Álgebra Lineal en Física e Instrumentación Espacial

TEXTOS UNIVERSITARIOS
CIENCIAS

UAH

Plaza de San Diego, s/n
28801 Alcalá de Henares
www.uah.es

I.S.B.N.: 978-84-18979-83-5

Composición: Solana e Hijos, A. G., S.A.U.
Impresión y encuadernación: Solana e Hijos, A.G., S.A.U.
Impreso en España

Álgebra Lineal en Física e Instrumentación Espacial

Juan Gerardo Alcázar

Universidad de Alcalá

EDITORIAL
UNIVERSIDAD DE ALCALÁ

Índice general

Introducción.

Estas notas están basadas en el curso sobre Álgebra Lineal del Grado en Física e Instrumentación Espacial de la Universidad de Alcalá. Cubren los temas clásicos del Álgebra Lineal (sistemas de ecuaciones lineales, espacios vectoriales, aplicaciones lineales, diagonalización y espacios euclídeos), más algunos temas de Geometría (isometrías vectoriales, espacio afín, movimientos rígidos en el plano y el espacio e introducción a las cónicas). Las notas comienzan, además, con un tema sobre números complejos.

Resulta difícil definir qué es el Álgebra Lineal cuando los conocimientos con los que cuenta el posible lector son, sobre todo, los de Bachillerato. Una definición informal podría ser que el Álgebra Lineal es el estudio de diversos temas en Matemáticas que, en último término, pueden reducirse al estudio de sistemas de ecuaciones lineales. Otra posible descripción informal es que el Álgebra Lineal trata de cuestiones que pueden expresarse, todas ellas, en forma matricial. Ambos son intentos nobles de proporcionar una idea intuitiva, próxima a la experiencia del lector. Lo cierto, en cualquier caso, es que el lector descubrirá pronto que el Álgebra Lineal es una disciplina abstracta.

El Álgebra tiene que ver con la noción de *estructura*: la naturaleza de los objetos con los que trabajemos no nos importa demasiado; lo que nos importa es el tipo de operaciones que pueden llevarse a cabo dentro del conjunto en el que trabajemos, y sus propiedades. Quizá el lector atraído por la Física sienta algún tipo de rechazo hacia lo abstracto, pero lo cierto es que buena parte de la Física actual es fuertemente abstracta. La Teoría de la Relatividad se desarrolla en un espacio-tiempo tetradimensional, que no podemos imaginar, aunque sí describir mediante ecuaciones, y habla de un universo curvado por la gravedad. La Física Cuántica es contraintuitiva, aunque su desarrollo formal concuerda perfectamente con las observaciones. La Mecánica de Fluidos tiene una complejidad matemática considerable, hasta el punto de que puede encontrarse, como campo de investigación, no sólo dentro de la Física, sino también de las Matemáticas, con algunos problemas célebres aún no resueltos.

En casos como los de la Teoría de la Relatividad o la Física Cuántica la intuición nos falla, pero tenemos una estructura y unas reglas formales con las que podemos trabajar. En Álgebra la situación es similar, aunque tendremos a mano un buen número de ejemplos sencillos para ayudarnos a interiorizar esas estructuras y reglas formales. Los conjuntos de vectores y puntos del plano y el espacio, las matrices o los polinomios, todos ellos objetos familiares, nos servirán de ayuda para integrar conceptos más abstractos como el de espacio vectorial o espacio afín.

Familiarizarse con las definiciones del Álgebra Lineal lleva tiempo. Los conceptos abstractos tienden a volatilizarse, y es necesario volver sobre ellos una y otra vez hasta que se asientan. La recompensa es un conjunto de temas que, más allá de su belleza intrínseca, son aplicables en el desarrollo de la tecnología GPS, en el análisis de señales, en la resolución de circuitos, en la modelización de movimientos en el plano y el espacio (reflexiones, giros, traslaciones) y en el estudio de las curvas que siguen los cuerpos que se mueven bajo la acción de fuerzas gravitatorias (curvas cónicas). Quizá los primeros pasos no sean fáciles, pero si el lector persevera, le aguarda un mundo maravillosamente ordenado, que le será de utilidad también en otras asignaturas relacionadas con Matemáticas, Física o Ingeniería.

Siendo el Álgebra Lineal una disciplina muy clásica, la bibliografía existente es abundante. Al final de estas notas se proporcionan diversas sugerencias de obras y textos donde se abordan tanto la teoría (que es lo que ocupa a estas notas) como problemas y ejercicios relacionados con el Álgebra Lineal. La bibliografía sugerida permite también profundizar y ampliar los contenidos de estas notas en otros temas relacionados con el Álgebra Lineal (análsisis matricial, descomposiciones matriciales, programación lineal, teoría de juegos, estadística, etc.) que no se abordan aquí.

Capítulo 1

Números complejos.

Cuando tratamos de calcular las soluciones de la ecuación $x^2 + x + 1 = 0$, obtenemos

$$x = \frac{-1 \pm \sqrt{-3}}{2}.$$

Como $\sqrt{-3}$ no es un número real, es decir, no hay nada en el universo que mida $\sqrt{-3}$, decimos que la ecuación no tiene soluciones reales. Sin embargo, en el siglo XVI Gerolamo Cardano tuvo el atrevimiento de hacer lo siguiente: llamó $i = \sqrt{-1}$ (es decir, $i^2 = -1$), y por tanto concluyó que las soluciones de la ecuación $x^2 + x + 1 = 0$ eran

$$x_1 = \frac{-1}{2} + \frac{\sqrt{3}}{2}i, \; x_1 = \frac{-1}{2} - \frac{\sqrt{3}}{2}i.$$

Estas expresiones no pueden interpretarse en términos de “cantidades”, pero sí son expresiones formales que pueden operarse. De hecho, para Cardano estas expresiones eran “intermediarias”que podían llevar a expresiones reales. En concreto, Cardano desarrolló un método para resolver ecuaciones cúbicas, que requería pasar por este tipo de expresiones. Por ejemplo, las soluciones de la ecuación cúbica

$$x^3 - 15x - 4 = 0$$

(`https://es.wikipedia.org/wiki/Ecuación_de_tercer_grado`) son, utilizando el método de Cardano,

$$\begin{array}{rcl} x_1 & = & (2+i) + (2-i) = 4, \\ x_2 & = & \omega(2+i) + \omega^2(2-i) = -2 + \sqrt{3}, \\ x_3 & = & \omega^2(2+i) + \omega(2-i) = -2 - \sqrt{3}, \end{array}$$

donde $\omega = \frac{-1}{2} + \frac{\sqrt{3}}{2}i$, $\omega^2 = \frac{-1}{2} - \frac{\sqrt{3}}{2}i$.

Posteriormente, este tipo de expresiones, que recibieron el nombre de *números complejos*, se fueron popularizando no sólo en Matemáticas, sino también en Física o Ingeniería, y son imprescindibles en campos como la Física Cuántica, la Mecánica de Fluidos o el Análisis de Circuitos. A su vez, en Matemáticas los números complejos se utilizan en muchas áreas, porque tienen menos restricciones que los reales: por ejemplo, sobre los complejos (sobre los reales esto no es cierto) toda ecuación polinómica (como las que aparecen en esta introducción) tiene solución, y de hecho tantas soluciones como indique su grado. Además, los números complejos tienen una cierta correspondencia con los vectores del plano, y de hecho algunas transformaciones geométricas (por ejemplo, traslaciones y rotaciones) pueden representarse con números complejos.

1.1. Conceptos generales.

Definición 1. *Un* **número complejo** *es una expresión de la forma* $z = a + ib$*, donde* $a, b \in \mathbb{R}$*, y* $i = \sqrt{-1}$*. Los valores* a, b *reciben el nombre de* **parte real** *y* **parte imaginaria***, respectivamente, del número complejo* z*; se escribe*

$$a = \mathrm{Re}(z), \;\; b = \mathrm{Im}(z).$$

El conjunto de todos los números complejos, es decir, de todas las expresiones de la forma anterior, se representa por $\mathbb{C}$. Resulta claro que si $b = 0$ entonces $z \in \mathbb{R}$, es decir, es un número real. Por lo tanto, $\mathbb{R} \subset \mathbb{C}$: el símbolo $\subset$ significa que el conjunto $\mathbb{R}$ está incluido en el conjunto de $\mathbb{C}$ (y no al revés), con lo que decimos que $\mathbb{C}$ *amplía* $\mathbb{R}$ (le contiene, e incorpora otros elementos que no pueden entenderse como números reales). Además, si $a = 0$ decimos que $z = ib$ es un **número imaginario puro**. A la expresión $a+ib$ se la llama **forma binómica** del complejo z; en breve veremos que hay otras maneras, alternativas, de representar un número complejo.

Por lo tanto, un número complejo z se corresponde con un par (a, b) de números reales, como también les sucede a los puntos del plano, y a los vectores del plano. De hecho, todo número complejo $z = a+ib$ se puede representar en el plano como un vector cuyo origen es el origen de coordenadas, y cuyo extremo es el punto de coordenadas (a, b): a dicho vector se le llama **afijo** del complejo z (ver Fig. 1.1).

Además, la longitud del afijo se llama **módulo** del número complejo (ver Fig. 1.1), y se representa por ρ, o también por $|z|$. El ángulo que va desde el semieje positivo de las x hasta el afijo, se llama **argumento** del número complejo (ver Fig. 1.1), y se representa por θ, o también por $\arg(z)$. Observemos que θ no es único, puesto que, asumiendo que θ está en radianes, $\theta + k \cdot 2\pi$, con $k \in \mathbb{Z}$ (esta expresión corresponde a sumar a θ un número entero de vueltas completas) nos define el mismo complejo; volveremos sobre esto más tarde, cuando hablemos de las raíces n-ésimas de un complejo.

Si conocemos ρ, θ tenemos identificado el extremo del afijo, y por lo tanto el número complejo en sí. En consecuencia, otra forma de representar el número complejo, alternativa a la forma binómica, es mediante el par (ρ, θ); en concreto, se llama **forma polar** del complejo a la expresión

$$z = \rho_\theta.$$

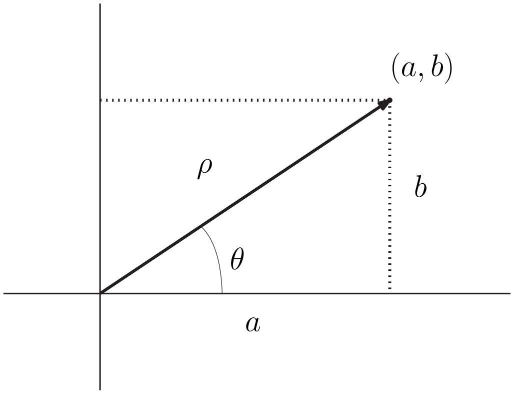

Figura 1.1: Afijo, módulo y argumento de un número complejo

En Fig. 1.1 observamos que se forma un triángulo rectángulo cuyos catetos son a, b, y cuya hipotenusa es ρ, siendo θ el ángulo opuesto a b. Por lo tanto, se tiene

$$\rho = \sqrt{a^2 + b^2},\ \theta = \text{arc tg}\frac{b}{a};\ a = \rho\cos(\theta),\ b = \rho\text{sen}(\theta).$$

Las dos primeras relaciones se utilizan para obtener ρ, θ a partir de la forma binómica. Insertando las dos segundas en la expresión de la forma binómica $z = a + ib$ del complejo, se obtiene

$$z = \rho\cos(\theta) + i\rho\text{sen}(\theta) = \rho(\cos(\theta) + i\text{sen}(\theta)),$$

que recibe el nombre de **forma trigonométrica del complejo**. Además, teniendo en cuenta el mismo triángulo rectángulo, y dado que la hipotenusa de un triángulo rectángulo es siempre mayor o igual que cualquiera de sus catetos, se tiene que $\forall z \in \mathbb{C}$,

$$\text{Re}(z) \leq |z|,\ \text{Im}(z) \leq |z|.$$

Definición 2. *El* **conjugado** *de un número complejo $z = a + ib$ es el número complejo $\overline{z} = a - ib$.*

Por lo tanto, el conjugado de un número complejo es otro número complejo que tiene la misma parte real, pero cuya parte imaginaria está cambiada de signo. En Fig. 1.2 se muestra el afijo de un número complejo (en negro) y de su conjugado (en rojo); es obvio que el afijo correspondiente al conjugado es el simétrico del afijo original respecto del eje horizontal. Además, el módulo del conjugado coincide con el del complejo original, y su argumento coincide con el del complejo original, cambiado de signo (porque el sentido positivo para medir ángulos es el antihorario).

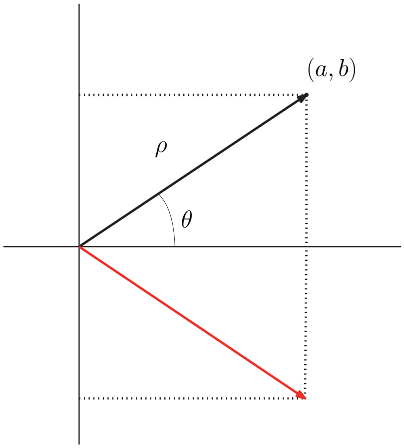

Figura 1.2: Conjugado de un número complejo

Se tienen entonces las siguientes propiedades (la única que no hemos mencionado antes es la primera de ellas):

- Un número complejo es real si y sólo si coincide con su conjugado. En notación matemática, $z \in \mathbb{R} \Leftrightarrow z = \overline{z}$.
- $|\overline{z}| = |z|$.
- $\arg(\overline{z}) = -\arg(z)$.

1.2. Operaciones con números complejos.

A las expresiones $z = a + ib$ se les da el nombre de "números"porque se pueden operar. De hecho, todas las operaciones que pueden realizarse con números reales (suma, resta, multiplicación, división, potencias, raíces,...) pueden realizarse también con números complejos.

Definición 3. *Dados $z_1, z_2 \in \mathbb{C}$, $z_1 = a_1 + ib_1$, $z_2 = a_2 + ib_2$, se define la* **suma** $+$ *de z_1, z_2 como*

$$z_1 + z_2 = (a_1 + a_2) + i(b_1 + b_2).$$

Se define el **producto** $\cdot$ *de z_1, z_2 como*

$$z_1 \cdot z_2 = (a_1a_2 - b_1b_2) + i(a_1b_2 + a_2b_1).$$

Para sumar dos números complejos, sumamos las partes reales, por un lado, y las imaginarias, por otro. Geométricamente, la suma de complejos se corresponde con la suma

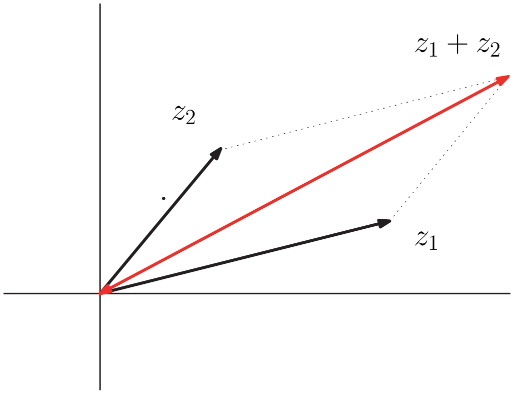

Figura 1.3: Suma de números complejos

de vectores (ver Fig. 1.3): puesto que cada complejo viene, de hecho, representado por un vector del plano (y viceversa), no resulta raro que la suma de complejos se corresponda con la suma de vectores. De hecho, lo que se representa en la Fig. 1.3 es la *regla del paralelogramo* para sumar dos vectores planos.

Para restar dos números complejos, sumamos al primero el **opuesto** del segundo, donde el opuesto de $z = a + ib$ se define como $-z = -a - ib$. Respecto a la multiplicación de números complejos, corresponde a la multiplicación de polinomios, donde i hace el papel de la variable x, pero teniendo en cuenta que $i^2 = -1$.

En Álgebra nos interesan las operaciones que satisfacen determinadas buenas propiedades, que se dan en contextos muy diferentes. En concreto, la suma de números complejos verifica las siguientes propiedades:

1. *Asociativa*: $\forall z_1, z_2, z_3 \in \mathbb{C}$,

$$z_1 + (z_2 + z_3) = (z_1 + z_2) + z_3.$$

   Esencialmente, la propiedad asociativa nos dice que a la hora de sumar *tres* complejos podemos empezar sumando los dos primeros, y luego sumar el resultado con el tercero, o bien los dos últimos, y luego sumar el resultado con el primero. En particular, para sumar tres complejos podemos escribir, simplemente, $z_1 + z_2 + z_3$, sin necesidad de paréntesis.

2. *Elemento neutro*: existe $e \in \mathbb{C}$ tal que $\forall z \in \mathbb{C}$,

$$z + e = e + z = z.$$

   El elemento neutro de la suma de complejos es $0 = 0 + i \cdot 0$.

3. *Elemento opuesto*: $\forall z \in \mathbb{C}$, existe otro número complejo ω tal que

$$z + \omega = \omega + z = e$$

   El elemento opuesto de la suma de complejos es $-z$: si $z = a + ib$, $-z = -a - ib$.

4. *Conmutativa*: $\forall z_1, z_2 \in \mathbb{C}$,

$$z_1 + z_2 = z_2 + z_1.$$

   La propiedad conmutativa nos dice que el orden, a la hora de sumar dos complejos, no importa. Si a esta propiedad le unimos la asociativa, lo que nos dicen conjuntamente es que sumar una cantidad arbitraria de complejos puede hacerse en el orden que deseemos.

Cuando un conjunto satisface las tres primeras propiedades (asociativa, existencia de elemento neutro y existencia de elemento opuesto), se dice que tiene estructura de **grupo**. Si además verifica la cuarta (conmutativa), se dice que forma un **grupo conmutativo o abeliano**. Decimos que $(\mathbb{C}, +)$ es un grupo conmutativo. Esta estructura aparece en muchos otros contextos, en Matemáticas: por ejemplo, los números enteros, con la operación suma, o las matrices, también con la operación suma, forman grupos conmutativos; sin embargo, las matrices cuadradas con la operación producto no lo forman, porque no toda matriz es invertible.

El producto de números complejos satisface las siguientes propiedades:

1. *Asociativa*: $\forall z_1, z_2, z_3 \in \mathbb{C}$,

$$z_1 \cdot (z_2 \cdot z_3) = (z_1 \cdot z_2) \cdot z_3.$$

2. *Elemento neutro*: existe $\tilde{e} \in \mathbb{C}$ tal que $\forall z \in \mathbb{C}$,

$$z \cdot \tilde{e} = \tilde{e} \cdot z = z.$$

   En el caso del producto, el elemento neutro es $1 = 1 + i \cdot 0$.

3. *Elemento opuesto*: $\forall z \in \mathbb{C} - \{0\}$, existe otro número complejo $\tilde{\omega}$ tal que

$$z \cdot \tilde{\omega} = \tilde{\omega} \cdot z = \tilde{e}$$

   Si $z = a + ib$, el elemento opuesto (que en este contexto se suele llamar "inverso") es

$$\frac{1}{z} = \frac{1}{a + ib} = \frac{a - ib}{a^2 + b^2} = \frac{a}{a^2 + b^2} - i\frac{b}{a^2 + b^2},$$

   lo cual se puede comprobar multiplicando el complejo anterior por $a + ib$, y viendo que obtenemos 1. La expresión anterior se ha obtenido multiplicando y dividiendo por el conjugado del denominador, $a - ib$, y teniendo en cuenta que $(a + ib)(a - ib) = a^2 - i^2b^2 = a^2 + b^2$. El único número complejo que no tiene un inverso, es 0.

4. *Conmutativa*: $\forall z_1, z_2 \in \mathbb{C}$,
$$z_1 \cdot z_2 = z_2 \cdot z_1.$$

Por lo tanto, $(\mathbb{C} - \{0\}, \cdot)$ también forma un grupo conmutativo. Además, se tiene la propiedad *distributiva* del producto respecto a la suma: $\forall z_1, z_2, z_3 \in \mathbb{C}$,

$$z_1 \cdot (z_2 + z_3) = z_1 \cdot z_2 + z_1 \cdot z_3.$$

La propiedad distributiva nos dice que para multiplicar un complejo por una suma, podemos multiplicar el complejo por cada uno de los términos de la suma, y sumar después. Es una propiedad que también verifican, por ejemplo, los números enteros, o las matrices cuadradas, con sus sumas y sus productos.

Finalmente, se tiene entonces que en $\mathbb{C}$ tenemos dos operaciones, $+$ y $\cdot$, que verifican: (1) $(\mathbb{C}, +)$ es un grupo conmutativo; (2) $(\mathbb{C} - \{0\}, \cdot)$ es un grupo conmutativo; (3) La operación $\cdot$ es distributiva respecto de la operación $+$. Cuando en un conjunto se dan (1)+(2)+(3), es decir, tenemos dos operaciones que cumplen lo anterior, se dice que el conjunto, junto con esas operaciones, forma un **cuerpo conmutativo**. Por lo tanto, $(\mathbb{C}, +, \cdot)$ es un cuerpo conmutativo. El conjunto de los números racionales, $\mathbb{Q}$, o el de los reales, $\mathbb{R}$, con la suma y el producto habituales, también son cuerpos conmutativos. Sin embargo, los enteros no, porque no todo entero tiene un inverso; y las matrices cuadradas, tampoco.

Lema 4. *Sean $z, z_1, z_2 \in \mathbb{C}$, $z = a + ib$. Son ciertas:*

(1) $z \cdot \overline{z} = |z|^2$.

(2) $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$ *(El conjugado de la suma es la suma de los conjugados).*

(3) $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$ *(El conjugado del producto es el producto de los conjugados).*

(4) $|z_1 + z_2| \leq |z_1| + |z_2|$.

(5) Se tiene
$$a = \frac{z + \overline{z}}{2}, \ b = \frac{z - \overline{z}}{2i}.$$

(6) $\overline{\overline{z}} = z$ *(El conjugado del conjugado de un complejo z, es él mismo).*

Demostración. En el caso de (1), si $z = a+ib$, entonces $\overline{z} = a-ib$, y $z \cdot \overline{z} = (a+ib)(a-ib) = a^2 + b^2 = |z|^2$. Para (2), si $z_1 = a_1 + ib_1$ y $z_2 = a_2 + ib_2$, entonces

$$\overline{z_1 + z_2} = \overline{(a_1 + a_2) + i(b_1 + b_2)} = (a_1 + a_2) - i(b_1 + b_2) = (a_1 - ib_1) + (a_2 - ib_2) = \overline{z_1} + \overline{z_2}$$

Para (3), se procede como en (2) (queda como ejercicio). Para (4), puede procederse geométricamente, observando en Fig. 1.3 que para que el triángulo formado por los afijos de $z_1, z_2, z_1 + z_2$ pueda cerrarse, cada lado debe ser menor o igual que la suma de los otros dos, o bien de forma algebraica (posible ejercicio para las clases de prácticas). Para demostrar (5) basta observar que si $z = a + ib$, entonces $\overline{z} = a - ib$; sumando entonces ambas expresiones se tiene la expresión buscada para a, y restándolas, la de b. Finalmente, (6) es fácil y se deja como ejercicio. $\square$

1.3. Forma exponencial de un complejo: definición y operaciones.

En las secciones anteriores hemos visto varias formas de representar un número complejo, en concreto las formas binómica, polar y trigonométrica. Ahora vamos a introducir una forma más, que descansa sobre la siguiente igualdad, llamada *fórmula de Euler*; la justificación de esta fórmula requiere algo que se verá en Cálculo I, llamado *desarrollo en serie Taylor*. La fórmula de Euler es la siguiente:

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

Probablemente sorprenderá el hecho de que elevar el número e a un número complejo tenga sentido. En realidad, como se verá en la asignatura de Métodos Matemáticos de la Física, tiene sentido aplicar todas las funciones conocidas (senos, cosenos, exponenciales, logaritmos, etc.) a los números complejos; de hecho, toda la teoría de funciones de variable real (la noción de derivabilidad, integrabilidad, etc.) se puede generalizar al caso complejo, aunque adaptando las ideas y las técnicas.

Definición 5. *Sea $z = a + ib$, y sean ρ, θ el módulo y el argumento (en radianes!!) de z. La* **forma exponencial** *del complejo z es*

$$z = \rho e^{i\theta}.$$

A partir de la fórmula de Euler, la expresión anterior se justifica fácilmente utilizando la forma trigonométrica del complejo. La razón para introducir esta última representación es que el producto y el cociente de números complejos son fáciles de calcular a partir de ella (no así la suma); además, con esta representación es fácil introducir las potencias y el cálculo de raíces.

Veamos entonces las siguientes operaciones en forma exponencial:

(1) **Producto:** sean $z_1 = \rho_1 e^{i\theta_1}$, $z_2 = \rho_2 e^{i\theta_2}$. Entonces

$$z_1 \cdot z_2 = \rho_1 e^{i\theta_1} \cdot \rho_2 e^{i\theta_2} = (\rho_1 \cdot \rho_2) e^{i(\theta_1+\theta_2)}.$$

Podemos traducir esto de la siguiente manera: *el módulo del producto es igual al producto de los módulos, y el argumento del producto es igual a la suma de los argumentos.*

(2) **División:** sean $z_1 = \rho_1 e^{i\theta_1}$, $z_2 = \rho_2 e^{i\theta_2}$. Entonces

$$\frac{z_1}{z_2} = \frac{\rho_1 e^{i\theta_1}}{\rho_2 e^{i\theta_2}} = \frac{\rho_1}{\rho_2} e^{i(\theta_1-\theta_2)}.$$

Podemos traducir esto como: *el módulo del cociente es igual al cociente de los módulos, y el argumento del cociente es igual a la resta de los argumentos.*

(3) **Potencia:** sea $z = \rho e^{i\theta}$. Entonces

$$z^n = \left(\rho e^{i\theta}\right)^n = \rho^n e^{in\theta}.$$

La expresión anterior se justifica fácilmente porque $z^n = z \overset{n}{\cdots} z$, y utilizando después la forma exponencial del producto.

Finalmente, vamos a introducir una operación más, en concreto la **raíz enésima** de un número complejo. Esta operación tiene también sentido sobre los números reales: $\sqrt[3]{-8} = -2$, porque $(-2)^3 = -8$; $\sqrt{16} = 4$ porque $4^2 = 16$. Por lo tanto, si queremos calcular, digamos, $\sqrt[5]{z}$, estamos buscando otro complejo (u otros complejos) ω con la propiedad de que $\omega^5 = z$. Es claro que en $\mathbb{R}$ esta operación no siempre tiene sentido: por ejemplo, $\sqrt{-1}$ no tiene sentido en $\mathbb{R}$. Veremos que en $\mathbb{C}$ siempre lo tiene.

(4) **Raíz n-ésima:** sea $z = \rho e^{i\theta}$. Queremos encontrar $\sqrt[n]{z}$, es decir, $\omega \in \mathbb{C}$ tal que $\omega^n = z$. Lo primero que debemos observar es que, en $\mathbb{C}$, todo complejo tiene dos raíces cuadradas, tres raíces cúbicas, cuatro raíces cuartas... y n raíces n-ésimas. Sobre los reales tenemos una versión mucho más débil de este fenómeno con las raíces de índice par: si $a \in \mathbb{R}$, $a > 0$, y n es par, entonces a tiene dos raíces de índice n. Por ejemplo, 4 tiene dos raíces cuadradas, 2 y -2, porque $2^2 = (-2)^2 = 4$; es cierto que cuando encontramos $\sqrt{4}$ tomamos, por convenio, de esas dos, la que tiene el signo que se muestra delante de la raíz (positivo), pero hay dos.

Para convencernos de que todo complejo tiene n raíces n-ésimas, y para ver cómo encontrarlas, recurrimos de nuevo a la forma exponencial, pero explotando el hecho de que el argumento de un número complejo no es único. Es decir,

$$z = \rho e^{i\theta} = \rho e^{i(\theta + 2k\pi)}, \ k \in \mathbb{Z}.$$

Calculemos entonces la raíz n-ésima de z. Se tiene

$$\sqrt[n]{z} = \sqrt[n]{\rho e^{i(\theta+2k\pi)}} = \sqrt[n]{\rho} e^{i\left(\frac{\theta}{n} + \frac{2k\pi}{n}\right)}.$$

Puesto que k puede tomar cualquier valor entero, al dar distintos valores a k vamos obteniendo las distintas raíces. En concreto, al substituir $k = 0, 1, 2, \ldots, n-1$ se obtienen

$$\sqrt[n]{e}^{i\left(\frac{\theta}{n}\right)}, \sqrt[n]{e}^{i\left(\frac{\theta}{n} + \frac{2\pi}{n}\right)}, \sqrt[n]{e}^{i\left(\frac{\theta}{n} + \frac{4\pi}{n}\right)}, \cdots, \sqrt[n]{e}^{i\left(\frac{\theta}{n} + \frac{2(n-1)\pi}{n}\right)}$$

Sin embargo, cuando damos el valor $k = n$, lo que obtenemos es

$$\sqrt[n]{e}^{i\left(\frac{\theta}{n} + 2\pi\right)} = \sqrt[n]{e}^{i\left(\frac{\theta}{n}\right)},$$

que corresponde a un complejo que ya habíamos obtenido (para $k = 0$). Es decir, al dar valores consecutivos a k, las raíces que encontramos se repiten al cabo de n valores (lo hemos observado empezando en $k = 0$, por simplicidad, pero sucede lo mismo si empezamos en cualquier otro valor de k). Por lo tanto, llegamos a las siguientes conclusiones:

- Todo número complejo $z = \rho e^{i\theta}$ tiene n raíces n-ésimas.
- Las raíces son:

$$\sqrt[n]{\rho}e^{i\left(\frac{\theta}{n}\right)}, \sqrt[n]{\rho}e^{i\left(\frac{\theta}{n}+\frac{2\pi}{n}\right)}, \sqrt[n]{\rho}e^{i\left(\frac{\theta}{n}+\frac{4\pi}{n}\right)}, \cdots , \sqrt[n]{\rho}e^{i\left(\frac{\theta}{n}+\frac{2(n-1)\pi}{n}\right)}$$

- Todas las raíces n-ésimas de un complejo $z = \rho e^{i\theta}$ tienen el mismo módulo, $\sqrt[n]{\rho}$, que coincide con la raíz n-ésima (positiva) del módulo ρ del complejo.
- Los argumentos de las raíces n-ésimas son:

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

  Aquí hay una regularidad, que resulta más clara si los escribimos así:

$$\frac{\theta}{n}, \frac{\theta}{n} + 1 \cdot \frac{2\pi}{n}, \frac{\theta}{n} + 2 \cdot \frac{2\pi}{n}, \ldots, \frac{\theta}{n} + (n-1) \cdot \frac{2\pi}{n}.$$

  En particular, si escribimos los sucesivos argumentos como $\theta_0, \theta_1, \theta_2, \ldots, \theta_{n-1}$, observamos que $\theta_0 = \dfrac{\theta}{n}$, y

$$\theta_{\ell+1} = \theta_\ell + \frac{2\pi}{n}$$

  para $\ell = 1, \ldots, n-2$, de manera que para pasar de un argumento al siguiente vamos sumando una cantidad fija, $\frac{2\pi}{n}$. Esta propiedad la interpretaremos geométricamente en la siguiente sección.

1.4. Traslaciones y rotaciones.

Como hemos visto en la sección anterior, al multiplicar dos complejos sus módulos se multiplican, y sus argumentos se suman. Si consideramos ahora un complejo de modulo unidad, es decir,

$$\omega_0 = 1 \cdot (\cos(\alpha) + i\mathrm{sen}(\alpha)) = e^{i\alpha},$$

y lo multiplicamos por un complejo cualquiera $z = \rho e^{i\theta}$, obtenemos

$$z \cdot \omega_0 = (\rho e^{i\theta}) \cdot e^{i\alpha} = \rho e^{i(\theta+\alpha)},$$

es decir, el módulo no varía, y el argumento se incrementa en α. La transformación que experimenta entonces el extremo del afijo de un complejo cuando se muliplica el complejo por un complejo de módulo unidad $e^{i\alpha}$ corresponde a un *giro* de centro el origen, y ángulo α (ver Fig. 1.4).

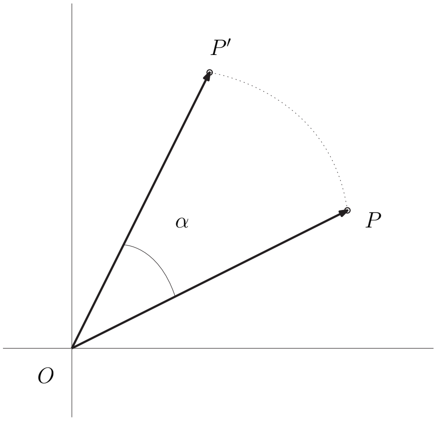

Figura 1.4: Giro en torno al origen

Con mayor detalle, un **giro** de centro el origen O, de ángulo α, es una transformación geométrica $\mathcal{G}_{O,\alpha}$ que transforma un punto P cualquiera en otro punto P', de modo que el vector OP' es el resultado de girar el vector OP en torno al origen un ángulo α (ver de nuevo Fig. 1.4). Si consideramos un centro cualquiera C, un **giro** de centro C y ángulo α es la transformación geométrica $\mathcal{G}_{C,\alpha}$ que transforma un punto P cualquiera en otro punto P', de modo que el vector CP' es el resultado de girar el vector CP en torno al punto C, un ángulo α (ver Fig. 1.5).

Una aplicación de lo anterior es el siguiente resultado sobre las raíces n-ésimas de un número complejo.

Teorema 6. *Los extremos de los afijos de las raíces n-ésimas de un número complejo son los vértices de un polígono regular de n lados.*

Demostración. Sea $z = \rho e^{i\theta}$. Sabemos que z posee n raíces n-ésimas, que llamamos $z_0, z_1, \ldots, z_{n-1}$, cuyos módulos son todos iguales y de valor $\sqrt[n]{\rho}$, y cuyos argumentos son

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

donde $\theta_0 = \frac{\theta}{n}$ y $\theta_{\ell+1} = \theta_\ell + \frac{2\pi}{n}$, con $\ell \in \{0, 1, \ldots, n-2\}$. Consideremos ahora dos raíces consecutivas, z_ℓ y $z_{\ell+1}$. Entonces

$$z_\ell = \sqrt[n]{\rho} e^{i\theta_\ell}, \ z_{\ell+1} = \sqrt[n]{\rho} e^{i\theta_{\ell+1}} = \sqrt[n]{\rho} e^{i\left(\theta_\ell + \frac{2\pi}{n}\right)}.$$

Por tanto,

$$z_{\ell+1} = \sqrt[n]{\rho} e^{i\theta_\ell} \cdot e^{i\frac{2\pi}{n}} = z_\ell \cdot e^{i\frac{2\pi}{n}},$$

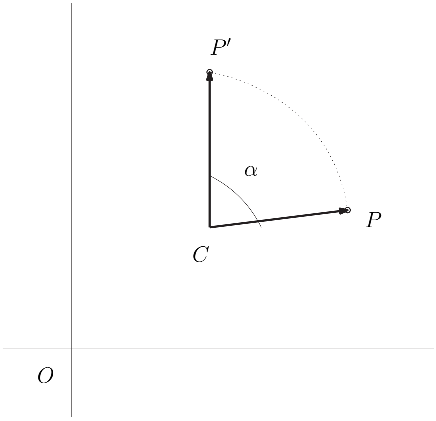

Figura 1.5: Giro en torno a un punto cualquiera

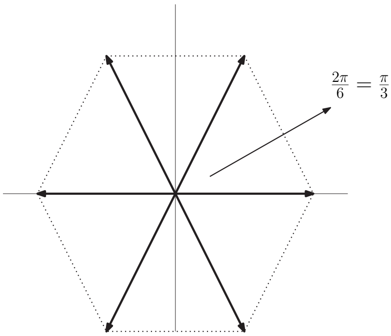

Figura 1.6: Raíces sextas de la unidad

es decir, cada raíz n-ésima se obtiene a partir de la anterior, multiplicando por el complejo $\omega_0 = e^{i\frac{2\pi}{n}}$, que tiene módulo 1. En consecuencia, geométricamente el afijo de cada raíz n-ésima se obtiene girando el afijo de la raíz anterior un ángulo $\frac{2\pi}{n}$ en torno al origen. Puesto que al cabo de n raíces se obtiene de nuevo la primera raíz (porque $n \cdot \frac{2\pi}{n} = 2\pi$), y puesto que todos los afijos tienen el mismo origen, que coincide con el origen de coordenadas, y el mismo módulo, los afijos de las sucesivas raíces van dibujando los vértices de un polígono regular de n lados (observemos que para un polígono regular de n-lados, todos los vértices están a la misma distancia del centro, que en este caso es el origen, y que el ángulo formado por los segmentos que unen el origen con dos vértices consecutivos es $\frac{2\pi}{n}$). $\square$

En Fig. 1.6, se observan los afijos de $\sqrt[6]{1}$, las raíces sextas de la unidad, que forman un hexágono regular.

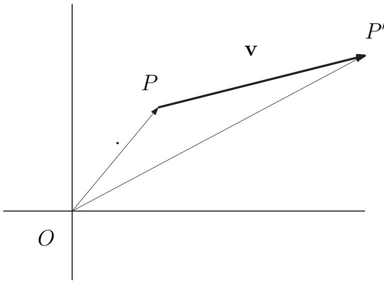

Figura 1.7: Traslación de vector $\mathbf{v}$

Respecto a la suma, cuando consideramos un complejo fijo z_0 y lo sumamos a otro complejo cualquiera z, la suma $z + z_0$ corresponde a la suma de los afijos de ambos. Así, la transformación que experimenta el extremo del afijo de un complejo cuando el complejo se suma con otro complejo z_0, corresponde a una **traslación** de vector igual al afijo del complejo z_0. Con más detalle, una **traslación** de vector $\mathbf{v}$ es una transformación geométrica $\tau_{\mathbf{v}}$ que transforma un punto P del plano en otro punto P' que verifica $PP' = \mathbf{v}$ (ver Fig. 1.7).

Ecuación de una traslación en forma compleja

Dado un vector $\mathbf{v}$, queremos encontrar las ecuaciones de una traslación de vector $\mathbf{v}$; es decir, una expresión que, a partir de un punto P, determine el punto P' tal que el vector PP' coincide con $\mathbf{v}$. Para ello, podemos beneficiarnos de los números complejos. Si llamamos z al complejo cuyo afijo es OP, y w al complejo cuyo afijo es OP', entonces $w = z + \mathbf{v}$, donde en esta expresión $\mathbf{v}$, por un abuso de notación, representa al complejo cuyas partes real e imaginaria son las coordenadas de $\mathbf{v}$ como vector. Puesto que las partes real e imaginaria de w son las de P', la expresión anterior permite encontrar P' a partir de $P, \mathbf{v}$. Si representamos por $\tau_{\mathbf{v}}$ a la traslación de vector $\mathbf{v}$ (que es una transformación geométrica), entonces $w = \tau_{\mathbf{v}}(z)$, y podemos escribir

$$\tau_{\mathbf{v}}(z) = z + \mathbf{v}.$$

Conocido un punto P (cuyo complejo correspondiente es z) y un vector $\mathbf{v}$, la expresión anterior nos da directamente el complejo que representa al punto P', trasladado de P según $\mathbf{v}$.

Ecuación de un giro en forma compleja

Comenzamos por un giro de centro el origen, y ángulo α; representamos por $\mathcal{G}_{O,\alpha}$ a dicha transformación. Dado un punto P, queremos encontrar el punto P' que resulta al girar P en torno a O, un ángulo α. De nuevo podemos utilizar números complejos para resolver este problema. Sea entonces z el complejo correspondiente a P, y w el complejo correspondiente a P' (que es lo que queremos encontrar) Como $w = z \cdot e^{i\alpha}$, esta expresión corresponde a la ecuación de la transformación. Podemos escribir

$$\mathcal{G}_{O,\alpha}(z) = z \cdot e^{i\alpha}.$$

Consideremos ahora un giro de centro un punto cualquiera C, y ángulo α; representamos por $\mathcal{G}_{C,\alpha}$ a la transformación correspondiente. Sean entonces los siguientes complejos:

- El complejo correspondiente al vector OP, que representamos por z, y que es conocido (porque P es el punto que queremos girar).

- El complejo correspondiente al vector OC, que representamos por z_0, y que es también conocido (porque C es el punto en torno al cuál queremos girar el punto P).

- El complejo correspondiente al vector OP', que representamos por w, y que queremos encontrar (es desconocido).

La relación entre estos complejos puede visualizarse en Fig. 1.8, utilizando dos números complejos auxiliares, llamados w_1, w_2, que corresponden a los vectores CP, CP', respectivamente. Observamos que CP' es el resultado de girar CP un ángulo α (de hecho, como los vectores que utilizamos son vectores libres, podemos considerar que ese giro es un giro en torno al origen, que en este caso correspondería, geométricamente, al punto C). Por lo tanto,

$$w_2 = w_1 \cdot e^{i\alpha}.$$

Ahora bien, como $CP = OP - OC$, $w_1 = z - z_0$; y como $CP' = OP' - OC$, $w_2 = w - z_0$. Por lo tanto,

$$w - z_0 = (z - z_0)e^{i\alpha}.$$

Despejando w y escribiendo $w = \mathcal{G}_{C,\alpha}(z)$, se tiene

$$\mathcal{G}_{C,\alpha}(z) = z_0 + (z - z_0)e^{i\alpha}.$$

1.5. Teorema fundamental del Álgebra.

Al principio del tema veíamos que, históricamente, el nacimiento de los números complejos estuvo vinculado a la resolución de ecuaciones polinómicas. En esta sección exploraremos un poco más la relación de los números complejos con este tipo de ecuaciones.

Definición 7. *Sea $P(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_0$ un polinomio donde $a_i \in \mathbb{C}$. Se dice que z_0 es una* **raíz** *de $P(z)$, si $P(z_0) = 0$.*

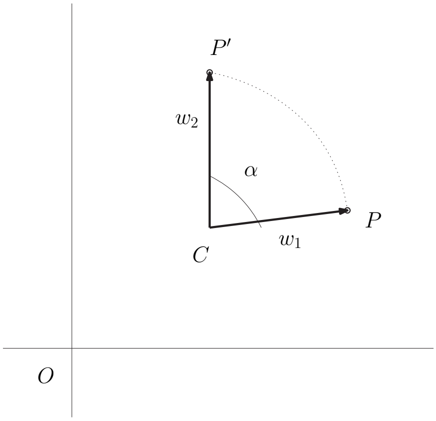

Figura 1.8: Ecuación de un giro en torno a un punto cualquiera

Por lo tanto, las raíces de un polinomio $P(z)$ son las soluciones de la ecuación $P(z) = 0$; de hecho, a veces se habla de las *raíces* de una ecuación para referirse a sus soluciones. Las raíces de un polinomio pueden ser reales o complejas: por ejemplo, las raíces de $P(z) = z^2-1$ son ± 1; las de $P(z) = z^2 + 1$ son $\pm i$. Sin embargo, el resultado siguiente nos dice que si un polinomio $P(z)$ *con coeficientes reales* (esto es esencial) tiene una raíz compleja $a + ib$, entonces también tiene que tener como raíz a su conjugada, $a - ib$; el resultado es falso si los coeficientes de $P(z)$ no son reales.

Lema 8. *Si $z_0 = a+bi$ es una raíz de un polinomio $P(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_0$ cuyos coeficientes son números reales (es decir, $a_i \in \mathbb{R}\ \forall i = 0, 1, \ldots, n$), entonces $\overline{z_0} = a - bi$ también es raíz de $P(z)$.*

Demostración. Si z_0 es raíz de $P(z)$, entonces, por definición de raíz, $P(z_0) = 0$; por lo tanto,

$$P(z_0) = a_n z_0^n + a_{n-1} z_0^{n-1} + \cdots + a_1 z_0 + a_0 = 0.$$

Tomando conjugados en la expresión anterior, y teniendo en cuenta que el conjugado del producto es el producto de conjugados, que el conjugado de la suma es la suma de conjugados, y que el conjugado de un número real es él mismo (con lo que $\overline{a_i} = a_i$ para $i = 0, 1, \ldots, n$, y $\overline{0} = 0$), se tiene que

$$\overline{P(z_0)} = a_n \overline{z_0}^n + a_{n-1} \overline{z_0}^{n-1} + \cdots + a_1 \overline{z_0} + a_0 = 0.$$

Pero la igualdad anterior implica que $\overline{z_0}$ es raíz de $P(z)$ (de hecho, lo que dice es que $\overline{P(z_0)} = P(\overline{z_0}) = 0$). □

Lo anterior implica que, si tenemos un polinomio $P(z)$ con coeficientes reales, sus raíces complejas siempre vienen *por pares*: si tenemos una raíz compleja, también debemos tener a su conjugada. Vamos a ver ahora que el problema del cálculo de raíces está absolutamente relacionado (de hecho, son las dos caras de una misma moneda) con otro problema, el de la factorización de polinomios. *Factorizar* un polinomio es escribirlo como producto de polinomios más sencillos, es decir, de menor grado; por ejemplo, $P(z) = z^2 - 1$, que tiene grado 2, puede escribirse como $(z+1)(z-1)$, es decir, como producto de polinomios de grado 1.

Si, por ejemplo, $P(z) = (z^2 - 1) = (z+1)(z-1)$, entonces al dividir $P(z)$ entre $z+1$ el resto es cero, es decir, la división es *exacta*. Necesitamos por tato recordar algunas cuestiones básicas sobre división. En la división de números naturales hay un *dividendo* D, un *divisor* d, un *cociente* C y un resto r, que cumplen

$$D = dC + r, \ r < d.$$

Observemos además que la condición $r < d$ es esencial, porque es la que nos indica cuándo detener el proceso de división. De la misma forma, cuando dividimos dos polinomios $P(z), Q(z)$, hay un dividendo, $P(z)$, un divisor, $Q(z)$, un cociente $C(z)$ y un resto $r(z)$, que verifican

$$P(z) = Q(z)C(z) + r(z), \ \text{grado}(r(z)) < \text{grado}(Q(z).$$

En este caso la condición $\text{grado}(r(z)) < \text{grado}(Q(z))$ reemplaza a la condición $r < d$ de la división entre números naturales, y de nuevo es la que nos indica cuándo detener el proceso de división.

Teorema 9 (Teorema del resto)**.** *El resto de la división* $P(z) : (z-a)$ *es* $P(a)$.

Demostración. Consideremos la división $P(z) : (z-a)$, donde el divisor es $Q(z) = z - a$. Por la expresión que hemos visto antes, se tiene que

$$P(z) = (z-a)C(z) + r(z),$$

donde $C(z)$ es el cociente de la división $P(z) : (z-a)$, y $r(z)$ es el resto. Pero observemos que $r(z)$, de hecho es una constante, es decir, no depende de z. La razón es que el grado del resto siempre es menor que el del divisor; como el divisor es $z - a$, que tiene grado 1, el grado del resto $r(z)$ debe ser 0, es decir, $r(z)$ debe ser una constante. Por consiguiente, podemos escribir $r(z) = r \in \mathbb{C}$. Evaluando entonces la identidad $P(z) = (z-a)C(z) + r$ en $z = a$, y puesto que r es constante, se tiene

$$P(a) = (a-a)C(a) + r.$$

Por lo tanto, como $a - a = 0$, se obtiene $r = P(a)$, es decir, el resto de la división $P(z) : (z-a)$ coincide con $P(a)$. □

La consecuencia de este teorema es el siguiente resultando, donde esencialmente se muestra que calcular raíces *es* de hecho equivalente a factorizar un polinomio, y al revés.

Corolario 10. *El valor $z = a$ es raíz de $P(z)$ si y sólo si existe $Q(z)$ tal que $P(z) = (z - a)Q(z)$.*

Demostración. ($\Rightarrow$) Si $z = a$ es raíz de $P(z)$, por definición de raíz se tiene que $P(a) = 0$. Por el Teorema del Resto, el resto de la división $P(z) : (z-a)$ es $r = P(a)$. Como $P(a) = 0$ entonces $r = 0$, luego la división es exacta, es decir, existe $Q(z)$ tal que $P(z) = (z-a)Q(z)$, y $Q(z)$ es el cociente de la división $P(z) : (z-a)$. ($\Leftarrow$) Supongamos que $P(z) = (z-a)Q(z)$. Entonces $P(a) = (a - a)Q(a) = 0 \cdot Q(a) = 0$, luego $z = a$ es una raíz de $P(z)$. □

Por lo tanto, encontrar soluciones para $P(z) = 0$, con $P(z)$ un polinomio, implica, también, factorizar $P(z)$. Observemos que si $z = a$ es una raíz de $P(z)$, y por tanto $P(z) = (z - a)Q(z)$, es decir, $z - a$ es un factor de $P(z)$, dicho factor puede estar elevado a un exponente mayor de 1. Por ejemplo, $P(z) = z^2 - 2z + 1 = (z - 1)^2$; ciertamente $z = 1$ es una raíz de $P(z)$, luego $z - 1$ es un factor de $P(z)$, pero aparece elevado al cuadrado. Esto motiva la siguiente definición.

Definición 11. *Sea $P(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_0$ un polinomio donde $a_i \in \mathbb{C}$. Se dice que z_0 es una* **raíz de multiplicidad** *$m \geq 1$ de $P(z)$, si*

$$P(z) = (z - z_0)^m \cdot Q(z),$$

con $Q(z)$ un polinomio de grado $n - m$.

Si en la definición anterior $m = 1$, se dice que la raíz es *simple*; si $m > 1$, que es *múltiple*.

Finalmente, nos preguntamos cuántas raíces tiene un polinomio de grado n. Claramente puede tener, como mucho, n raíces, porque si tuviera más de n raíces, teniendo en cuenta que cada raíz da lugar a un factor de grado 1 (si la raíz es múltiple el grado es mayor), al multiplicar nos encontraríamos que el grado del polinomio es mayor que n. Por lo tanto debe tener, como mucho, n. Si nos preguntamos por las raíces reales, entonces no hay mucho más que podamos decir. Pero si nos preguntamos por las raíces complejas, la pregunta se puede responder totalmente, y viene dada por el siguiente teorema, cuya demostración requiere técnicas avanzadas, por ejemplo de Variable Compleja, que aparecerán en la asignatura de Métodos Matemáticos de la Física.

Teorema 12 (Teorema Fundamental del Álgebra)**.** *Todo polinomio $P(z)$ de grado n, con coeficientes complejos, tiene n raíces sobre $\mathbb{C}$ (contadas con multiplicidad).*

Observemos que no todas las raíces tienen por qué ser distintas (puede haber raíces múltiples). Además, es equivalente a decir que, sobre los complejos, cualquier polinomio $P(z)$ puede escribirse como

$$P(z) = a_n(z - z_1)(z - z_2) \cdots (z - z_n),$$

donde a_n es el coeficiente del término de mayor grado, y los z_i, $i = 1, \ldots, n$, son las raíces complejas (algunas de las cuáles pueden ser reales, y algunas de las cuáles pueden coincidir, si las raíces son múltiples) de $P(z)$. El teorema es falso sobre los reales: por ejemplo, $P(z) = z^2 + 1$ no tiene factorización posible sobre $\mathbb{R}$, aunque sobre $\mathbb{C}$ se tiene $P(z) = (z + i)(z - i)$.