2 - 2\cos(2\pi/n)$$

el cual no depende de k, como se afirmó. De lo anterior, se desprende de inmediato que la distancia entre vértices consecutivos es la misma y por tanto la sucesión forma un polígono regular. ■

Además de el teorema anterior, mucho se puede decir al definir un polígono de esta manera, sin embargo esto es todo lo que necesitamos de momento para hablar geométricamente de la solución de un interesante conjunto de ecuaciones con solución en los números complejos:

$$z^m = 1.$$

7.2. Raíces m-ésimas de la unidad

Vamos ahora a definir un concepto completamente vinculado a las solución de ecuaciones muy particulares de las cuales exploraremos sus propiedades tanto geométricas como algebraicas.

Definición 7.2. Sea m un entero positivo. Un número complejo ζ se dice *una raíz m-ésima de la unidad*, si satisface

$$\zeta^m = 1.$$

Hasta ahora, el único caso en el que hemos encontrado todas las raíces de la unidad es cuando $m = 2$; en éste, las únicas posibles resultan ambas reales siendo éstas 1 y -1. Fuera de este caso, poco o nada sabemos, por lo que nos vemos obligados a explorar su significado. Comenzaremos probando una hermosa identidad atribuida al matemático francés Abraham de Moivre, que de hecho nos revelerá todas las raíces que buscamos.

Teorema 7.2 (De Moivre)**.** *Para cualquier entero positivo m y real θ, se tiene*

$$(\cos\theta + i\,\mathrm{sen}\,\theta)^m = \cos(m\theta) + i\,\mathrm{sen}(m\theta).$$

Demostración. Para probar el resultado procedemos por inducción: El resultado con $m = 1$ es inmediato, supongamos entonces que

$$(\cos\theta + i\,\mathrm{sen}\,\theta)^m = \cos(m\theta) + i\,\mathrm{sen}(m\theta);$$

en ese caso

$$\begin{aligned}(\cos\theta + i\,\mathrm{sen}\,\theta)^{m+1} &= (\cos\theta + i\,\mathrm{sen}\,\theta)^m(\cos\theta + i\,\mathrm{sen}\,\theta)\\ &= (\cos(m\theta) + i\,\mathrm{sen}(m\theta))(\cos\theta + i\,\mathrm{sen}\,\theta)\\ &= \cos(m\theta)\cos\theta - \sin(m\theta)\sin\theta + i(\cos\theta\sin(m\theta) + \cos(m\theta)\sin\theta)\\ &= \cos(m\theta + \theta) + i\,\mathrm{sen}\,(m\theta + \theta)\\ &= \cos((m+1)\theta) + i\,\mathrm{sen}\,((m+1)\theta).\end{aligned}$$

Por inducción, la igualdad planteada es válida como afirma el enunciado del teorema. ■

La identidad de Moivre, nos permite encontrar las raíces de la unidad de manera muy simple recurriendo a la expresión en coordenadas polares de un número complejo.

Teorema 7.3. *Sea m un entero positivo. Entonces, un complejo ζ es una raíz m-ésima de la unidad si y sólo si existe un entero $0 \leq k < m$ de forma que*

$$\zeta = \cos\left(\frac{2\pi k}{m}\right) + i\,\mathrm{sen}\left(\frac{2\pi k}{m}\right)$$

Demostración. Supongamos primero que $\zeta = \cos\left(\frac{2\pi k}{m}\right) + i\,\mathrm{sen}\left(\frac{2\pi k}{m}\right)$, entonces, por la identidad de De Moivre,

$$\zeta^m = \cos(2\pi k) + i\,\mathrm{sen}\,(2\pi k) = 1,$$

por tener las funciones sen y cos periodo 2π. Lo anterior muestra que ζ es una raíz m-ésima de la unidad.

Si ahora suponemos que ζ es una raíz m-ésima de la unidad, entonces $|\zeta| = 1$ (¿por qué?); en ese caso somos capaces de escribir

$$\zeta = \cos\theta + i\,\mathrm{sen}\,\theta$$

donde $0 \leq \theta < 2\pi$. Por hipótesis, la identidad de De Moivre implica

$$1 = \zeta^m = \cos(m\theta) + i\,\mathrm{sen}(m\theta)$$

lo que a su vez nos permite concluir $\cos(m\theta) = 1$. Lo anterior sucede únicamente si $m\theta = 2\pi k$ para algún entero k, el cual por la representación de coordenadas polares que asumimos debe satisfacer $0 \leq k < n$. En otras palabras

$$\zeta = \cos\left(\frac{2\pi k}{m}\right) + i\,\mathrm{sen}\left(\frac{2\pi k}{m}\right).$$

■

Corolario 7.4. *Hay exactamente m raíces m-ésimas de la unidad.*

El teorema anterior y su corolario nos permiten calcular explícitamente todas las raíces m-ésimas de la unidad, pero por la forma en que quedan expresadas, podemos enumerarlas usando su argumento y de acuerdo al teorema 7.1, se obtiene un polígono regular.

Corolario 7.5. *La sucesión de argumentos de las raíces m-ésimas, inscribe un polígono regular de m lados en la circunferencia unitaria.*

Para ilustrar la idea detrás de las raíces m-ésimas, calculemos las cuatro raíces cuartas de las unidad, i.e., todos los complejos que satisfagan $\zeta^4 = 1$. Según el teorema 7.3 éstas debe ser cuatro y están descritas por

$$\begin{aligned}
\zeta_0 &= \cos(0) + i\,\mathrm{sen}\,(0) = 1 \\
\zeta_1 &= \cos\left(\frac{\pi}{2}\right) + i\,\mathrm{sen}\left(\frac{\pi}{2}\right) = i \\
\zeta_2 &= \cos(\pi) + i\,\mathrm{sen}\,(\pi) = -1 \\
\zeta_3 &= \cos\left(\frac{3\pi}{2}\right) + i\,\mathrm{sen}\left(\frac{3\pi}{2}\right) = -i.
\end{aligned}$$

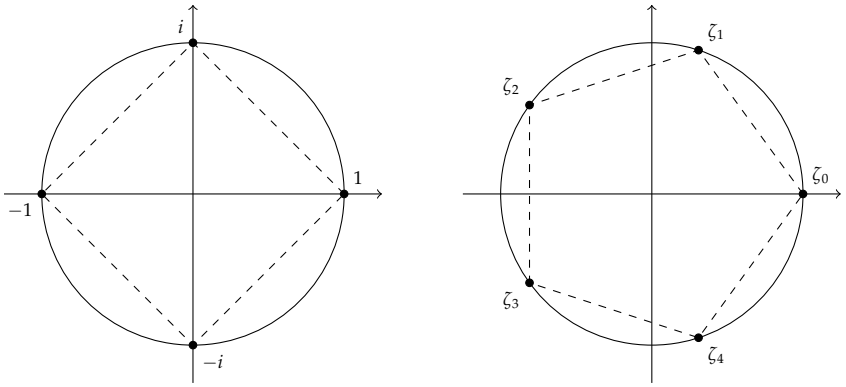
Vamos ahora a explorar algunas de las propiedades algebraicas de las raíces de la unidad. Estos resultados motivarán algunos conceptos posteriores, es importante estudiarlos con cuidado.

Teorema 7.6. *El producto de dos raíces m-ésimas de la unidad es una raíz m-ésima.*

Demostración. Consideremos dos raíces m-ésimas, ζ y η. En ese caso

$$(\zeta\eta)^m = \zeta^m\eta^m = 1 \cdot 1 = 1,$$

lo que nos lleva a concluir que $\zeta\eta$ es una raíz enésima de la misma forma. ■



(a) Las raíces cuartas (b) Las raíces quintas

Figura 2: Las raíces m-ésimas como un polígono.

Las raíces de la unidad, juegan un papel en encontrar raíces m-ésimas de cualquier complejo. Por ejemplo, si deseamos encontrar todos los complejos que resuelvan $z^4 = 16$, comenzamos tomando una raíz $\alpha = 2$ y multiplicándola por cada una de las cuatro raíces cuartas de la unidad, obteniendo con esto los complejos 2, $2i$, -2 y $-2i$, los cuales es sencillo comprobar son soluciones a la ecuación. Vamos precisar y generalizar lo mencionado anteriormente.

Definición 7.3. Sea m un entero positivo y sea α un número complejo. Un número complejo ζ se dice *una raíz m-ésima de α* si satisface

$$\zeta^m = \alpha.$$

Proposición 7.7. *Sea α un número complejo cualquiera. Si ζ es una raíz m-ésima de la unidad y η es una raíz m-ésima de α, entonces el producto $\zeta\eta$ es una raíz m-ésima de α.*

Se puede formular un teorema análogo al teorema 7.3 para las raíces m-ésimas de un complejo cualquiera donde se muestra que basta una raíz de la unidad, a decir

$$\cos\left(\frac{2\pi}{m}\right) + i\,\text{sen}\left(\frac{2\pi}{m}\right),$$

para generar todas las raíces m-ésimas del complejo en cuestión (ejercicio 7.11), mostrando que, por curioso que resulte, el caso fundamente es la obtención de las raíces de la unidad.

Debemos notar que las raíces segundas de las unidad 1 y -1 son también raíces cuartas y de la misma forma son raíces sextas. La pregunta que debemos responder es bajo qué condiciones las raíces m-ésimas de la unidad, son raíces también raíces n-ésimas.

Proposición 7.8. *Para un entero cualquiera n, si $m \mid n$, entonces cualquier raíz m-ésima de la unidad es una raíz n-ésima de la unidad.*

Demostración. Si ζ es una raíz m-ésima de la unidad, entonces $\zeta^m = 1$ y si $m \mid n$, entonces podemos encontrar q de forma que $n = qm$ por lo que

$$\zeta^n = \zeta^{qm} = (\zeta^m)^q = 1^q = 1,$$

por lo que ζ es una raíz n-ésima como afirmamos en el enunciado de la proposición. ∎

De alguna forma, la proposición nos indica que la raíces de la unidad se pueden distinguir entre ellas. Por ejemplo, en las raíces cuartas 1 y -1 son raíces segundas, pero i y $-i$ son raíces que no son ni terceras, ni segundas ni primeras. ¿Qué tienen de especial? La siguiente definición es la piedra angular para distinguirlas.

Definición 7.4. Sea ζ una raíz m-ésima de la unidad. Decimos que ζ *tiene orden* n, si n es el menor entero positivo tal que $\zeta^n = 1$. Además, si el orden de la raíz coincide con m decimos que ζ es *una raíz m-ésima primitiva*.

Para ilustrar la definición, consideremos de nueva cuenta las raíces cuartas. Por un lado 1 tiene orden 1, -1 orden 2 mientras que i y $-i$ tienen orden 4. Eso quiere decir que tanto i y como $-i$ son primitivas. Esta definición, además de permitirnos clasificar a las raíces de la unidad, nos deja distinguir la raíz m-ésima que inició esta discusión aparte de permitirnos dar un resultado contrapositivo de la proposición 7.8. Sin embargo, antes de continuar, debemos mostrar que las raíces primitivas existen en el caso general.

Proposición 7.9. *Para cada entero positivo m, existe una raíz m-ésima primitiva de la unidad indicada por*

$$\zeta = \cos\left(\frac{2\pi}{m}\right) + i\,\text{sen}\left(\frac{2\pi}{m}\right).$$

Demostración. Por la identidad de De Moivre,

$$\begin{aligned}\zeta^m &= \cos\left(\frac{2\pi m}{m}\right) + i\,\text{sen}\left(\frac{2\pi m}{m}\right)\\ &= 1.\end{aligned}$$

Ahora, debemos probar que el orden coincide con m. Para mostrar esto supongamos que n es el orden de ζ, i.e., es el entero positivo más pequeño de forma que $\zeta^n = 1$. En ese caso, se debe tener que $0 < n \leq m$ y además

$$1 = \zeta^n = \cos\left(\frac{2\pi n}{m}\right) + i\,\text{sen}\left(\frac{2\pi n}{m}\right).$$

Tenemos entonces que $\cos\left(\frac{2\pi n}{m}\right) = 1$ y como $0 < \frac{2\pi n}{m} \leq 2\pi$, la única posibilidad resulta en satisfacer $\frac{2\pi n}{m} = 2\pi$, o en otras palabras $n = m$. Lo anterior nos faculta para concluir que ζ es una raíz primitiva. ■

Proposición 7.10. *Sea ζ una raíz m-ésima primitiva. Entonces, si n es un entero que satisface $\zeta^n = 1$, se debe tener que $m \mid n$.*

Demostración. Comencemos expresando $n = qm + r$ con $0 \leq r < m$, usando el teorema de la división. En ese caso,

$$1 = \zeta^n = \zeta^{qm+r} = \zeta^{qm}\zeta^r = \zeta^r.$$

Como ζ es primitiva, la única posibilidad es tener $r = 0$ (de otra forma ζ no sería primitiva), en ese caso $m \mid n$ como afirma el enunciado. ■

La proposición anterior, es en realidad una forma particular de un resultado mucho más general que nos indica cómo obtener todas raíces primitivas a partir de solamente una.

Teorema 7.11. *Sea ζ una raíz m-ésima primitiva. Entonces, para un entero positivo k, el complejo ζ^k es una raíz primitiva si y sólo si $(m,k) = 1$.*

Demostración. Para probar que asumir ζ^k como una raíz primitiva, implica que $(m,k) = 1$, usaremos contraposición. Supongamos entonces que $(m,k) \neq 1$, como el máximo común divisor de dos positivos es distinto de 0, entonces $(m,k) > 1$. Tomemos ahora $m = m'(m,k)$ y $k = k'(m,k)$, en particular debemos tener que $m' < m$ y además

$$(\zeta^k)^{m'} = (\zeta^{km'}) = \zeta^{k'm'(m,k)} = (\zeta^m)^{k'} = 1;$$

lo que nos deja concluir que el orden de ζ^k es cuando más m' lo cual indica que ζ^k es no es primitiva. Hemos probado que, si $(m,k) \neq 1$, entonces ζ^k no es primitiva, lo que nos permite concluir el resultado que buscamos por contraposición.

Supongamos ahora que $(m,k) = 1$ y tomemos n como el orden de ζ^k, esto quiere decir que

$$\zeta^{kn} = \left(\zeta^k\right)^n = 1.$$

De acuerdo a la proposición 7.10, se debe tener $m \mid kn$ y como $(m,k) = 1$, el lema de Euclides garantiza $m \mid n$ por lo que $m \leq n$. Además

$$\left(\zeta^k\right)^m = (\zeta^m)^k = 1$$

lo que nos lleva a concluir que m es el orden de ζ^k obteniendo así ζ^k como una raíz primitiva como buscábamos. ∎

Corolario 7.12. *Si p es un primo y ζ es una raíz p-ésima primitiva, entonces para cualquier entero k que cumpla con $0 \leq k < p$, ζ^k es una raíz p-ésima primitiva.*

Una segunda mirada al teorema 7.11, nos permite encontrar cierta relación con el corolario 3.19, además su corolario resulta muy parecido al teorema 4.6. En una linda sorpresa, los enteros $\mathbb{Z}_m$ y las raíces m-ésimas guardan una relación importante, pero para explicarla, es necesario desarrollar un poco más de terminología de un concepto con el que ya nos hemos topado un par de veces pero que no hemos formalizado.

Ejercicios

Ejercicio 7.1. Sea $S^1 = \{x \in \mathbb{R}^2 \mid |x| = 1\}$, i.e., el círculo de radio unitario. Describe explícitamente una función $f\colon S^1 \to S^1$ de forma que la imagen de un polígono regular resulta en el mismo polígono regular rotado φ grados.

Ejercicio 7.2. Muestra que si ζ es una raíz n-ésima de la unidad, entonces $|\zeta| = 1$.

Ejercicio 7.3. Calcula las ocho las raíces octavas de la unidad.

Ejercicio 7.4. Prueba la proposición 7.7.

Ejercicio 7.5. Muestra que si ζ es una raíz m-ésima de la unidad, entonces ζ^{-1} es también una raíz m-ésima de unidad.

Ejercicio 7.6. Muestra que si ζ es una raíz m-ésima de la unidad, entonces ζ^k es también una raíz m-ésima de unidad para cualquier entero positivo k.

Ejercicio 7.7. Encuentra todas las raíces sextas de la unidad que son primitivas.

Ejercicio 7.8. Prueba el corolario 7.12.

Ejercicio 7.9. Sea ζ una raíz m-ésima de la unidad. Demuestra que ζ es primitiva si y sólo si, en la sucesión $\zeta^0, \zeta^1, \ldots, \zeta^{m-1}$, los elementos son todos distintos entre sí.

Ejercicio 7.10. Sean $x \geq 0$ y $y \geq 0$. Muestra que si $x\cos\varphi = y\cos v$ y $x\operatorname{sen}\varphi = y\operatorname{sen} v$, entonces $x = y$ y $\varphi = v + 2\pi k$.

Ejercicio 7.11. Sea $\alpha = r(\cos\theta + i\operatorname{sen}\theta)$ un número complejo expresado en coordenadas polares.

1. Demuestra que η es una raíz m-ésima de α.

$$\eta = \sqrt[m]{r}\left(\cos\left(\frac{\theta}{m}\right) + i\operatorname{sen}\left(\frac{\theta}{m}\right)\right).$$

2. Muestra que cualquier raíz m-ésima de α se puede escribir como $\zeta^k\eta$ para algún $0 \leq k < m$ y

$$\zeta = \cos\left(\frac{2\pi}{m}\right) + i\operatorname{sen}\left(\frac{2\pi}{m}\right)$$

Sugerencia: Para mostrar 2., usa una analogía de la prueba del teorema 7.3 y el ejercicio anterior.

Referencias

[Kur77] Kurosch, Alexander G.: *Curso de álgebra superior*. Editorial MIR, 1ª edición, 1977.

Las notas anteriores juegan algunas veces a ser un simple resumen de lo que otros autores han presentado, otras menos a reinterpretarlo y en una cantidad ínfima de ocasiones intentan pobremente aumentalo. El único objectivo real al que sirven, es preparar el curso de Álgebra Superior II impartido en la carrera de Actuaría de la FES Acatlán. Su versión es, en consecuencia, susceptible a errores gramaticales, imprecisiones técnicas y cambios constantes.